Cybersecurity, Your Company, and the Safeguards Rule

This presentation is for educational purposes only. It is not legal advice for any particular situation. Laws change all the time. Always verify that information is accurate and up to date before you rely on it.

DISCLAIMER
Darius Davenport
Cybersecurity and Data Privacy Practice Group
Chairman, Crenshaw Ware & Martin, P.L.C.

Darius’ practice focuses on data privacy laws and regulations, helping clients mitigate cyber risk, and dealing with the legal and practical problems resulting from cyber incidents.

Agenda

01 Cybersecurity Overview
02 The Safeguards Rule
Cybersecurity Is Not Just an IT Issue...

Data Breach Statistics

### Root Causes of Data Breaches

- **Human Error**: 50%
- **System Glitch**: 42%
- **Malicious/Criminal**: 8%

### Framework
Cybersecurity Frameworks

- NIST Cybersecurity Framework.
- ISO 27001 and ISO 27002.
- SOC2.
- NERC-CIP.
- HIPAA.
- GDPR.
- FISMA.
The Safeguards Rule

• Title 16 Chapter I Subchapter C Part 314
• Enacted in 2003
• Amended in 2021 to keep pace with technology and provide more concrete guidance to businesses
• Purpose – ensure that covered entities protect the security of customer information.
The Safeguards Rule

• Application
  • Applies to Financial Institutions
  • Financial Institutions Defined – a business engaged in an activity that is financial in nature or incidental to such financial actives as defined in section 4(k) of the Bank Holding Company Act of 1956 12 U.S.C. 225.28 and 225.86
  • Very Broad Definition

The Safeguards Rule

• Financial Institutions Continued -
  • mortgage lenders, “pay day” lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders
The Safeguards Rule

• Financial Institutions Continued-
  • mortgage lenders, “pay day” lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders.

The Safeguards Rule

• Financial Institutions Continued-
  • A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity, and investment advisory companies.
  • Exemption for financial institutions with fewer than 5k consumers.
The Safeguards Rule Requirements

• Requirements
  • Develop, implement and maintain an information security program
  • Program must have (1) Administrative, (2) Technical, and (3) physical safeguards to protect Customer Information

• Customer Information – any record containing nonpublic personal information (paper, electronic or other form) maintained by you or an affiliate

The Safeguards Rule Requirements

• Put your Program In Writing
• Must match the size and complexity of your business
• Must match the nature and scope of your activities
• Must match the sensitivity of the personal information
• Must (1) ensure security and confidentiality, (2) protect against threats to security and information integrity, and (3) protect against unauthorized access that could result in harm
The Safeguards Rule Security Element 1

• Qualified Program Supervisor
  • Employee
  • Service Provider
  • Qualifications and know-how based on complexity of your organization
• Outside Service Providers must have their own Information Security Program
• You are still responsible if you outsource program supervision (Vet your providers)

The Safeguards Rule Security Element 2

• Conduct a Risk Assessment
  • Know what data (sensitive data) you have
  • Know where your data is stored
  • Know how much data you have
  • Know what (1) applications and (2) hardware you are using
  • Know who has network access
  • Understand the risk associated with all of the above
The Safeguards Rule Security Element 3

- Design Safeguards to Control Risk
  - Review access controls
  - Know what data you have and where it is stored
  - Encrypt customer/sensitive information
  - Application Inventory
  - Multi-Factor Authentication (MFA)
  - Data Retention/Secure Data Destruction
  - Anticipate and adapt to network changes
  - Log authorized users

The Safeguards Rule Security Element 4

- Monitor and Test Safeguards
  - Test your ability to respond to a data incident
  - Tabletop Exercises
  - Penetration Testing
  - Vulnerability Scans
The Safeguards Rule Security Element 5

• Training
  • Have a cybersecurity employee policy
  • Train your staff on your cybersecurity employee policy
  • Provide security awareness training
  • Provide reoccurring training opportunities

The Safeguards Rule Security Element 6

• Monitor Service Providers
  • Vet your service providers
  • Contracts should detail your security requirements
  • Contracts should detail incident response handling
  • Contracts should mandate incident response cooperation
  • Service providers should have their own INFOSEC program
The Safeguards Rule Security Element 7

