

TESTIMONY BEFORE THE ERISA ADVISORY COUNCIL WORKING GROUP ON PRIVACY  
AND SECURITY ISSUES AFFECTING EMPLOYEE BENEFIT PLANS

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

July 20, 2011

I am David Wray, President of the Profit Sharing/401k Council of America (PSCA). For more than sixty years, PSCA, a national non-profit association of 1,000 companies and their six million employees, has advocated increased retirement security through profit sharing, 401(k), 403(b), and related defined contribution programs to federal policymakers and makes practical assistance with profit sharing, 401(k), and 403(b) plan design, administration, investment, compliance, and communication available to its members. PSCA is based on the principle that “defined contribution partnership in the workplace fits today’s reality.” PSCA’s services are tailored to meet the needs of both large and small companies with members ranging in size from Fortune 100 firms to small, entrepreneurial businesses.

In my comments today I will address privacy and security in employer-sponsored defined contribution plans as affected by the move from paper-based plan access and decision execution to the Internet. I will begin by documenting the change.

PSCA first collected data about Internet administrative practices for the 1997 plan year. Our most recent data is for the 2009 plan year. The table below illustrates the change in the use of the Internet in just this short period.

Table 1. Percentage of Companies Providing Services Via The Web

| Service Provided               | 1997  | 2009  |
|--------------------------------|-------|-------|
| Enrollments                    | 3.9%  | 57.0% |
| Balance Inquiries              | 36.2% | 91.9% |
| Contribution Changes           | 12.2% | 69.7% |
| Investment Changes             | 28.3% | 90.7% |
| Loans                          | 5.5%  | 64.6% |
| Hardship Distributions         | 3.5%  | 39.5% |
| Final/Retirement Distributions | 2.4%  | 51.6% |
| None                           | 60.2% | 7.2%  |

Since its introduction in 1981 the 401(k) system has been constantly improving. This move from paper to the Internet is one such improvement. Compared to paper, the Internet delivers far more information, far more conveniently, and at far less cost. The Internet is also the preferred medium of younger workers.

The Council has indicated that this move to the Internet has raised concerns about privacy, security, and fraud as well as opportunities for greater control. I will address each of these concerns. I will address the small company situation specifically. Also, I will incorporate the results of the PSCA snapshot survey responses of 234 plan sponsors on this topic.

## Internet Vulnerability

The Internet is vulnerable in three places: where the data resides, the computer(s) and practices of the end user, and the communications system that connects them. Those responsible for protecting the data accessible through the Internet are aware of all three of these vulnerabilities. Based on my research, conversations with providers, and the results of our snapshot survey, it is clear that to date the employer-sponsored retirement system has not experienced significant problems.

## Multifactor Authentication

Existing authentication methodologies involve three basic “factors:”

- Something the user knows (e.g., password, PIN);
- Something the user has (e.g., the insertion of ATM card, smart card); and
- Something the user is (e.g., biometric characteristic, such as a fingerprint).

Currently, retirement plans rely on two user “knows” pieces, the username and password. In other words the retirement system requires one type of authentication. At this time no one is considering issuing ATM- like cards or requiring physical authentications. However, there is consideration of adding more “user knows” items, as well as other approaches such as sending an additional code to a smart phone.

## Privacy

Employer-sponsored defined contribution plans are individual account plans and a significant amount of personal information must be attached to each participant account. Overwhelmingly plan sponsors have outsourced the management of this information and it resides in the databases of third-party record keepers. Typically, both plan sponsors and participants access this data using the Internet. These third-party record keepers have extensive protections in place to attempt to prevent “hackers” from obtaining the information of the individuals in their record-keeping systems and the defenses against attacks are constantly evolving. For example, providers can now use IP addresses to track anyone attempting to gain illegal access. To the best of my knowledge, to date, there has been no successful breach by outsiders of these defenses.

Sponsors and participants access their defined contribution plan data by having unique usernames and personal passwords. This process mirrors standard practice throughout the financial services industry. However, it too is evolving. Initially usernames and passwords could be simple and short. Systems increasingly are requiring longer usernames and passwords with a mix of letters and numbers. Overall this system has provided privacy protection for plan participants, as with others with financial accounts, unless a participant carelessly secures their information or improperly shares it with others.

