AICPA & CIMA
Together as the Association of International Certified Professional Accountants®

STATEMENT OF JASON EDDY
CHAIR
AICPA EMPLOYEE BENEFIT PLANS EXPERT PANEL

BEFORE THE ERISA ADVISORY COUNCIL
REGARDING
RECORDKEEPING IN THE ELECTRONIC AGE

JULY 19, 2023

Thank you for inviting me to testify here today. I am Jason Eddy, a member of the Employee Benefit Plans Expert Panel (the Expert Panel) of the American Institute of Certified Public Accountants (AICPA) and a Managing Director with Grant Thornton. I am the national practice leader for Grant Thornton's employee benefit plan practice.

We applaud the Council's focus on recordkeeping in the electronic age, including examining the tools and technologies used by plan sponsors and third-party service providers to manage and retain plan records electronically; identifying recent trends in electronic recordkeeping systems; and exploring the authenticity, accuracy, and completeness of the electronic recordkeeping, the long-term availability and retention of plan records, and the disclosures and controls in place to ensure the reliability of electronic records.

You have asked for testimony today to address whether guidance would be beneficial with respect to records retention, the authenticity and reliability of the electronic records, and the data security of electronic records. We believe such guidance would be beneficial to plan sponsors in meeting their fiduciary responsibilities and would help ensure that participants will receive all benefits owed to them.

Plan sponsors are subject to fiduciary responsibilities for plan administration functions such as maintaining the financial books and records of the plan — including protecting sensitive data — and filing a complete and accurate annual return/report for the plan (Form 5500, *Annual Return/Report of Employee Benefit Plan* (Form 5500)). In addition, an integral component of ERISA is providing protections for plan participants, one of which is a plan financial statement audit. Failure to properly maintain and retain adequate plan records violates the plan sponsor's fiduciary responsibilities and also may weaken the protection of plan participants contemplated by ERISA.

Central to the accounting profession's mission is to help ensure meaningful financial reporting to protect ERISA plan participants and other financial statement users. Independent auditors of plan financial statements are not involved in the plan's recordkeeping activities, including the decision to outsource; however, independent auditors do require access to relevant, reliable, and complete records in order to perform the annual audit. As such, our remarks will focus on the effect of electronic recordkeeping on the auditor's ability to perform a quality audit, including the authenticity and reliability of the electronic records; the consequences of inadequate records retention; and the data security of electronic records that affect the plan's financial reporting.

Accuracy and Reliability of Information

The shift to electronic/digital recordkeeping is increasingly affecting the auditor's ability to do a quality

audit in accordance with professional standards. This, in turn, affects plan sponsors' ability to meet their fiduciary responsibility for filing a complete and accurate Form 5500. We believe that small plan sponsors are particularly affected, as I'll discuss throughout my testimony.

Auditors must comply with Generally Accepted Auditing Standards (GAAS) in performing plan financial statement audits. Two standards, Statement on Auditing Standard (SAS) No. 142, *Audit Evidence*, and SAS No. *145, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement,* are particularly relevant to the audits performed in an electronic environment in which source documents are not created and/or maintained. SAS No. 142 requires that the auditor consider the possibility that information may not be reliable and whether the information is sufficiently precise and detailed. In the electronic environment, several risks may affect the reliability of audit evidence. SAS No. 145 requires auditors to assess the risks of material misstatement in the plan's financial statements through understanding the plan and its environment, including the plan's internal control and outsourced activity relating to plan recordkeeping and reporting functions. SAS 145 places an increased focus on testing of the IT system.

When information to be used as audit evidence is available only in electronic form, the sufficiency and appropriateness of the audit evidence usually depends on the effectiveness of controls over their accuracy and completeness. Furthermore, the potential for improper initiation or alteration of information to occur and not be detected may be greater if information is initiated, recorded, processed, or reported only in electronic form, and appropriate controls are not operating effectively.

When information has been transformed from its original medium (for example, documents filmed, digitized, or otherwise transformed to electronic form), the reliability of that information may depend on the controls over the information's transformation and maintenance. In some situations, the auditor may be able to perform substantive audit procedures to address reliability. For example, when participant forms have been scanned into the HRIS or payroll system, the auditor may inspect the hard copies in personnel files to validate the authenticity of information in electronic form. However, if hard copies of the personnel records are not maintained, the auditor may determine that it is necessary to test controls over the transformation and maintenance of the information.

