ASPPA®
WORKING FOR AMERICA'S RETIREMENT

4245 North Fairfax Drive
Suite 750
Arlington, VA 22203
P 703.516.9300 F 703.516.9308
www.asppa.org

Statement for the Record of Richard Carpenter Submitted to the Advisory Council on Employee Welfare and Pension Benefit Plans

On Behalf of The American Society of Pension Professionals and Actuaries (ASPPA)

September 1, 2011

Data Security and Privacy

INTRODUCTION

The ancient city of Nineveh (Assyria not Indiana) is mentioned in Genesis. There, archeologists uncovered what is believed to be the oldest lock. Over the next four millenniums, there have been constant and significant advancements in technology designed to protect property. Securing property is a problem as old as civilization.

The internet is a way of life in the 21st century. For all the advances the internet has provided, it is now easier for the criminal element to conduct its business. There are primarily two risks to the third party administrators of retirement plans ("TPAs"); the criminals can steal from a participant's account or they can steal a participant's identity. The threats are both internal and external and it is imperative that we are diligent against both.

THIRD PARTY ADMINISTRATORS (TPAs)

Types of Retirement Plan TPAs

As 401(k) plans have evolved over the past 30 years, so has the definition of a TPA. Retirement plan industry observors generally divide the TPA industry into two groups:

Recordkeeping Services - Bookkeeping for retirement plans' trading transactions and individuals' accounts (the major activity in recordkeeping).

Administration Services - Administrative functions including compliance testing against relevant pension and tax laws and filing of government reports such as Form 5500, *Annual Return/Report of Employee Benefit Plan*. This type of TPA is commonly known as a "Compliance TPA." The duties of a Compliance TPA include:

- Contribution deductibility calculations (Internal Revenue Code ("Code") § 404);
- Annual additions testing (Code § 415);

- Top heavy testing (Code § 416);
- General testing (Code § 401(a)(4) - for new comparability plans and DB/DC combo plans);
- Coverage testing (Code § 410(b));
- ADP/ACP testing (applicable to 401(k) plans);
- Preparation of Form 5500 and related schedules; and
- Preparation of Summary Annual Report for participants.

How Many TPAs?

Cerulli Associates issued a special report on the TPA marketplace stating that there were 1,154 TPAs.[1] I believe that the Cerulli report fails to recognize TPA operations that are part of law firm, accounting firms and advisory firms.

I have over 2,000 TPAs in my database and Tim McCutcheon of FT William – A Wolters Kluwer company, believes the number is close to 4,000. One thing is clear; the vast majority of TPAs are very small businesses. As discussed further below, the U.S. Department of Labor estimates that there are nearly 512,000 401(k) plans.[2] If we assume that there are 2,000 TPA firms, than the average is only 256 plans per TPA.

TPAs – Reliance on Others

The 401(k) marketplace is very competitive. In order to be competitive, providers must offer services that include participant websites, educational materials, investment descriptions, toll-free telephone support and daily accounting. Providing these services is capital intensive and beyond the financial resources of the vast majority of TPAs. These TPAs have become compliance firms. They have formed alliances with major financial services companies, including banks, insurance companies, mutual fund companies, and trust companies to do recordkeeping functions. I do not know of a single compliance TPA in the 401(k) marketplace that does not rely exclusively on alliance partners for recordkeeping functions. These financial service company alliance partners are among the most regulated companies in the industry.

While the TPA firms' consulting and compliance activities are integral to the operations of the plans, the administrative duties of a compliance TPA are primarily ministerial. They help insure that participant data is accurate and they prepare often complex discrimination tests. Compliance TPAs NEVER take custody of plan assets. Also, in most cases, there are separate contractual relationships between the plan/plan sponsor and the compliance TPA and the plan/plan sponsor and the financial service company doing recordkeeping.

How Many Plans Are Defined Contribution Plans?

[1] Cerulli Associates, *Evolving Role of TPAs in the Small- and Mid-Sized Retirement Plan Markets: Implications for Asset Managers and Distributors*, Cerulli Special Report (2011).
[2] U.S. Department of Labor, *Private Pension Plan Bulletin: Abstract of 2008 Form 5500 Annual Reports* 44 (2008), available at http://www.dol.gov/ebsa/PDF/2008pensionplanbulletin.PDF (indicating that there are 511,582 401(k) plans) (hereinafter "2008 Form 5500 Annual Reports").