• Keep INFOSEC Plans Current
  • Update your plans
  • Update after network changes
  • Update after application changes
  • Update after hardware changes
  • Update after Tabletop Exercises
  • Update after Cyber Employee Policy changes

The Safeguards Rule Security Element 8

• Develop a written Incident Response Plan (IRP)
  • IRP identifies who is on the Incident Response Team
    • Leaders, IT, Incident Counsel, Data Forensics
  • IRP defines team member roles and communication plan
  • IRP outlines responses to data incidents
  • IRP provides contact information for team members
  • IPR initiates incident investigation
  • Leads to incident after action report
The Safeguards Rule Security Element 9

• Report to your Leadership/Board of Directors
  • Your Qualified Individual must report to your board or equivalent body/individual
  • Report must be in writing
  • Report must assess company compliance with INFOSEC Plan
  • Must address risk management, control decisions, service provider arrangements, test results, security events, after action reports, recommended changes.
Safeguarding Taxpayer Data
A GUIDE FOR YOUR BUSINESS

CWM

CYBERSECURITY PROGRAM BEST PRACTICES

The Employee Benefits Security Administration has prepared the following best practices for plan fiduciaries and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plan service providers should:

1. Have a formal, well-documented cybersecurity program.
2. Conduct periodic risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business continuity program addressing business continuity, disaster recovery, and incident response.
10. Protect sensitive data stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

A Formal, Well-Documented Cybersecurity Program:

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fulfills its documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudentity designed program will:

Protect the infrastructure, information systems, and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- Identify the risks to assets, information, and systems.
- Protect each of the necessary assets, data, and systems.
- Develop and respond to cybersecurity incidents.
- Recover from the event.
- Disclose the event as appropriate.
- Restore normal operations and services.

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approved by senior leadership.
- Reviewed at least annually with updates as needed.
- Terms are effectively communicated to users.
- Reviewed by an independent third party auditor who confirms compliance.
- Documentation of the particular frameworks used to assess the security of its
TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

As sponsors of ERISA and other types of pension plans, business owners often rely on other service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices.

To help business owners and administras meet their responsibilities under ERISA to prudently select and monitor such service providers, we prepared the following tips for plan sponsors of all sizes:

1. Ask about the service provider’s information security standards, policies, practices, and audit results, and compare them to the industry standards adopted by other financial institutions.
   - Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity. You can have much more confidence in the service provider if the security of its systems and practices are tested by annual audit reports that verify information security system-wide availability, processing integrity, and data confidentiality.
2. Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.
3. Evaluate the service provider’s track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor’s services.
4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
5. Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identify theft breaches (including breaches caused by internal threats, such as recklessness by the service provider’s own employees or contractors, and breaches caused by external threats, such as a third party footing a plan participants’ accounts).
6. When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards — and be sure contract provisions that tie the service provider’s responsibility for IT security breaches. Also try to include terms in the contract that would enhance cybersecurity protection for the plan and its participants, such as:
   - Information Security Reporting. The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.

Example
Questions

Darius K. Davenport, Esq.
Crenshaw, Ware & Martin, P.L.C.
(757)623-3000
ddavenport@cwm-law.com
Cyber Hotline: (757) 802-9043
Thank You
Overview