Determining whether controls are effectively designed and implemented (including general IT controls, as appropriate) may help the auditor design appropriate audit procedures to evaluate the reliability of information. In some cases, the reliability of such information may only be established when the related controls, whether manual or automated, including those over the preparation and maintenance of the information, have been tested and determined to be operating effectively.

Recordkeeping functions for both large and small plans—both DB and DC—are outsourced by most plans of all types, which means auditors may need to consider the controls at service organizations to evaluate the reliability of information; System and Organization Control (SOC) can help with this. A SOC 1 report focuses on controls over outsourced services that could impact a company's financial reporting. Type 2 SOC 1 reports, which address management's description of a service organization's system and the suitability of the design and operating effectiveness of controls throughout a specified period are the most useful to plan sponsors and their auditors.

Most of the recordkeepers for the plans audited by larger audit firms are the very large and reputable organizations where type 2 SOC 1 reports are available. Because SOC 1 reports can be extremely important to plan sponsors in fulfilling their fiduciary duties and may significantly reduce the cost of an audit, it is important that plan sponsors obtain those reports. However, many plan sponsors are not familiar with SOC 1 reports and the benefits they provide. Even plan sponsors who do obtain SOC 1 reports may not understand how they should be used and/or that there must be complementary user entity controls (CUECs) in place on their end. The CUECs are integral to the design and operating effectiveness of the *overall* control environment and must be in place in order rely on the SOC 1 report.

It is important to note that service organizations are not required to furnish SOC 1 reports, and in

many cases, smaller service providers do not. With the DOL's change in the audit threshold for defined contribution retirement plans, it is estimated that approximately 10,000 plans that are currently audited will not require an audit when the regulation takes effect. Without the added protections that a GAAS audit provides, it is even more important that those plan sponsors understand the value of a SOC 1 report, and that they make sure when hiring a service provider that the service provider obtains a SOC 1 report. In addition, plan sponsors should be educated about the importance of obtaining and reading the report and following up on any issues noted.

While type 2 SOC 1 reports are valuable for the purpose of determining the nature, timing and extent of substantive procedures that must be performed, they may not address the reliability of information input into the system. In situations where a type 2 SOC 1 report does not address data input or is not available, or recordkeeping is not outsourced (e.g., in house payroll systems), the auditor will need to place greater emphasis on information technology (IT) systems work in the human resource information system (HRIS) and payroll system to determine the reliability of the information. This means that firms will need IT experts to adequately evaluate systems.

While large firms have IT experts in house that can assist in the plan audits, small firms typically do not. As such, small firms would need to engage IT experts or stop performing EBP audit engagements. If small firms were to engage IT experts, it likely would result in an increase in audit fees, which negatively affects plan sponsors and/or participants. And many large firms are reducing the size of their employee benefit plan audit practices, so currently, much of the work is getting pushed down to smaller firms. The population of firms has been steadily shrinking (7,300 firms performed EBP audits in 2011; in 2020 that number was 4,300), which means there are fewer small firms to take on the engagements that in the past were performed by large firms. This makes it more difficult for plan sponsors to find a quality auditor at an affordable price. And firms of all sizes have recently had to turn away potential clients because they didn't have the capacity to perform the work.

If plan sponsors are unable to hire an auditor to perform their plan audits, they will be unable to fulfill their fiduciary responsibilities for filing a complete and accurate Form 5500, which will result in the rejection of the Form 5500 filing. In addition to rejecting the Form 5500, the DOL has the right to assess substantial monetary penalties on plan sponsors for the deficient filing. And fiduciaries who do not follow the basic standards of conduct may be personally liable to restore any losses to the plan.

Another issue we are seeing is an increase in the number of qualified SOC 1 reports. Depending on the reason for the qualification, it may call into question the reliability of the information provided by the service organization. This may affect the auditor's ability to rely on the report. If the qualification is relevant to the controls over information being audited, such a system failure will require the auditor to perform alternate procedures. When no hard copy records are available, the options available to auditors for performing alternate procedures is limited.

Alternate procedures that are increasingly performed include confirmation of participant information. While confirmation of personal information is straightforward and reliable, confirmations may not be as effective for financial information such as account balances and investment elections, as participants frequently rely on the information provided by the recordkeeper to complete the confirmation. In those situations, the auditor still may be unable to determine the reliability of the information and must do further controls testing or other alternate procedures if no source documents are available.