The Department of Labor reports that the qualified plan marketplace included approximately 718,000 private pension plans, including nearly 670,000 defined contribution plans. [3] There were over 511,000 participant-directed 401(k) plans.[4]

2008 Form 5500 Data

	All DC Plans[5]	Small DC Plans[6]		Large DC Plans[7]	
Total DC Plans	669,156	597,240	89%	71,916	11%
Total Assets	$2,662,537 million	$488,659 million	18%	$2,173,878 million	82%
Number of Participants	82,509,000	11,545,000	14%	70,964,000	86%
Average # of Participants	**123**	19		987	
Average Plan Assets	$3,978,948	$818,195		$30,228,016	
Average Participant Account	$30,270	$42,326		$30,634	

In April of 2011, Pensions & Investments issued a report on the largest defined contribution plan record keepers.[8] Pensions & Investments indicated that 53 firms responded to the survey.[9] According to this study, these firms provided services for over 587,000 plans, covered nearly 79 million participants and had total defined contribution plan assets of nearly $3.9 trillion.[10]

For all intents and purposes, this group of 53 firms comprises the vast majority of the defined contribution plan marketplace. I would add a few companies, but my analysis would otherwise be unchanged. Only a handful of these firms could be described as a "compliance" TPA. I know of no firm in this group that does not have a SAS 70 audit. The top ten firms on the Pensions & Investments report by number of plan sponsors handle approximately 57% of DC plan sponsors, 47% of all DC participants and 75% of all DC assets.[11]

[3] 2008 Form 5500 Annual Reports, *supra* at 3.
[4] *Id.* at 49.
[5] 2008 Form 5500 Annual Reports, *supra* at 3.
[6] *Id.* at 5 (plans with fewer than 100 participants).
[7] *Id.* at (plans with 100 or more participants).
[8] Robert Steyer, *Large DC record keepers tighten grip*, Pensions & Investments (Apr. 2011), available at http://www.pionline.com/article/20110404/PRINTSUB/304049997. See also, *Special Report: DC Record Keepers*, Pensions & Investments (Apr. 2011).
[9] *Id.*
[10] *Id.*
[11] *Special Report: DC Record Keepers*, Pensions & Investments (Apr. 2011) (indicating that the top ten DC record keepers by number of plan sponsors handle 380,340 plan sponsors, 38,553,630 participants, and $2,008,885 million in assets). As indicated above, the Department of Labor reported that in 2008, there were 669,156 DC plans, 82,509,000 DC participants, and $2,662,537 million in DC assets.

EMERGI-LITE II?

Around Labor Day in 1997, the 135 workers at Emergi-Lite's plant in Westbrook, Connecticut, which manufactured emergency signs, were told that their factory would be shutting down. To make matters worse, a couple of months later the 85 participants in the 401(k) plan were told that all the money in their plan had been stolen. Eventually, the plan's TPA/investment advisor was convicted of embezzling more than $1 million.

As one might imagine, there was a significant desire in the legislative and regulating communities to "do something." U.S. Congressman Sam Gejdenson introduced the Small Business Employee Retirement Protection Act of 1998.[12] This act would have attempted to solve the problem by forcing small plan sponsors to hire accountants to audit their plans or hire corporate trustees to safeguard the plan assets.

ASPPA had many conversations with the legislative staff in Representative Gejdenson's office. We strongly suggested that the cost of their correction would be onerous and that a more reasonable solution would be to expand the bonding limits from 10% of assets to 100%. The premiums for ERISA bonds are very low because there are very few losses.

The expanded bonding requirements were eventually adopted through regulatory action by the Department of Labor and we believe it has greatly enhanced the security of retirement plan assets without unnecessarily increasing costs that would ultimately be borne by participants. It is also important for the ERISA Advisory Council to recognize that it is not possible to completely prevent fraudulent acts from occurring. As recent headlines have indicated, computer hacking and other fraudulent activities go on even within the most highly respected and government regulated institutions and data security companies.[13]

ASPPA CERTIFICATION for SERVICE PROVIDER EXCELLENCE

The retirement industry has been proactive with regards to data security and privacy. ASPPA and the Centre for Fiduciary Excellence, LLC ("CEFEX") have introduced a standard set of practices for recordkeeping and administration firms in the U.S. retirement industry entitled, "Standard of Practice for Retirement Plan Service Providers."[14] These practice standards form the basis for a certification program intended to increase assurance among plan sponsors and fiduciaries that a recordkeeping or administration firm is utilizing the industry's best practices. Firms that successfully complete the CEFEX review process are awarded the ASPPA Certification for Service Provider Excellence (the "ASPPA/CEFEX Certification").

