2024 FIDUCIARY TRAINING SERIES
PART 4: AVOIDING SCAMS

November 2024

LISA KEITH

Senior Manager of Plan Consulting | CAPTRUST

DAN DIGIACOMO

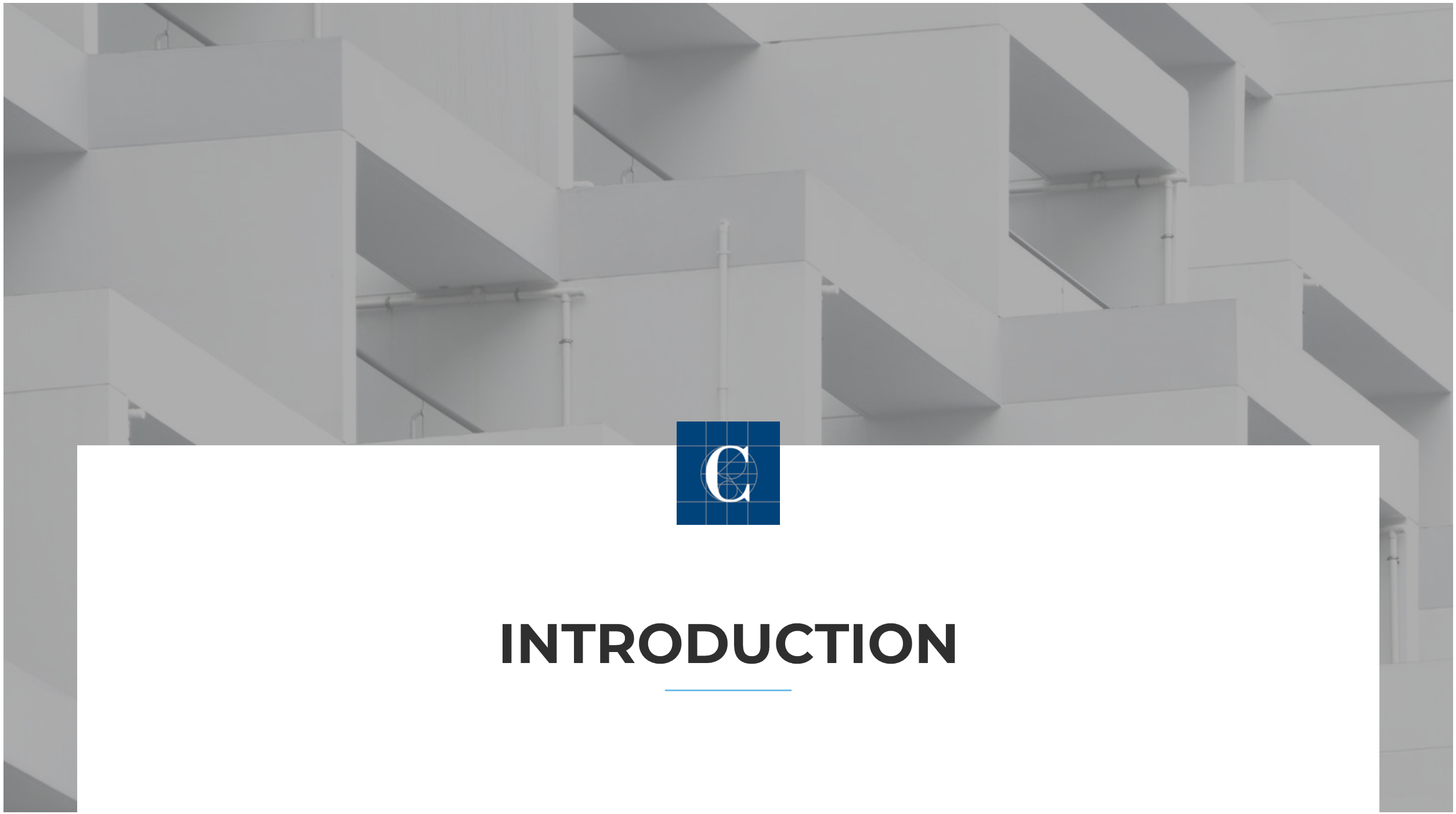
Principal and Financial Advisor | CAPTRUST

JON ATCHISON

Senior Team Lead of Governance, Risk, and Compliance | CAPTRUST

CYNTHIA BOYLE LANDE

Attorney | BrownWinick Law



INTRODUCTION

CYBERSECURITY BASICS

CYBERSECURITY BASICS | ACCESS CONTROL

Good Cybersecurity protects the **confidentiality**, **integrity** and **availability** of information.

- **Strong Access Control Requirements**
  - PW + MFA / SSO
- **Secured Communications**
  - Secure Message Portal
- **Secured Network Resources**
  - Principle of Least Privilege (PLP)
  - Role-Based-Access-Control (RBAC)
  - Regular Access Reviews

- **Secured Resiliency**
  - Encrypted, immutable backups
- **Prudent Risk Assessments**
  - Independent Third-Party
  - SOC 2 Engagement
  - Penetration Test
- **Guidance by Department of Labor's (DOL) "Cybersecurity Program Best Practices"**

KEY AREAS OF FOCUS FOR PLAN SPONSORS

Raise the Bar On Understanding the Threat Landscape

- Expertise Not Required
- Ask questions for the purpose of understanding.
- You bring strong business acumen to the cyber arena. Create synergy with your technology and cyber teams/vendors. Combining expertise from complementary domains always creates a better outcome.