Audit Changes

Impacts to Plan Fiduciaries

Auditing Changes SAS 134-141

<table>
<thead>
<tr>
<th>Standard (SAS)</th>
<th>Description</th>
<th>Effective for audits of financial statements for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>134</td>
<td>Auditor reporting and amendments</td>
<td>Periods ending on or after December 15, 2021</td>
</tr>
<tr>
<td>135</td>
<td>Omnibus – certain changes to conform to PCAOB standards</td>
<td>Periods ending on or after December 15, 2021 (Except amendments to AU-C 930 – effective for interim periods of fiscal years ending on or after December 15, 2021)</td>
</tr>
<tr>
<td>136</td>
<td>Auditor reporting on employee benefit plans</td>
<td></td>
</tr>
<tr>
<td>137</td>
<td>Other information included in annual reports</td>
<td>Periods ending on or after December 15, 2021</td>
</tr>
<tr>
<td>138</td>
<td>Amendments to the description of materiality</td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>Amendments to AU-C 800, 805, 810 for auditor reporting changes</td>
<td></td>
</tr>
<tr>
<td>140</td>
<td>Amendments to AU-C 725, 730, 935, and 940 for auditor reporting changes Amendments to AU-C 930</td>
<td>Periods ending on or after December 15, 2021 (Except amendments to AU-C930 – effective for interim periods of fiscal years beginning on or after December 15, 2021)</td>
</tr>
<tr>
<td>141</td>
<td>Deferral of effective dates for SAS 134-140</td>
<td>Effective upon issuance</td>
</tr>
</tbody>
</table>
What has changed?

- Addresses auditor’s responsibility to form an opinion on the financial statements and other related matters
- Changes form and content for all auditor’s reports under U.S. GAAS
- Contains requirements for when the auditor concludes that a modification to the auditor’s opinion is necessary and when additional communications are necessary in the auditor's report
Changes to the Auditor’s Report

Expanded descriptions of the responsibilities of:

Management
  • relating to going concern evaluation when required by the applicable financial reporting framework

The Auditor
  • relating to:
    • Professional judgment and professional skepticism
    • Going concern
    • Communications with those charged with governance

SAS 134

SAS 135 Summary
Primarily addresses guidance related to

- Communications with those charged with governance
- Consideration of fraud when there are significant unusual transactions
- Evaluation of transactions with related parties

SAS 135
Providing solutions. Creating value.

43

SAS 136 Summary
Forming an Opinion and Reporting on Financial Statements of Employee Benefit Plans subject to ERISA

Providing solutions. Creating value.

44
Overview

Auditing standard changes for retirement plans.

Three primary goals of SAS 136

• Improve auditor performance
• Enhance the quality of employee benefit plan audits
• Increase the communicative value and transparency of the auditor’s report

Effective for years ending on or after December 15, 2021.

What has changed?

• Engagement acceptance and obtaining additional management representations
• Performing additional risk assessment procedures related to the plan document, tax status, prohibited transactions, and responding to risks
• Communicating certain audit procedures and results to those charged with governance
• Performing additional audit procedures
• Issuing a new form of the auditor’s report
• No longer a limited scope audit
  • 103(a)(3)(C) audit
Engagement Acceptance

Auditor must document Management has:

- Maintained a current plan document, including plan amendments
- Administered the plan in accordance with plan provisions
- Determined a 103(a)(3)(C) audit is applicable

Reportable Findings:

Auditor is required to ascertain if reportable findings have occurred. Defined as:

- Noncompliance or suspected noncompliance with laws or regulations
- Using auditor judgement, a finding from the audit that is significant and relevant to those charged with governance
- Indication of deficiencies in internal control identified during the audit that are sufficient to merit management’s attention
- Obtain written representations of management
- Read a draft of the 5500
- Communication of Reportable findings to management or those charged with governance.
  - Description of the reportable finding
  - Sufficient information to enable those charged with governance and management to understand the context of the communication
  - An explanation of the potential effects of the reportable finding(s)

How does this affect Plan Fiduciaries?
• Maintain a *signed* plan instrument, including plan amendments

• Ensure the plan is operating within the plan's provisions.
  • Including keeping relevant documentation to support transactions

• Understand what a 103(a)(3)(c) audit is and if you qualify under ERISA.

• Review your 5500!
  • Accountant’s opinion section should be reviewed closely.

---

**What Fiduciaries should be prepared for**

*Documented responsibility*

  • Fiduciaries have always had the same amount of responsibility. However, auditors are required to more formally document that you are aware of your responsibilities.

  • Additional questions from auditors and representations from plan management.