The program arose through the efforts of an ASPPA task force first established in 2007 whose members saw the need for an independent review and certification program for retirement plan administration and recordkeeping firms. Based on that task force's recommendations, ASPPA and CEFEX jointly developed a complete certification program, using a format similar to that

[12] House Resolution 4238 (1998).
[13] *See, e.g.*, John Markoff, *SecureID Company Suffers a Breach of Data Security*, The New York Times B7 (Mar. 17, 2011), available at http://www.nytimes.com/2011/03/18/technology/18secure.html?ref=emccorporation.
[14] Centre for Fiduciary Excellence, *Standard of Practice for Retirement Plan Service Providers*, available at http://www.cefex.org/downloads/ASPPA%20Standard%20of%20Practice%20v1.51%20FINAL.pdf.

deployed for fiduciary advisor certifications under similar CEFEX programs. The intent of the ASPPA/CEFEX Certification program is to establish a comprehensive system of assurance for retirement plan sponsors. A plan sponsor whose plan is being serviced by a firm that has attained ASPPA/CEFEX Certification can be assured that the industry's best practices are in use throughout that firm's administration and/or recordkeeping procedures. Just recently in 2010, the program was revised to provide a unique certification for Compliance TPAs.

Before a firm can qualify for certification, a comprehensive investigation and review process is used to verify adherence to each standard of practice, using evidence from interviews, data gathering, and document review. With respect to technology and data security, the Technology Practice Criteria[15] include the following standards and evidence of compliance.

Criteria 1: Technology Plan

The organization has a well-documented technology plan addressing hardware and software maintenance and development needs. Evidence of this plan could include:

- The plan is updated on a regular basis.
- There is evidence of regular technology maintenance. Software inventory, including version(s) in use, is documented.
- A policy on how often system, application and custom software security patches are applied.
- There is a high level of security consciousness amongst IT staff and users.
- Evidence can include messages from IT staff to users regarding security tips.
- The default system set-up policy disables all unused hardware.
- There is a security strategy for in-house developed systems.
- A limited number of people have "'administrator" rights and there is a policy on granting access.

Criteria 2: Back-Up and Disaster Recovery

Back-up procedures and disaster recovery plans are in place. Evidence of these procedures and plans could include:

- Evidence that the disaster recovery plan has been tested.
- Security procedures for the clients' assets. There is a log of past back-ups.

[15] *See generally*, Centre for Fiduciary Excellence, *Standard of Practice for Retirement Plan Service Providers*, Practice Standard 1.4.1.

- Back-up tapes are password-protected.

Criteria 3: Up-To-Date Technology

The organization has up-to-date technology, which is supported by qualified staff. Evidence of this could include:

- Information systems that are sufficient to support Employee Retirement Income Security Act of 1974 ("ERISA") compliance administration and daily recordkeeping services if applicable.

- The firm has established a useful life for hardware. Hardware is replaced on a regular basis.

- IT staff have minimum training requirements.

- The organization checks for up-to-date critical security patches (e.g., the service available at http://windowsupdate.microsoft.com can be used from any user desktop).

- The IT staff maintains up-to-date virus protection.

- Security logs are reviewed regularly.

- IT staff maintains internet filtering and restrictions are placed upon the users.

Criteria 4: Protections Against Theft and Embezzlement

There are adequate processes and procedures to ensure that client assets and information are protected from theft and embezzlement. Evidence of these processes and procedures could include:

- Encryption software is utilized and updated as appropriate.

- Data is not transported off-site, unless on encrypted laptops (or other encrypted means).

- Documented security procedures are in place to protect client information and assets, which are clearly understood by staff.