There also are data protection risks that come with the confirmation process, which is increasingly performed electronically. If confirmations containing social security numbers, salary information, account numbers, addresses, and other personally identifying information (PII) are sent in an incorrect manner, such as via unsecured email, it may result in data loss. There is also a risk that electronic confirmations could be emailed to the wrong person. I'll address other data protection issues later in my testimony.

Plan Records Retention

As fiduciaries, plan sponsors are responsible for plan administration functions, such as maintaining and retaining the financial books and records of the plan. Records retention is critical in the determination of the benefit entitlements of a participant or beneficiary. In addition, if adequate records are not properly retained, it is possible that plan sponsors will not be able to fulfill their fiduciary responsibility for obtaining a financial statement audit for the plan.

To perform the audit of an employee benefit plan, the auditor needs access to a variety of plan and participant level records to perform testing and form conclusions on which to base the audit opinion. Therefore, it is important that the plan sponsor maintain current and historical records that support the activity of the plan and the participants who participate in the plan. For initial plan audits, that may include records that date back to the plan's inception.

Certain electronic information may be destroyed or deleted after a specified period of time (for example, if files are changed and back-up files do not exist). If the plan sponsor is unable to provide the requested data, the auditor will have to consider whether there are alternative procedures that can be performed that allow the auditor to obtain sufficient evidence to opine on the financial statements. Alternative procedures may include confirmations with individual participants, obtaining source documentation from a third-party provider to the plan (for example, an actuary), or testing larger numbers of transactions rather than relying on sampling, all of which could be very costly. If alternative procedures cannot be performed, the auditor may be unable to obtain sufficient appropriate audit evidence in order to form an opinion on the financial statements.

If the plan was previously audited by another firm, depending on the auditor's review of the information available from the prior auditor, the auditor might conclude additional testing of the plan's opening balances is necessary. Events such as plan mergers, plan spin-offs, a significant change in the number of plan participants, or a newly established plan also may result in an "initial audit" where opening balances must be tested.

It is not uncommon for a plan to change service providers. Recently, we have found that service providers may not maintain records for plans for which they no longer perform recordkeeping or may not grant auditors access to historical records if the plan no longer uses that service provider. This is particularly important for small plans that have been around for a number of years and grown to the point that it meets the requirements for an audit under ERISA. The auditor will need access to the historical accounting records and other information underlying the opening balances, which in an employee benefit plan, could span many years.

The significance of the plan records not made available to the auditor will dictate the type of report the auditor is able to issue as well as whether the auditor will even be able to accept the engagement. When the records are insufficient — even in circumstances beyond the control of the entity — it likely would result in a modification of the auditor's opinion (either a disclaimer of opinion or a qualified opinion).

A qualified opinion will be expressed when the auditor is unable to obtain sufficient appropriate audit evidence on which to base the opinion but concludes that the possible effects on the financial statements of undetected misstatements, if any, could be material but not pervasive. The auditor will disclaim an opinion when he or she is unable to obtain sufficient appropriate audit evidence and concludes that the possible effects on the financial statements of undetected misstatements, if any, could be both material and pervasive.

When the auditor disclaims an opinion, the auditor will state in the opinion paragraph that because of the significance of the matter(s) described in the basis for disclaimer of opinion paragraph, the auditor has not been able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion, and accordingly, the auditor does not express an opinion on the financial statements.

It is important to note that, generally, the DOL will reject Form 5500 filings that contain modified opinions.

If the auditor is aware of the fact that there is a lack of sufficient records such that the auditor believes the limitation will result in the auditor disclaiming an opinion on the financial statements as a whole, the auditor is prohibited from accepting the engagement which, again, would impede the plan sponsors ability to file a complete and accurate Form 5500.

Inadequate plan records may also have negative consequences in defense of litigation, including significant legal costs and fees, and even unfavorable judgments. Many judgments have been entered against plan administrators for failure to produce documentation supporting the plan's participant benefit calculations.

Records Retention Requirements

ERISA requires plan sponsors to retain broad categories of records related to meeting its fiduciary responsibilities. ERISA Sections 107 and 209 establish the requirements for record retention by the sponsor. Section 107 of ERISA includes requirements for the retention of records used to support plan filings. Section 209 addresses maintaining participant records used to determine benefits.

