PROTECTING YOUR COMPANY AND PARTICIPANT INFORMATION FROM FRAUD

Identities are being stolen, financial assets are at risk

July 23, 2019

Eric Brickman - EVP, Global Technology and Digital Innovation
Scott Pollack - EVP, Client Services
Newport Group

How to Participate in this Webinar

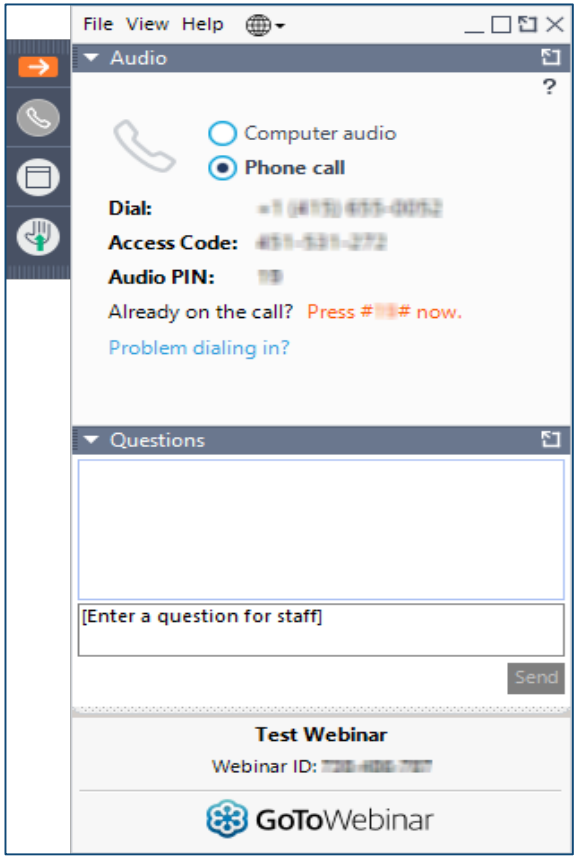
How to Listen: Choose *Computer Audio* to use your computer's speakers or *Phone Call* and dial in using the information provided

Ask Questions: Submit questions and comments via the *Questions* section of the main control panel

Learn More: Download additional materials via the *Handouts* section of the main control panel

Help Us Improve: Complete the brief survey at the end of today's webinar so we can incorporate your feedback in future events

Watch Again: A recording of this webinar will be available in the days ahead



PROTECTING YOUR COMPANY AND PARTICIPANT INFORMATION FROM FRAUD

Identities are being stolen, financial assets are at risk

July 23, 2019

Eric Brickman - EVP, Global Technology and Digital Innovation
Scott Pollack - EVP, Client Services
Newport Group

Quick Poll

Before we begin...

For a company to experience cyber fraud activity, it means there has been a security breach where the company's information system has been compromised?

A. True

B. False

Stay tuned for the results!

Agenda

Cybersecurity and Cyber Fraud: What's the difference?

- *The Role of Cybersecurity in the Retirement Industry*
- *Best-in-Class Information and Cybersecurity Framework*
- *Best-in-Class Cybersecurity Ecosystem*
- *Establishing Standard Industry Definitions*
- *Data Breaches in the News*
- *Personally Identifiable Information (PII)*
- *Comprehensive Fraud Prevention Architecture*
- *Key Components of Cyber Fraud Prevention*

Protocols and Considerations to Prevent Fraudulent Activity

- *What does fraud in the Retirement Industry look like*
- *Newport Group's Proactive Approach*
- *Consider these items in mitigating your risk*