For the purposes of our discussion it is important to differentiate privacy from the other issues raised by the Council in that protecting plan participant privacy is not a fiduciary obligation. Certainly there are other reasons for securing the privacy of participant information for both plan sponsors and record keepers. Plan sponsors offer plans to attract, retain, and motivate high-quality workers. Any breach of plan participant privacy would significantly damage the plan's credibility and undermine an employer's ability to achieve plan-related objectives. Record keepers have contractual obligations with employers to secure the privacy of participant information. In addition, record keepers are held to privacy practices supervised by their regulating agencies and by statute. For example, the Gramm–Leach–Bliley Act (*GLB*),

also known as the Financial Services Modernization Act of 1999, imposes privacy protection requirements on financial services companies, and the Security and Exchange Commission and the Federal Trade Commission have imposed, by regulation, specific safeguards as has the OCC for banks. It should be noted that GLB-imposed Internet security requirements do not extend to the recordkeeping done for retirement plans and there are no federal requirements for record keepers that are not also financial institutions.

States also are taking action. For example, California has special rules for disposing of user information. Of special importance is the Massachusetts law that went into effect on January 1, 2010. This law identifies the standards that have to be met to safeguard the personal information contained in both paper and electronic records by anyone who owns or licenses personal information about a resident of the Commonwealth of Massachusetts. This law affects employers, employer plans, and retirement plan service providers. In part, and with some paraphrasing, the law requires that every person who owns or licenses personal information about a resident of the state and electronically stores or transmits such information, to establish and maintain a security system covering its computers, including any wireless system that at a minimum has in place:

- secure user authentication protocols including:
  - controlling user IDs and other identifiers
  - establishing a reasonably secure method of assigning and selecting passwords
  - controlling data security passwords and protection of those passwords
  - restricting access to active users and active user accounts
  - blocking access to user identification after multiple unsuccessful attempts to gain access
- secure access control measures that:
  - restrict access to records and files containing personal information to those who need such information to perform their job duties
  - assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls
- encryption of all transmitted records and files that travel across public networks
- reasonable monitoring and systems for unauthorized use of or access to personal information
- encryption of all personal information stored on laptops and other portable devices
- for files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches
- reasonably up-to-date versions of system security software which must include malware protection and reasonably up-to-date patches and virus definitions
- education and training of employees on the proper use of computer system security and the importance of personal information security.

I have attached a copy of the Massachusetts statute to my prepared remarks.

Because of cost considerations most providers have only one set of Internet security protections. As a result, those who maintain electronically available data, at a minimum, typically structure their programs to meet the highest regulatory standard. This means that even those not technically protected by a particular regulation or statute can benefit from the highest levels of protection.

I would add that the move to the Internet has enhanced the privacy of plan participants as the old paper-based systems managed internally by plan sponsors were far less secure. When I was a plan administrator

in the early 1980s my staff maintained the participant records and produced the reports distributed to plan participants and copies were secured in locked file drawers in the finance department. This process required that several employees have access to participant information. The privacy of plan participant information was far more vulnerable than today when, as plan administrator of PSCA's plan, I am the only person with access to that information. Also, I rely on my ability to access necessary plan-related information maintained by my record keeper using the Internet so that I am able to keep paper files in the office to a bare minimum.

In our snapshot survey plan sponsors were asked to rank as high, medium, or low the vulnerability to a privacy breach with paper, phone, and the Internet. Twenty-four percent said that the risk of a breach affecting distributions/loans/withdrawals with paper was high, 18% said the risk with phone access systems was high, and 16% said the risk was high with the Internet. It should be noted that some call center personnel access participant information using the internet which requires that participants provide their user name and password before they can receive service.

In our discussions during the preparation of my testimony, concern was expressed about the access that providers have to participant information and what they may or may not be doing with that information. It has been an ongoing concern by both the DOL and plan sponsors that plan service providers not use participant information for cross selling or other inappropriate uses. However, this concern arises out of the decision by plan sponsors to outsource the record keeping function and is not necessarily exacerbated by the move to provide access to plan data using the Internet.

## Security

ERISA imposes a fiduciary obligation on plan sponsors to have processes in place so that plan assets are where they should be, when they should be there. This includes ensuring that plan distributions are only made to those who own the assets, i.e. the participants. The use of the Internet in effectuating a loan, withdrawal or distribution has two aspects. The first aspect concerns a participant's decision to take a loan, withdrawal, or distribution, and the need to access their plan information by entering a username and password to connect to their account and direct that plan-related action. The second occurs at the time of the actual delivery of the money and how it is received. Because Federal law requires that those receiving loans acknowledge receipt of certain mandatory disclosures, plan trustees make plan loan disbursements utilizing paper checks mailed to the participant's home address with acknowledgement through the participant's endorsement. Withdrawals and distributions are also usually effectuated by paper checks mailed to the participant's home address. However, some record keepers make available to participants the electronic transfer of a distribution, especially when the assets are being rolled over into an IRA.

