Invesco

Cyber/Fraud in ERISA Plans

Bruce G. Lanser

Bruce Lanser, CIMA® CRPS® CRPC® AIF® CPM® CBFA® CPFA® CHSA®

Senior Retirement Plan Consultant

How we can help you

Bruce focuses his practice on delivering insights and results in three key areas within corporate retirement planning: sponsor and participant success, investment counseling and fiduciary guidance. He provides in-depth knowledge and experience to retirement committees with a well-documented process designed to help them comply with fiduciary responsibilities and optimize participants' retirement outcomes. To Bruce, advising a 401(k) plan is not just about investments and fees. It's about people, families and helping them feel confident about their future.

What makes us knowledgeable

For more than 30 years, Bruce has been helping plan sponsors strengthen their employee retirement plans and has been recognized and accredited for his hard work:

- PLANADVISER Top 100 Retirement Plan Advisers, 2019 and 2020
- Financial Times Top 401 Retirement Advisers, 2015 – 2019
- Certified Investment Management Analyst®
- Chartered Retirement Plans Specialist®
- Accredited Investment Fiduciary®
- Chartered Retirement Planning Counselor℠
- Series 7, 63 and 65 licenses
- B.S.B.A., accounting, Marquette University

Getting to know us

Bruce served as chairman of the Investments Committee of Junior Achievement of Wisconsin. He enjoys speed skating and is an international starter and one of just 24 individuals who qualify to be a starter at the Olympic Games. He and his wife Bernadette, enjoy spending time with their two wonderful children, BJ and Erica, both of whom are doctors