Q&A

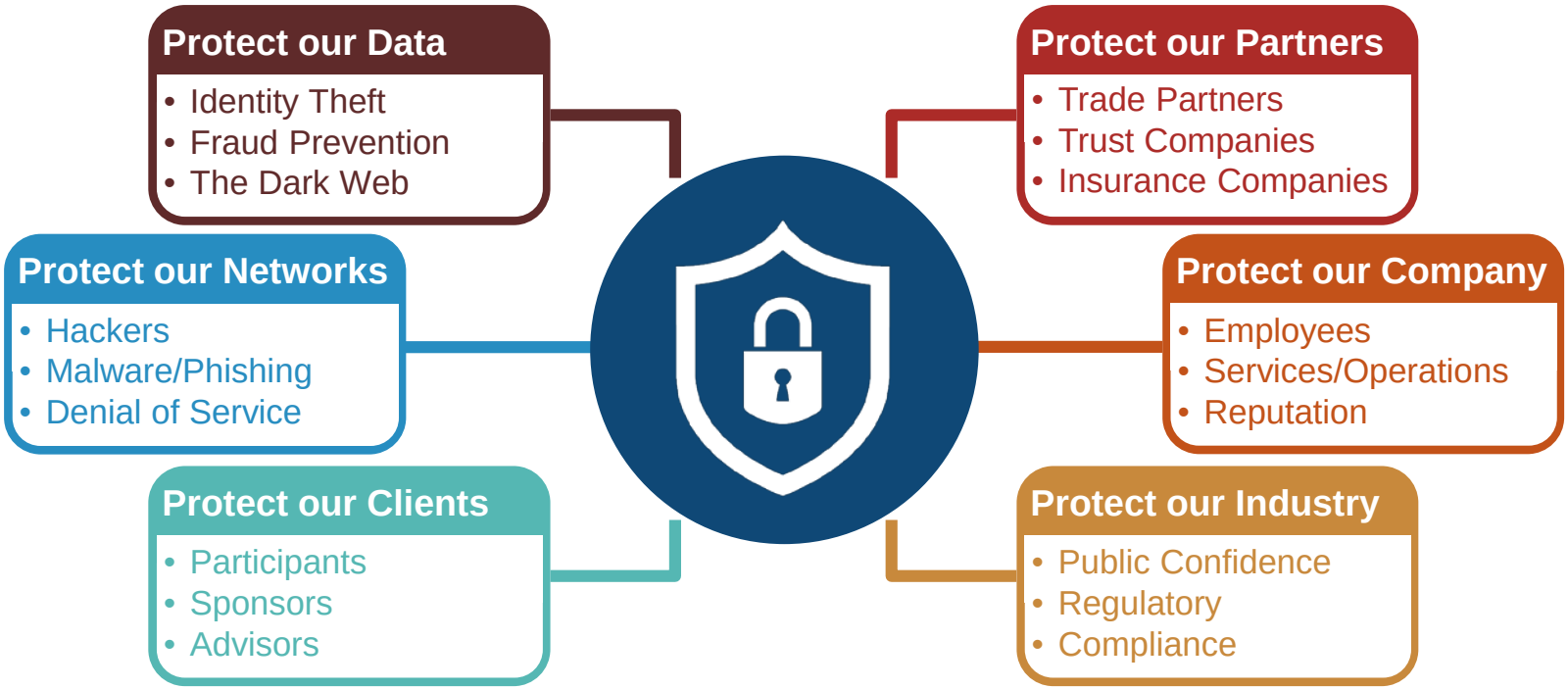
Cybersecurity and Cyber Fraud What is the difference?

Presented by:

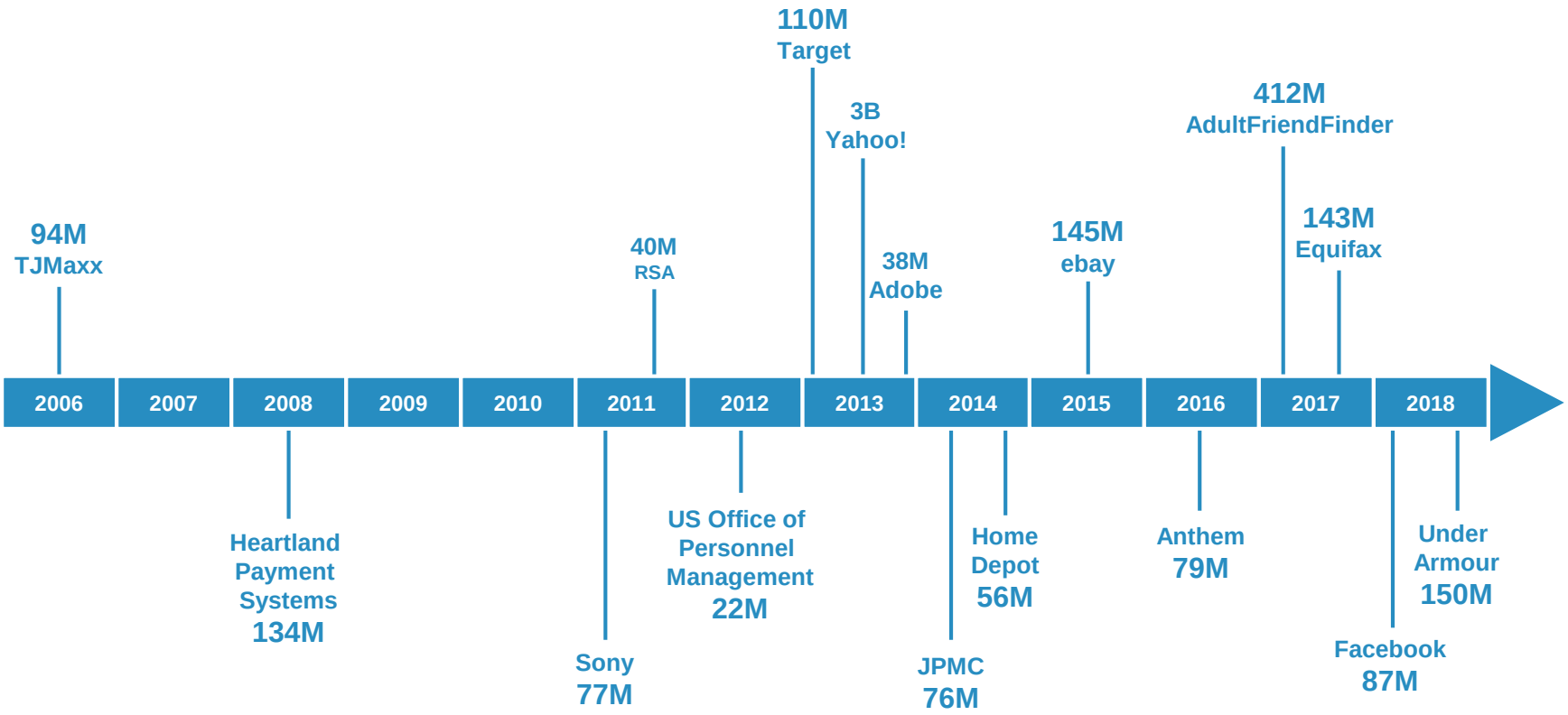
Eric Brickman – EVP, Global Technology and Digital Innovation
Newport Group