As Table 1 demonstrates, while virtually all plans allow participants to access their plan information using the Internet, a smaller percentage allow participants to direct the plan to disburse loans, hardships and withdrawals. According to the PSCA snapshot survey 41% permit direct deposit or electronic transfers. 27% have an extra higher level of security for transactions directed either by paper or through the internet. 11% allow their participants to "lock down" their accounts so that no distributions can be made unless the account is "unlocked" by the participant.

Another consideration should be addressed regarding data security depending on plan size. While it is becoming routine for a large plan sponsor to include a requirement that a provider explain its process to secure data available over the Internet when it sends out a Request For Proposal (RFP) for plan services, I do not have any data but I doubt that small companies raise this issue when they send out an RFP. In the

PSCA snapshot survey about half the respondents have privacy and security policies that applied to their retirement plan, though in most cases they are part of a general policy covering benefits.

It should be noted that the payroll process is now overwhelming internet based. Electronic fund transfer of paycheck deposit and plan contributions is standard. As of January 1, 2011, all payroll tax payments must be made online. The Internet security of financial transactions has far greater scope than that for retirement plans.

## Fraud

A famous miscreant once said that he robbed banks because that's where the money is. It has always been important to protect plan assets from plan sponsor and plan provider employees with access to plan assets. Today most employee contributions are made by electronic fund transfer directly from an employer's payroll system to the system of the record keeper. This system is far more secure and accurate than when the plan sponsor's accounting department mailed a check and a spreadsheet to those managing plan assets and keeping the plan's records. Also, the availability of detailed activity in participant's accounts has given plan them the opportunity to verify that their contributions are where they are supposed to be when they were supposed to be there.

In plans, fraudulent misappropriation of assets occurs primarily in three situations: when the plan sponsor executes the fraud, when the plan sponsor fails to exercise the required fiduciary oversight, or when there is fraudulent behavior by those who manage the money. Such situations are rare, but they do happen and the Department of Labor has been successful at identifying and prosecuting those guilty of fraud. It is my understanding that participant complaints generate a significant percentage of DOL investigations. The fact that participants have access to far more complete information about their accounts than ever before because of the Internet helps enhance the DOL's fraud fighting capability.

To the extent there have been issues, and three percent of sponsors responding to our survey said there had, they have been the result of family fraud and identity theft. In no case has a participant lost plan assets as a result of hacking either directly into a provider's record-keeping system or the communications system that connects end-users with their stored data. It important to note that fraud is a criminal activity and is subject to the criminal justice system.

Finally, plan sponsors are required to purchase a ERISA bond to reimburse the plan in the event plan participants are damaged by fraudulent activity. Specifically, a plan sponsor must purchase a bond equal to 10% of the maximum assets that the insured thinks will be held in the plan over the fiscal year (per the federal statute). The maximum bond limit required by federal statute is \$500,000 (unless the insured is advised otherwise by the U.S. Department of Labor). Also, many plan sponsors purchase fiduciary insurance which would cover them in the event of a fiduciary breach.

## Employers And The Opportunities For Greater Control

As I mentioned before, employer-sponsored defined contribution plans are individual account plans and a significant amount of personal information must be attached to each participant account. Plan sponsors also access plan information using the Internet. They too use usernames and passwords to access plan data. They benefit just like participants from having access to more complete information 24/7. But plan sponsor internet access to plan data has an additional benefit. In the past the generic management reports available from providers were crude and out of date. To obtain management reports that were customized

to the plan sponsor's need and were based on up-to-date information required special provider intervention and generated additional cost either to the employer or the plan. Today plan administrators can access up-to-date plan information using any number of pre-prepared reports, and even create their own.

Clearly plan sponsors should not use participant account information for other than administrative and fiduciary required purposes and 62% of those responding to PSCA's snapshot survey indicate that they do not permit employer access to retirement and benefit data beyond what is necessary. However, what is necessary is extensive. For example, plan sponsors are required to ensure that each participant's contribution is being properly deposited in the plan and properly allocated among the plan's investment options. Plan sponsors are also responsible for ensuring that account balances are correct and that any distributions, but especially final distributions, are for the correct amounts. They are also responsible for complex compliance testing that requires detailed participant information. In the event such testing requires refunds of participant contributions, the plan sponsor is responsible for making those refunds and providing the explanation to each participant that those refunds require. Plan administrators and fiduciaries must have access to detailed participant information if they are to fulfill their legally required plan related obligations.