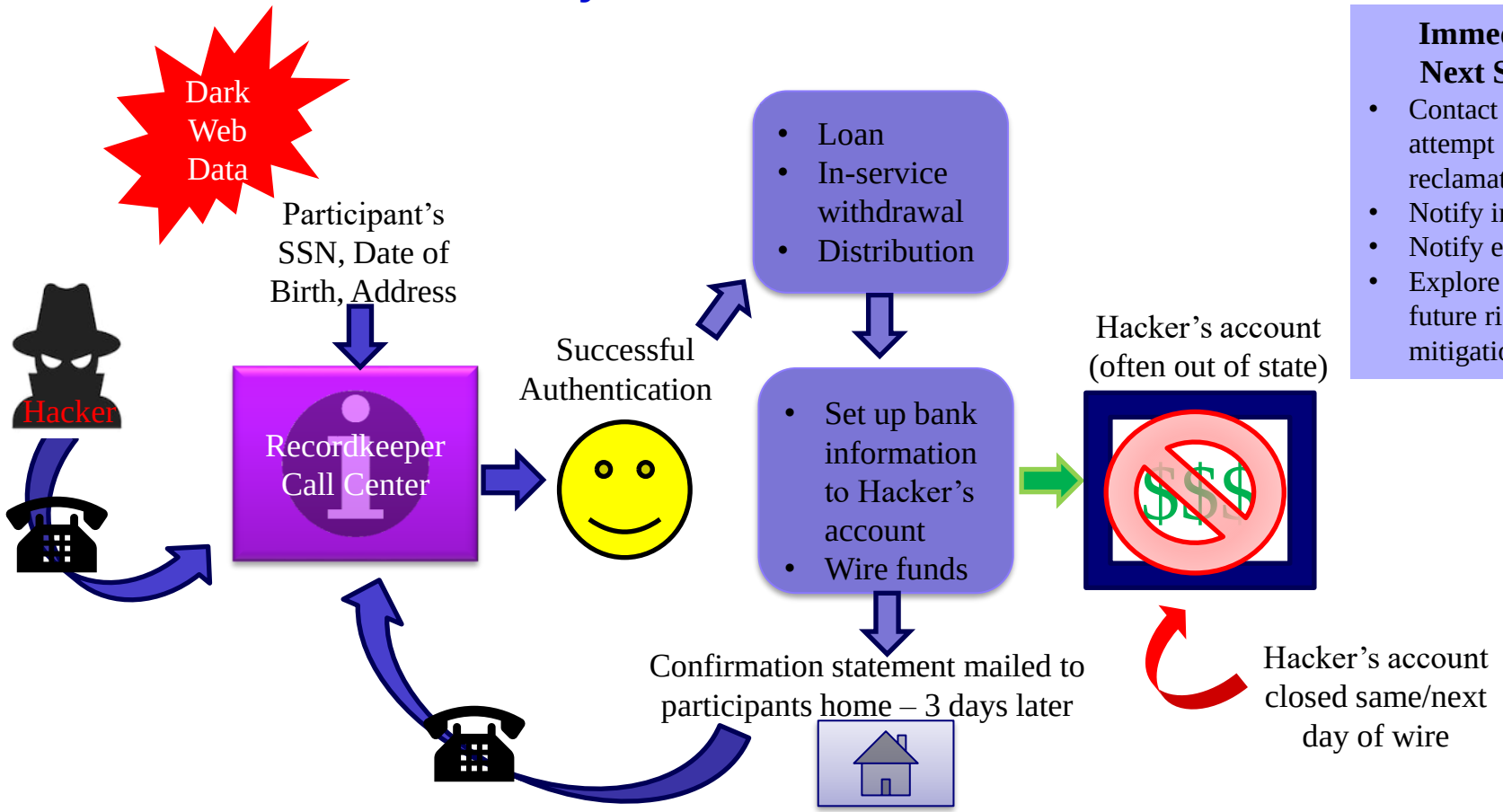
Speaker: Marina Edwards

Marina Edwards

Marina@marinaretirement.com
(608) 770-7658

- Founder of Marina Retirement, LLC in 2022
- 30 Year career focused on ERISA compliance and fiduciary risk mitigation
- Recent 2½ years with Invesco as Sr. DC Strategist
- 20+ Years with Willis Towers Watson as Senior DC Consultant focused on DC plans with $1B AUM
- Areas of specialization:
  - Plan governance
  - Compliance
  - Fiduciary training
  - Vendor search
  - Plan benchmarking

DC Plan hacked – A true story



Immediate Next Steps

- Contact RK and attempt reclamation
- Notify internally
- Notify externally
- Explore steps for future risk mitigation

Let the Litigation Begin . . .

- **Case 1** – **$99k** total of 3 unauthorized distributions ($12k, $37k, $50k)
  - Complaint alleged “failing to establish distribution processes to safeguard the plan assets against unauthorized withdrawals” and “failing to identify and halt suspicious distribution requests”
- **Case 2** – **$245k** Fraudulent online access, changed password and moved money to new bank account
- **Case 3** – **$360k** in theft from fraudulently obtaining employee personal information
  - Hacker placed US Mail post office hold on mail delivery
  - Retrieved held mail from post office using face employee ID and a forged written note
- **Case 4** – **$751k** in a single distribution where hacker accessed the account, changed mailing address, phone number, banking information
  - Compliant states the fact that the phone number and email address were from one country and the mailing address was a different country – “should have been a red flag that triggered some further action to confirm the legitimacy of the request.”

Source: Various court documents.

"Unauthorized acquisition of personal information . . ."

Nationwide Retirement Solutions, Inc. data breach

- **9/3/2022** – Nationwide stated "an unauthorized party accessed and copied data from the system"
  - 1,687 participants were impacted
  - Breached data included "everything" (Full Name, Social Security Number, Address, Email, Telephone Number, Date of Birth, Gender)
  - Nationwide services 2.6 million participants across 34,000 retirement plans with $174 billion AUM
- **9/27/2022** – *Jackson v. Nationwide Retirement Solutions, Inc.* filed in federal court in Ohio – complaints include breach of fiduciary duty to participants
  - Sheryl Jackson requested Personal Identifiable Information (PII) be deleted and destroyed "unless Nationwide can provide to the court reasonable justification for the retention and use of such information when weighed against the privacy interests of plaintiff and the class."
- Nationwide notified participants, plan sponsors, regulators and the FBI for criminal investigation
- Nationwide offered 2 years of credit monitoring and identity theft protection from Equifax

Source: Jackson v. Nationwide Retirement Solutions, Inc.

DOL Guidance on Managing Cybersecurity Risk

Steps to address cybersecurity risk and vulnerabilities

Establish a formal, well documented cybersecurity program

- ***DOL provides a list of 12 best practices for ERISA-covered plans***
- Identify personally identifiable information (PII) data to be protected
- Issue a Cyber/Fraud RFI with current and competing leading service providers
  - Determine how data is accessed, shared, stored, controlled, transmitted, secured and maintained
- Establish protocols and policies covering assessment of cybersecurity procedures
  - Updating, reporting, training, data retention, controlling access and third-party risks

Review service provider contracts and practices

- ***DOL provides a service provider review checklist for plan sponsors***
- Define security obligations, indemnifications, reporting and monitoring responsibilities

Communicate to participants

- ***DOL provides a retirement account tip sheet for participants***
- Educate participants on protecting their assets, what to do and who to contact if their accounts or identity has been compromised

Review insurance coverages

- Understand overall insurance programs covering plans and service providers
- Evaluate whether cyber insurance has a role in a cyber risk management strategy and consider the need for a separate policy covering the DC plan