Vendor Management & Accountability

- Contracts that Require Like Standards
- Can’t Transfer Accountability

DOL Guidance on Cybersecurity

- How does your cyber program compare to the framework put forth by the Department of Labor?

Cyber Insurance

- Research coverage options, consult with insurance professionals who understand your business so they can guide you to purchasing an effective policy, offer protection if the unthinkable happens.

WHEN PROPER PROTECTIONS ARE NOT IN PLACE

- Assumptions can be costly
- Non-validated security controls can & will be exploited
- Unpatched systems are a prime target for opportunistic attackers
- Negative headlines await
- **Attackers DO NOT CARE** about:
  - Fines or consequences resultant to their successful attack
  - Your clients
  - Your career
  - Your family

TAKING ACTION

- **Start with DOL Guidance on Cybersecurity Program Best Practices.**

- **Build a consistent and thorough third-party risk management program that focuses on:**
  - Independently Validated Security Posture (SOC 2 Type II)
  - Penetration Test Results
  - Strong contractual agreements, holding the third-party to acceptable security standards
  - Reassessment

- **Communicate to your employees about the scams that could cost them money.**
  - Romance Scams
  - Pig Butchering
  - Extortion on False Pretenses (Pay a ransom to release your kidnapped child!)

DOL GUIDANCE AND LITIGATION

BROWNWINICK LAW

Be Bold. Be Wise.

ERISA CYBERSECURITY

Safeguarding Retirement Plans

Why Cybersecurity Matters for ERISA Plans

- Risk profile
- Targeting of retirement plans
- Integration of plan operations and technology
- Regulatory expectations

ERISA Fiduciary Duties

- ERISA turned 50 in September!
- ERISA Fiduciaries must act prudently in protecting plan assets, including digital data. Fiduciaries are responsible for:
  - Selection and monitoring of service providers for cybersecurity risks.
  - Continuous evaluation of the effectiveness of cybersecurity practices.
- Process is more important than the outcome.

DOL’s Cybersecurity Guidance (Sept. 2024)

Best practices for plan sponsors:

Develop a comprehensive cybersecurity program.

Conduct risk assessments regularly.

Engage with service providers that have strong cybersecurity policies.

Carefully review service provider agreements.

Limit access to the extent needed to reasonably complete plan functions.

Provide recurring, current participant training.

Cybersecurity Program Best Practices:

Implement access control and identity management.

Ensure data encryption and secure system operations.

Regularly monitor and update security measures.

Online Security Tips for Participants:

Create online login credentials.

Use strong passwords and multi-factor authentication.

Be cautious of phishing and suspicious emails.

Incident Response Plan

Preparation

Develop and train response teams

Establish communication protocols

Deploy tools and resources

Detection & analysis

Monitor systems

Classify incidents based on severity and type

SCOPE & impact

Containment, eradication & recovery

Notify law enforcement and insurer

Limit spread

Remove the root cause (e.g., malware, unauthorized access)

Restore effected systems

Post incident activities

Debrief each incident

Update the program as needed.

Documentation!

Colgate-Palmolive Co.

- Fraudster stole $750,000 by accessing a participant's account, changing credentials, and directing a distribution of funds to the fraudster's account
- Impacted participant sued plan sponsor, recordkeeper, and custodial bank, alleging that the fiduciaries missed certain "red flags"
- Custodial bank was released from the case at the motion to dismiss phase because, the court found, it was not acting as a fiduciary in processing the distribution
- Plan sponsor and recordkeeper were not released from the case, but in September of 2024 the parties settled this case on undisclosed terms

Abbott Laboratories

- Bad actor breached the 401(k), transferring $245,000 out of the country.
- Several security lapses occurred, including failure of online security questions and inadequate account communications.
- Abbott and the service provider (Alight) were sued for breach of fiduciary duties for not securing the participant's account and not properly verifying the authorization for funds.
- The case highlighted that a failure to safeguard plan assets and ensure that service providers maintain adequate cybersecurity controls can result in liability for ERISA fiduciaries.
- Ultimately, the court found for the plan fiduciaries in this case.

Estee Lauder

- Estee Lauder's 401(k) plan was subject to a cybersecurity incident that resulted in unauthorized access to participant accounts.
- Hackers exploited weak security protocols (e.g., lack of notifications of transaction requests).
- The breach raised concerns about the adequacy of the plan’s cybersecurity measures.
- This case emphasized the need for continuous monitoring and updating of cybersecurity practices.

NEXT STEPS

TAKE ACTION

1. Provide practical steps that plan sponsors can take today to understand the potential risks to participants and how to protect them.
2. Review cybersecurity protocols of recordkeepers and other service providers.
3. Communicate with participants, providing tips on how to avoid being the victim of a scam.

QUESTIONS

Disclosure

This material is intended to be informational only and does not constitute legal, accounting, or tax advice. Please consult the appropriate legal, accounting, or tax advisor if you require such advice. The opinions expressed in this report are subject to change without notice. This material has been prepared or is distributed solely for informational purposes. It may not apply to all investors or all situations and is not a solicitation or an offer to buy any security or instrument or to participate in any trading strategy. The information and statistics in this report are from sources believed to be reliable but are not guaranteed by CAPTRUST Financial Advisors to be accurate or complete.

THANK YOU