Section 107 of ERISA requires those plan records used to support filings, including, but not limited to the following, to be retained for at least six years from the filing date:

- Copies of the Form 5500 (including all required schedules and attachments);
- Nondiscrimination and coverage test results;
- Required employee communications;
- Financial reports and supporting documentation;
- Evidence of Plan's fidelity bond;
- Corporate income-tax returns (to reconcile deductions)

Section 209 of ERISA states that an employer must "maintain benefit records, *in accordance with such regulations as required by the DOL*, with respect to each of [its] employees sufficient to determine the benefits due or which may become due to such employees [emphasis added]." The records used to determine the benefits that are or may become due to each employee include, but are not limited to:

- Plan documents, and items related to the plan document including, adoption agreements, amendments, summaries of material modifications (SMMs), summary plan descriptions (SPDs), the most recent IRS determination letter, etc.
- Census data and support for such information including records that are used to determine eligibility, vesting, and calculated benefits (such as rates of pay, hours worked, deferral elections; employer contribution calculations)
- Participant account records and actuarial accrued benefit records
- Support and documentation relating to plan loans, withdrawals and distributions
- Board or administrative committee minutes and resolutions
- Trust documents

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes standards for the electronic exchange, privacy and security of health information, for ERISA welfare benefit plans

DOL Rule 29 CFR § 2520.107-1, *Use of electronic media for maintenance and retention of records*, provides guidance on the retention of plan information through electronic format, as follows:

- The electronic recordkeeping system has reasonable controls to ensure the integrity, accuracy, authenticity and reliability of the records kept in electronic form;
- The electronic records are maintained in reasonable order and in a safe and accessible place, and in such manner as they may be readily inspected or examined;
- The electronic records are readily convertible into legible and readable paper copy as may be needed to satisfy reporting and disclosure requirements or any other obligation under Title I of ERISA;
- The electronic recordkeeping system is not subject, in whole or in part, to any agreement or restriction that would, directly or indirectly, compromise or limit a person's ability to comply with any reporting and disclosure requirement or any other obligation under Title I of ERISA; and
- Adequate records management practices are established and implemented
- All electronic records must be legible and readable.

Generally, most original paper records may be disposed of any time after they are transferred to an electronic recordkeeping system that complies with the requirements of the DOL. However, plan sponsors should be aware that original paper records may need to be retained for audit purposes.

IRS Revenue Procedure 98–25 (revenue procedure) provides additional guidance on requirements for maintaining electronic tax records, including:

- The machine-sensible records provide sufficient information to support and verify entries made on the taxpayer's return and to determine the correct tax liability. The Revenue Procedure specifies how the plan may meet this requirement.
- The revenue procedure also requires that the plan maintain documentation of the business processes that create, modify and maintain records; support and verify entries made on the plan's return; and evidence the authenticity and integrity of the plan's records, and includes details about how this requirement may be met.

The use of a service organization does not alleviate the plan sponsor's responsibilities to retain adequate records. Additionally, the IRS revenue procedure specifies that a taxpayer's use of a third-party service organization (e.g., custodial or management services) in respect of machine-sensible records does not relieve the taxpayer of its recordkeeping obligations and responsibilities.

Based on our experience, standards are lacking with respect to monitoring outsourced service providers, including identification of performance standards, benchmarking of costs and mitigating conflicts of interest. We see many situations in which monitoring is not done regularly and in a systematic, prudent manner.

In addition, ERISA and DOL do not specifically address the retention of records related to a plan audit. The list of records necessary to perform an audit is quite extensive, and plan sponsors often are not aware of the importance of retaining them. There are certain common records and reports

which the auditor might initially request when auditing the financial statements of an employee benefit plan, some of which may already be addressed by ERISA and DOL rules, but others that are not. In addition to information requested at the beginning of an audit, the auditor will select samples of plan transactions and participants to test substantively. The information needed for the sample testing will depend on the type of plan, the nature of the transaction being tested, whether the plan has been audited previously, and the auditor's testing strategy.

We believe it would be beneficial to plan sponsors if the DOL provided additional guidance related to the retention of records that the auditor may need in order to perform the audit of the plan's financial statements, including initial information necessary to perform the audit as well as detailed information to support plan transactions and participants selected to test substantively. Because of the variables noted above, it is not possible to provide a complete listing of what detailed information might be requested by the auditor; however, I have included some examples of commonly requested items in the recommendations section below.

Data Protection

Plan sponsors are required to make sure that the plan complies with ERISA, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which establishes standards for the electronic exchange, privacy and security of health information, for ERISA welfare benefit plans.