Service provider insurance matrix

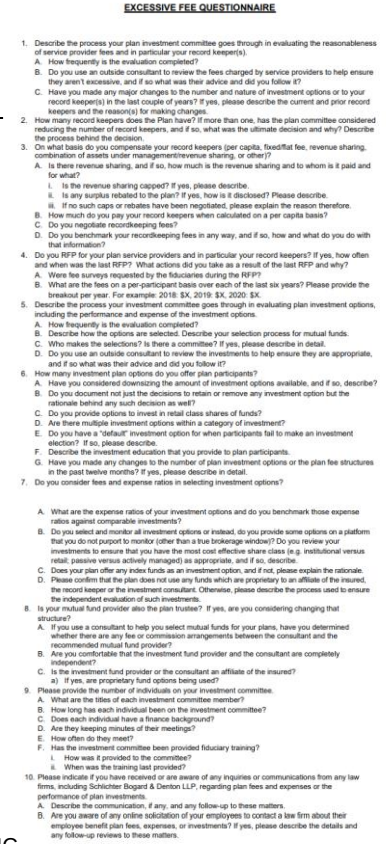
Coverage	Total Limits Carried Including All Access Coverage	Primary/First Layer Insurer	Retention/Deductible
Professional Liability			
Fiduciary Liability (if purchased separately from Professional Liability)			
Fidelity Insurance			
Cyber/Network Security Insurance			
Other?			

Underwriters Begin Asking Detailed Questions on DC plans

EXCESSIVE FEE QUESTIONNAIRE

1. Describe the process your plan investment committee goes through in evaluating the reasonableness of service provider fees and in particular your record keeper(s).
   A. How frequently is the evaluation completed?
   B. Do you use an outside consultant to review the fees charged by service providers to help ensure they aren't excessive, and if so what was their advice and did you follow it?
   C. Have you made any major changes to the number and nature of investment options or to your record keeper(s) in the last couple of years? If yes, please describe the current and prior record keepers and the reason(s) for making changes.
2. How many record keepers does the Plan have? If more than one, has the plan committee considered reducing the number of record keepers, and if so, what was the ultimate decision and why? Describe the process behind the decision.
3. On what basis do you compensate your record keepers (per capita, fixed/flat fee, revenue sharing, combination of assets under management/revenue sharing, or other)?
   A. Is there revenue sharing, and if so, how much is the revenue sharing and to whom is it paid and for what?
      i. Is the revenue sharing capped? If yes, please describe.
      ii. Is any surplus rebated to the plan? If yes, how is it disclosed? Please describe.
      iii. If no such caps or rebates have been negotiated, please explain the reason therefore.
   B. How much do you pay your record keepers when calculated on a per capita basis?
   C. Do you negotiate recordkeeping fees?
   D. Do you benchmark your recordkeeping fees in any way, and if so, how and what do you do with that information?