RECOMMENDATIONS

The data security and privacy issues discussed in my testimony are concerns that are almost universally known and appreciated. Unfortunately, the scope of the threats and avoidance procedures are less known. No business owner, if for no other reason than reputation risk, wants their computer systems compromised. Education is an integral part of any solution and the Department of Labor ("DOL") can play an integral part. I suggest that the DOL *Strategic Plan for Participant & Compliance Outreach, Education and Assistance* be amended to include programs to assist the regulated community in dealing with these issues.

Additionally, ASPPA sponsors regional and national conferences that attract thousands of attendees. These conferences provide a perfect venue for the DOL to help professionals and participants alike.

Part of the DOL educational outreach should address the issue of insurance against these risks, much in the way FEMA educates homeowners about flood risks.

By addressing these issues through education, practical solutions can continue to be developed as was done in the Emergi-lite situation. As then, it is critically important to make sure that any new requirements balance the potential benefits against the potential costs, which, as noted earlier, are ultimately borne by participants.

♦ ♦ ♦

Thank you for the opportunity to discuss these issues. We welcome the opportunity to discuss these issues with you. If you have any questions regarding the matters discussed herein, please contact Craig Hoffman, ASPPA General Counsel and Director of Regulatory Affairs at (703) 516-9300.

Largest DC Recordkeepers – Pensions & Investments – April 4, 2011

Record Keeper	# of Plans	Rank	# of Participants	Rank	Assets	Rank
Paychex	52000	1	600000	29	13200	32
ING Retirement Services	50903	2	5419944	2	291868	3
John Hancock	44187	3	1660965	16	63388	16
Nationwide	43136	4	2662693	10	83881	14
Bank of America Merrill Lynch	41523	5	3668627	5	118007	9
AXA Equitable	35497	6	811668	26	18639	29
Principal	30755	7	3104123	8	96805	12
Fidelity	28760	8	14963600	1	940488	1
VALIC	26847	9	2496269	11	55381	18
TIAA CREF	26732	10	3165741	7	327228	2
Ascensus	26687	11	1409951	18	31821	23
Lincoln Financial	24276	12	1374109	19	38824	21
Great West	24271	13	4405807	4	146618	7
MetLife	23944	14	1222054	21	28991	25
TransAmerica	14930	15	576102	30	14471	31
Security Benefit	10752	16	196302	40	4954	41
AUL	9860	17	369102	33	10084	34
ICMA	7143	18	816203	25	35640	29
MassMutual	6470	19	1116153	24	47967	20
Wells Fargo	6202	20	2818862	9	157900	6
Prudential	4624	21	2357843	12	98267	11
Alliance Benefit Group	3994	22	340255	34	11464	33
CPI Qualified Plan Consultants	3957	23	293816	37	6480	38
Standard Insurance	3884	24	612262	27	14709	30
UNIFI	3371	25	112642	45	5333	40
Insperity	3126	26	70133	48	1472	48
Securian	2557	27	204834	39	9658	35
Diversified Investment Advisors	2383	28	1505450	17	48610	19
T Rowe Price	2256	29	1879960	14	113544	10
Newport Group	2112	30	404726	32	22120	26
Alerus	2090	31	151954	42	7541	36
Lincoln Trust	1880	32	6161	52	773	49
New York Life	1724	33	1140555	23	29392	24
Vanguard	1689	34	3460645	6	273805	5
Mid-America Admin	1571	35	601034	28	640	51
DailyAccess	1300	36	295000	36	6500	37
BB&T	1221	37	150736	43	6141	39
Charles Schwab	1174	38	1257399	20	90856	13
EPIC Advisors	1133	39	80353	47	3553	44
Correll	988	40	47000	50	650	50
Milliman	853	41	562046	31	19006	28
M&I Trust	769	42	324782	35	21777	27
JP Morgan	688	43	1718766	15	119041	8
Sun Trust	643	44	126655	44	4636	43
Federated	445	45	65600	49	2525	47

Record Keeper	# of Plans	Rank	# of Participants	Rank	Assets	Rank
Mercer	425	46	1189545	22	62249	17
USI Consulting	418	47	193726	41	3501	45
BOK Financial	410	48	214253	38	4940	42
McCready & Keene	256	49	85181	46	3215	46
ACS	171	50	1916392	13	71600	15
Reed-Ramsey	152	51	13900	51	304	52
Aon Hewitt	104	52	4653374	3	288205	4
GAMCO	6	53	538	53	22	53
Totals	**587249**		**78895791**		**3878684**	