ERISA does not specifically address whether or how plans should protect personally identifiable information (PII). PII maintained in electronic form could be maintained by plan sponsors and/or service organizations. Because any data that is stored electronically is potentially vulnerable, it is important to develop policies and safeguards for protecting that data.

The hiring of a service organization to assist in plan administration—such as bank trust departments, data processing service bureaus, insurance companies or other benefits administrators—is a fiduciary function. It is important that the service organizations a plan uses to perform investment processing, recordkeeping and/or benefit payments, claims processing, and other services that require access to the plan's sensitive data have adequate protections in place to safeguard that information.

Due to the substantial shift to electronic/digital recordkeeping, we believe that guidance should be provided to plan sponsors to help them ensure their data is protected, including performing adequate due diligence prior to hiring a service organization that handles PII and periodically monitoring the service organization to ensure it is properly protecting the data.

Recommendations

Authenticity and Reliability of Plan Records

We believe the DOL should educate plan sponsors about the importance of establishing strong records management practices that ensure the authenticity and reliability of their electronic records. We also recommend the DOL clarify that records management practices be documented, similar to the guidance in IRS Revenue Procedure 98–25.

As noted previously, service organizations are not required to furnish SOC 1 reports. Because SOC 1 reports can be extremely important to plan sponsors in fulfilling their fiduciary duties, we recommend the DOL educate plan sponsors about the importance of obtaining and reading those reports and ensure the necessary CUECs are in place. In addition, the DOL should encourage plan sponsors to make certain when hiring or retaining the service organization that the service organization agrees to obtain a SOC 1 report.

Records Retention

We believe that the DOL should issue more detailed regulations related to plan records retention, including:

- Detailed information about what records that need to be maintained and for what purpose and the period of time that these records must be maintained.
- Examples of records that may be required for an independent financial statement audit. ERISA Section 209 does not provide a specific period of time for retaining participant-level records such as demographic information, compensation and elections sufficient to determine benefits due, these records should be kept for an indefinite period of time in a format that is easily retrieved to ensure they are available upon request by the participant or auditor in case of an audit. As such, the regulations should note that certain benefit plan records may need to be maintained indefinitely.
- *Maintaining necessary paper records* — If electronic records don't establish a substitute or duplicate record of the paper records from which they are transferred under the terms of the plan or applicable federal or state law, the original records should not be discarded.
- A requirement that a plan sponsor establish best practices for ensuring adequate record retention, including:
    - *Establishing a written record retention policy governing how the organization periodically reviews, updates, preserves, and discards documents related to plan administration.* It should be approved by ERISA counsel or those charged with governance over the plan to ensure that federal and state retention laws are being considered and adhered to. When service organizations (e.g., recordkeeper, investment custodian) maintain plan records, the plan sponsor needs to understand the retention policies of those service organizations for plan records they prepare and/or maintain.
    - *Monitoring compliance with the written record retention policy* — If the plan uses service organizations, the plan sponsor should also monitor the service organizations' compliance with their respective retention policies.
    - *Categorizing and documenting plan records* — Data should be organized such that it can be easily and readily retrieved. Documentation should include the type of record, a brief description of the type of record, and the category to which records of this type belong. Records in the same category often have the same retention periods and might require similar treatment in other ways. Some general types of records that should be addressed as a part of any policy include:
        - Employer remittances and contribution reports
        - Benefit claims, benefit applications and supporting information
        - Vendor invoices, billings and contracts
        - Plan documents including the trust, Summary Plan Description, and related amendments and modifications
        - Employment-related records, including payroll records
        - Receipts and proof of disbursements, bank and

investment statements, and loan documents, if applicable

- Electronic data including emails and scanned documents
- Board of Trustee minutes, budgets, financial statements and annual reports/tax returns