Excerpt from detailed 10 item questionnaire



EXCESSIVE FEE QUESTIONNAIRE

1. Describe the process your plan investment committee goes through in evaluating the reasonableness of service provider fees and in particular your record keeper(s).
   A. How frequently is the evaluation completed?
   B. Do you use an outside consultant to review the fees charged by service providers to help ensure they aren't excessive, and if so what was their advice and did you follow it?
   C. Have you made any major changes to the number and nature of investment options or to your record keeper(s) in the last couple of years? If yes, please describe the current and prior record keepers and the reason(s) for making changes.
2. How many record keepers does the Plan have? If more than one, has the plan committee considered reducing the number of record keepers, and if so, what was the ultimate decision and why? Describe the process behind the decision.
3. On what basis do you compensate your record keepers (per capita, fixed/flat fee, revenue sharing, combination of assets under management/revenue sharing, or other?
   A. Is there revenue sharing, and if so, how much is the revenue sharing and to whom is it paid and for what?
      i. Is the revenue sharing capped? If yes, please describe.
      ii. Is any surplus rebated to the plan? If yes, how is it disclosed? Please describe.
      iii. If no such caps or rebates have been negotiated, please explain the reason therefore.
   B. How much do you pay your record keepers when calculated on a per capita basis?
   C. Do you negotiate recordkeeping fees?
   D. Do you benchmark your recordkeeping fees in any way, and if so, how and what do you do with that information?
4. Do you RFP for your plan service providers and in particular your record keepers? If yes, how often and when was the last RFP? What actions did you take as a result of the last RFP and why?
   A. Were fee surveys requested by the fiduciaries during the RFP?
   B. What are the fees on a per-participant basis over each of the last six years? Please provide the breakout per year. For example: 2018: $X, 2019: $X, 2020: $X.
5. Describe the process your investment committee goes through in evaluating plan investment options, including the performance and expense of the investment options.
   A. How frequently is the evaluation completed?
   B. Describe how the options are selected. Describe your selection process for mutual funds.
   C. Who makes the selections? Is there a committee? If yes, please describe in detail.
   D. Do you use an outside consultant to review the investments to help ensure they are appropriate, and if so what was their advice and did you follow it?
6. How many investment plan options do you offer plan participants?
   A. Have you considered downsizing the amount of investment options available, and if so, describe?
   B. Do you document not just the decisions to retain or remove any investment option but the rationale behind any such decision as well?
   C. Do you provide options to invest in retail class shares of funds?
   D. Are there multiple investment options within a category of investment?
   E. Do you have a "default" investment option for when participants fail to make an investment election? If so, please describe.
   F. Describe the investment education that you provide to plan participants.
   G. Have you made any changes to the number of plan investment options or the plan fee structures in the past twelve months? If yes, please describe in detail.
7. Do you consider fees and expense ratios in selecting investment options?
   A. What are the expense ratios of your investment options and do you benchmark those expense ratios against comparable investments?
   B. Do you select and monitor all investment options or instead, do you provide some options on a platform that you do not purport to monitor (other than a true brokerage window)? Do you review your investments to ensure that you have the most cost effective share class (e.g. institutional versus retail; passive versus actively managed) as appropriate, and if so, describe.
   C. Does your plan offer any index funds as an investment option, and if not, please explain the rationale.
   D. Please confirm that the plan does not use any funds which are proprietary to an affiliate of the insured, the record keeper or the investment consultant. Otherwise, please describe the process used to ensure the independent evaluation of such investments.
8. Is your mutual fund provider also the plan trustee? If yes, are you considering changing that structure?
   A. If you use a consultant to help you select mutual funds for your plans, have you determined whether there are any fee or commission arrangements between the consultant and the recommended mutual fund provider?
   B. Are you comfortable that the investment fund provider and the consultant are completely independent?
   C. Is the investment fund provider or the consultant an affiliate of the insured?
      a) If yes, are proprietary fund options being used?
9. Please provide the number of individuals on your investment committee.
   A. What are the titles of each investment committee member?
   B. How long has each individual been on the investment committee?
   C. Does each individual have a finance background?
   D. Are they keeping minutes of their meetings?
   E. How often do they meet?
   F. Has the investment committee been provided fiduciary training?
      i. How was it provided to the committee?
      ii. When was the training last provided?
10. Please indicate if you have received or are aware of any inquiries or communications from any law firms, including Schlichter Bogard & Denton LLP, regarding plan fees and expenses or the performance of plan investments.
    A. Describe the communication, if any, and any follow-up to these matters.
    B. Are you aware of any online solicitation of your employees to contact a law firm about their employee benefit plan fees, expenses, or investments? If yes, please describe the details and any follow-up reviews to these matters.

DOL Begins random audits on cyber procedures

DC plan sponsors are receiving questionnaires to help spot possible fiduciary weaknesses:

1. What are the service provider's processes and systems for dealing with cyber security threats and protection of PII?
2. Is there a privacy and security policy, and does the policy apply to data held by benefit plans?
3. Is the policy clear with respect to storing PII on laptops and portable storage devices? What is that policy?
4. Is advanced authentication used? Can the service provider explain the process? Can the company explain it?
5. Are technology systems regularly updated?
6. Are all personnel who come in contact with PII trained on adequate protection of the information?
7. Does the service provider carry cyber security insurance?
8. Has the service provider experienced any security breaches?

Source: DOL – June 2021.

Participant defenses to protect your account

- ✓ Claim your online account
- ✓ Review account transactions
- ✓ Provide all contact information
- ✓ Always use multi-factor authentication, especially email
- ✓ Use password manager
- ✓ Freeze credit at all 3 bureaus
- ✓ Watch for mail delivery changes
- ✓ Change passwords frequently

Thank you!

Invesco

Disclosures

NOT A DEPOSIT | NOT FDIC-INSURED | NOT GUARANTEED BY THE BANK | MAY LOSE VALUE | NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY

The opinions expressed are those of the author, are based on current market conditions and are subject to change without notice. These opinions may differ from those of other Invesco investment professionals.

The information provided is general in nature and may not be relied upon nor considered to be the rendering of tax, legal, accounting or professional advice. Readers should consult with their own accountants, lawyers and/or other professionals for advice on their specific circumstances before taking any action.

This is not intended to be legal or tax advice or to offer a comprehensive resource for tax qualified retirement plans.

This does not constitute a recommendation of any investment strategy or product for a particular investor. Investors should consult a financial professional before making any investment decisions.

Invesco Distributors, Inc. is the US distributor for Invesco's Retail Products and Collective Trust Funds. Invesco Advisers, Inc. provides investment advisory services and does not sell securities. Both are indirect, wholly owned subsidiaries of Invesco Ltd.

Invesco.com/dcadvisors NA2080054 4/22