This is in contrast to the plan sponsor's obligation for their employee health insurance programs. In these programs the plan sponsor need merely insure that participants are properly enrolled in the program and premiums are paid. There is no compliance testing requirement and no asset management responsibilities unless the sponsor is using a VEBA to fund the program. Even when using a VEBA there are no participant privacy issues as the VEBA is a collective trust and there are no individual accounts. Imposing HIPPA-like privacy requirements on the employer-sponsored defined contribution system could only be done if at the same time plan sponsors were relieved of most of their fiduciary responsibilities. In PSCA's opinion this would seriously diminish the major benefit of the employer-sponsored defined contribution system, which is intensive employer oversight of every aspect of the program.

I would point out that employers have had and continue to have significant information about those who work for them. The ability to access information stored electronically off-site has not changed the employer's access and use of such information. For example, employers with defined benefit pension plans have typically reviewed the vested status of employees as they have developed early retirement packages.

### Small Companies

The move to electronic administration and Internet access has significantly enhanced the opportunities for small employers to offer programs comparable to companies with much larger numbers of employees. Today small employers have a much wider range of plan choices than even 10 years ago. Because of the ability to aggregate large numbers of small plans on one electronically administered platform and provide plan access to participants and plan sponsors using the Internet, small companies can choose from among open architecture and bundled programs with a menu of plan design features originally available only to larger companies. Also, while small company plans are still more expensive than larger plans, the move to electronic administration and Internet access has resulted in the elimination of front end loads and the reduction and even elimination of expensive wrap arrangements.

At the same time plan sponsors, both small and I believe large as well, do not have the technology competence, time, or the leverage with their providers to impact web privacy and security processes. They have no choice but to rely on those servicing their plans to provide Internet protections.

## Recommendations

Based on conversations with plan sponsors and feedback from plan sponsors participating in PSCA's snapshot survey I have the following recommendations:

**Privacy and security policies:** it would be useful if the ERISA advisory Council developed templates that plan sponsors could use in developing their own retirement plan Internet privacy and security policies, either as stand-alone policies or for inclusion in more broad-based benefits policies.

**Questions for providers:** it would be useful if the ERISA Advisory Council developed a template of suggested questions that plan sponsors could use as part of a Request for Proposal (RFP) or ongoing monitoring process to determine if their record keepers have privacy and security protections in place.

**Regulation:** there should not be Department of Labor regulation in this area. Federal agencies and state law already require those managing individual information electronically and making it available over the Internet to maintain high levels of privacy and security protections. Further, holding plan sponsors accountable to 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.

## Conclusion

In conclusion, permitting plan participants and those with administrative or fiduciary responsibility for plans to access employer-sponsored defined contribution data using the Internet has benefited both participants and sponsors. It gives them more complete information 24 hours a day, every day of the year. It increases plan transparency and enhances plan oversight. In the case of small companies more plan flexibility is now available at lower cost.

While there is potential for damage from a breach if one of the major recordkeeping systems is successfully hacked by an outsider, so far no such breach has occurred. Privacy and security breaches are typically the result of participants either sharing or casually protecting their usernames and passwords. At the same time, Internet privacy and security issues now affect every aspect of our lives and addressing retirement plan concerns are just one part of a much larger puzzle.

Plan sponsors and providers have significant motivation to protect the privacy of plan participants but it is not a fiduciary obligation. It is a fiduciary obligation to protect the plan assets. Plan sponsors have an obligation to ensure that processes are in place to prevent unauthorized people who work for the plan sponsor and those who manage plan assets as well as hackers and others using the Internet from fraudulently taking money from a participant's account. At the same time, plan sponsors do not have the technology competence, time, or the leverage with their providers to impact web privacy and security solutions. They are dependent on their providers for Internet privacy and security protections.

Clearly plan sponsors should not use participant account information for other than administrative and fiduciary required purposes. However, plan sponsor employees with administrative or fiduciary responsibility for operating the plan need access to detailed participant information if they are to fulfill

their legal obligations. This is very different than is the case for employer-provided health insurance programs.

The move to electronic administration and Internet access has significantly enhanced the opportunities for small employers to offer programs comparable to companies with much larger numbers of employees.

One plan sponsor summed it up well in a comment they provided in the PSCA snapshot survey. "Security risk is inherent in all we do nowadays. You mitigate it by choosing reliable vendors and being careful with your own and your employee's data. More regulations aren't going to change the risk."

Thank you for the opportunity to address this important topic and I would be pleased to answer any questions.