- Guidance related to the retention of records that the auditor may need in order to perform the audit of the plan's financial statements, including initial information necessary to perform the audit as well as detailed information to support plan transactions and participants selected to test substantively. Following is a list of common records and reports which the auditor might request when auditing the financial statements of an employee benefit plan:
  - Plan document
  - Adoption agreement
  - Plan amendments
  - IRS determination or opinion letter
  - ESOP loan documents
  - Copies of any correspondence with regulatory authorities
  - Any investment contracts
  - Trust agreements
  - Service organization agreements
  - Actuarial reports and written confirmation of selected information used in preparing the report
  - Investment policy
  - Information about internal controls related to plan operations and financial reporting
  - A listing of all parties working with the plan
  - Plan accounting records for the year being audited, including trust, custodian or insurance company statements and recordkeeper statements
  - A detailed annual participant-level account summary
  - A listing of all employees employed at any time during the year and dependents eligible for plan benefits (including name, unique identifier, demographic data necessary for determining eligibility, compensation and plan contributions)
  - A listing of all benefit or claim payments made by the plan during the year being audited
  - A schedule of contributions to the plan
  - A listing of participant loans outstanding and new loans taken during the year
  - A schedule of expenses paid and accrued by the plan
  - Year-end payroll records

- Support for any plan mergers or transfers during the year
- Support for any prohibited transactions or litigation involving the plan
- Demographic data support (such as date of birth, date of hire, or date of termination)
- Enrollment, deferral and investment election support
- Payroll information (in total and for selected participants for the year and for specific pay periods)
- Support for an individual's wage rate and hours worked
- A participant's account statement
- Distribution requests, including support for hardship payments, death certificates, or other items that support the type of distribution
- Support for an individual's vesting
- Support for the calculation of benefit payments (including payments to dependents eligible for plan benefits), including source documentation to support the inputs to the calculation
- Loan authorization forms
- Amortization schedules
- Rollover paperwork
- Expense invoices

Although this does not comprise a comprehensive list, it provides an indication of the volume of the data that is required for a plan auditor to perform an audit in accordance with relevant professional standards.

Data Protection

We believe that the DOL should establish best practices for plan sponsors related to electronic data security, which may include:

- Follow the "minimum necessary" and "business need" principles and only share the minimum amount of data (especially personal data) needed to accomplish a task.
- Retain only that information that is truly necessary for the business purpose. Collect less data and purge unnecessary PII from your records to reduce vulnerability.
- Use caution in public spaces when handling or viewing personal information; be aware of your environment and use privacy screens on computers.
- Keep workspaces clear of personal information when not in use.
- Use secure methods to transmit personal information. For example, encrypt documents containing confidential information when emailing. Preferably, use an approved, secure collaboration site to transfer confidential data. Email generally should not be used to send personal information.
- De-identify data where possible. Mask or truncate government identifiers and health identifiers whenever possible.

- Control access to PII. Sensitive information should only be accessible by people who need it to do their jobs. This includes the information shared with the financial statement auditor. Check with the auditor to determine what PII is necessary for the audit.
- Require the service organization to complete a detailed questionnaire to assess its services and ability to adequately protect PII.
- Define PII broadly to make sure it includes all sensitive information to which the service organization will have access.
- Obtain acknowledgement from the service organization that the services require the processing of the plan's PII, and it will:
    - Comply with the privacy laws that apply to that PII;
    - Keep PII confidential;
    - Provide information and support as the plan may require to comply with privacy laws;
    - Limit its use of the PII to the fulfillment of services described in the contract and for no other purpose; and
    - Permit the plan sponsor to monitor the service organization's performance related to the protection of PII.
- Involve the plan's internal IT security personnel to evaluate the level of security offered by the service organization.
- Define a data security breach broadly to include suspected breaches and require that the service organization establish adequate procedures to prevent, detect, and remediate a breach.
- Require that the service organization notify the plan sponsor of, investigate, and remediate a breach, and assist the plan with any required notices to affected individuals.
- Obtain and review a SOC 2 report each year related to the services provided and follow up on any items of concern. SOC 2 reports on an organization's controls that directly relate to the security, availability, processing integrity, confidentiality and privacy as a service organization.
- Require the plan auditor, actuary, consultants, and others who provide professional services to the plan to:
    - Ensure encryption when transferring electronic files, file passwords, etc.
    - Establish physical safeguards over confidential information (for example, safeguarding of computers that contain confidential information, proper safeguarding of physical documents, etc.).
    - De-identify claims information in audit documentation.
    - Use SharePoint or a similar document management site to store client data.
    - Only use audit firm-issued thumb drives that are encrypted.
    - Direct any questions concerning IT security issues to client.

benefit plan records and *Effective monitoring of outsourced plan recordkeeping and reporting functions,* which were submitted along with the written testimony, provide additional information that may be of use in educating plan sponsors and developing best practices in these areas.

Conclusion

Thank you for your interest in this important matter and the opportunity for me to testify before the ERISA Advisory Council today. I will be happy to answer any questions.