*More detailed comments about audit findings going to governance*

  • Reportable findings should be shared with governance.
Other Compliance Considerations

- Compensation
- Plan Loans
- Remittances
- Eligibility
- Insurance
- Other

Questions?
Plan Sponsor’s Perch

With a Participant’s Perspective for Retirement
Best Practices

© Actuarial Benefits & Design Company
Specializing in Qualified Retirement Plan Consulting, Design & Compliance Testing

Lisa Germano, JD, CPA, CGMA
President and General Counsel
Actuarial Benefits & Design Company
804-379-4900
Lisa@ab-d.com

Areas of ERISA Consulting
- Privately Held Companies
- Nonprofits
- Retirement Plan Compliance with Tax Code
- Fiduciary Plan Governance – ERISA Title I
- Operational Internal Controls
- Government Enforcement Examinations
- Voluntary Plan Corrections

Industry Involvement
- Fellow, Virginia Law Foundation, 2019
- Mid-Atlantic IRS Pension Liaison Group Co-Chair, 2018, 2021
- Former Board Member, AICPA – 2006-2008
- Past chair, Virginia Society of CPAs – 2015-2016
- Fellow, American College of Employee Benefit Council - 2011
- Co-Founder, Central Virginia Employee Benefits Council - 1992
- Recipient: Arthur J. Dixon Memorial Award – 2015
- Inaugural AICPA Sustained Contribution Award – 2011
- President, Virginia Commission on Women and Minorities in the Legal Profession – 1993-1994

What are YOU reading?
I am always looking for a good book.
Currently I am reading Operation Pineapple Express by Scott Mann

Expertise & Passion:
- Perspective from early involvement in ERISA – bringing that to the clients we serve and professionals we collaborate with to keep qualified plans compliant.
- Developing plan governance processes and procedures.
- Speaking on leadership, employee benefit plan topics and authoring related articles, essays and courses.
- Working closely with other professionals to protect clients’ retirement plans and to meet plan sponsor goals.
Roles & Responsibilities
Plan Sponsor, Plan Administrator & Trustees

- Settlor Function
- ERISA 3(16) – Operational Duty
- ERISA 3(21) – Investment
- ERISA 3(38) - Investment
- ERISA 404(a) and (c) – Plan Participants as co-fiduciary
- Directed Trustee – In name only

Administration of Plan – Daily Operations

- Trustee
- Corporate Officers & Directors
- Employers
- Investment Managers
- Plan Administrators
- Third Party Administrators, Recordkeepers
- Third Party Consultant
- Insurance Companies and Agents
- Banks
- Professional service providers
- Accountants
- Actuaries
- Attorneys
- Auditors
- Brokers
Multiple Employer Plans and Pooled Employer Plans

• Read the agreement. All of them. Each MEP or PEP is structured a bit differently. Identify where the conflicts are in the roles being played. Who is a fiduciary.

• Most of these arrangements contain inherent conflicts of interest. As CPAs we understand independence and all arrangements must be given due diligence. Individuals who perform purely "ministerial" functions for an employee benefit plan within a framework of policies, interpretations, rules, practices, and procedures made by other persons are not fiduciaries.

Ministerial Functions

• In the day-to-day administration of an employee benefit plan, various individuals are responsible for performing functions that do not involve individual discretion or the rendering of investment advice. These functions are often referred to as "ministerial."

• Individuals who perform purely "ministerial" functions for an employee benefit plan within a framework of policies, interpretations, rules, practices, and procedures made by other persons are not fiduciaries.
Problematic Areas

High Alert

- Traditionally bundled arrangements
- MEPs
- PEPs
- Adopting Employer (Association Plans, Affiliate Plans)

- Who knows to read what in the contracts?
- What entity is responsible “in total” for the arrangement.
- Oversight for fiduciary function, hiring the Parent in Charge
Be Aware

• Plan Autopilot.

• Prudent Expert.

• Advocate.

Service Providers

• Not all providers are created equal
• Service Providers should be monitored
• Gaps in compliance identified
• Expert help to oversee
• “On Call” Counsel
Due Diligence
All the Time

• Periodic Investment Oversight
• Annual Check-up
• Plan Fiduciary Documents
• Service Matrix
• Ministerial Duties

Questions?