The Role of Cybersecurity in the Retirement Industry

Cybersecurity is an Integral Component of our Service-Oriented Industry



Data Breaches in the News



Total personal records exposed across these breaches alone = 4.7B

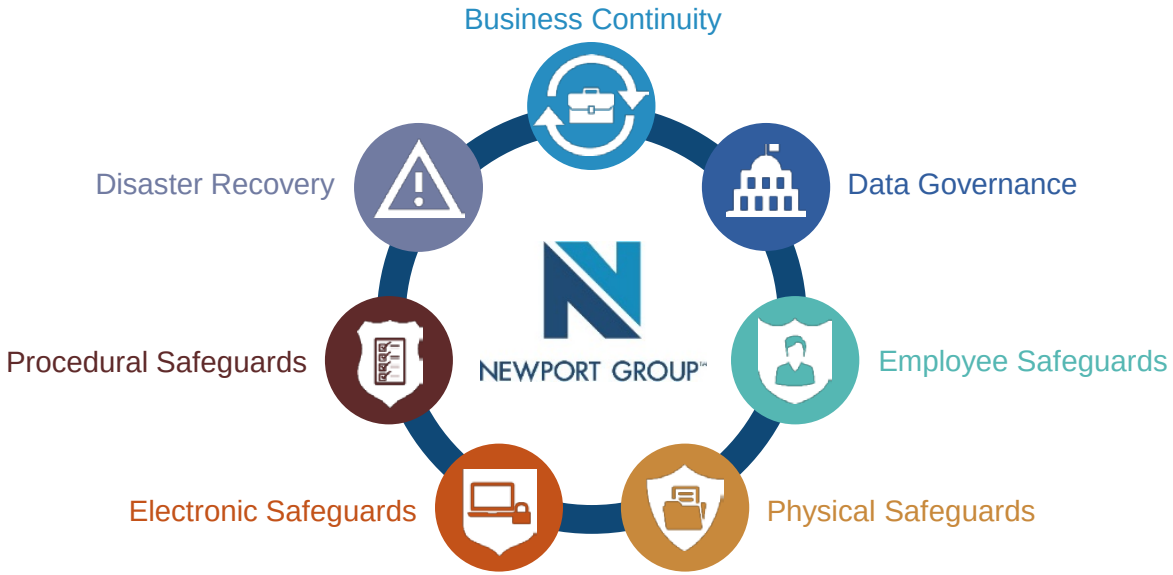
Source: CSOonline.com (IDG) 2018

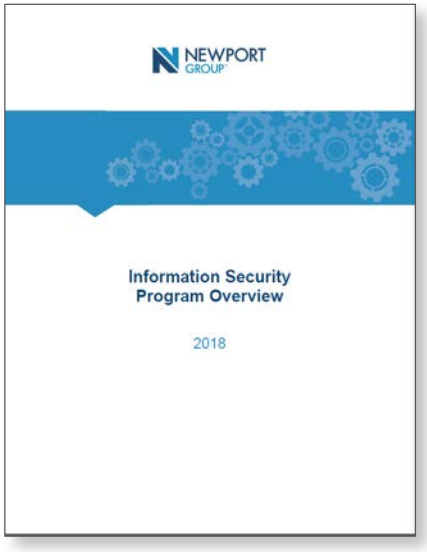
Personally Identifiable Information (PII)

- ERISA plan fiduciaries and service providers have a duty to protect the confidential personally identifiable information (PII) of plan participants and beneficiaries
- Fraudsters can use information illegally obtained in a data breach to gain access to plan sponsor and participant accounts.
- Examples include:
  - Social Security Number
  - Date Of Birth
  - Address
  - Username and password combinations

Best-in-Class Information and Cybersecurity Framework

Newport Group's Commitment to Information and Cybersecurity





Compliance

SOC-1 Audits for Internal Operations

NY DFS 23 NYCRR 500

Third Party Vulnerability Assessment and Penetration Test

Active Client Assessment Program

Mature IT Security and Governance Policy

SOC-2 Audits for Data Center Compliance

Best-in-Class Cybersecurity Ecosystem

The Standard for Anti-Hacking Coding Standards & Developer Training

WhiteHat SECURITY

3rd Party Auditor for Data & Network Security and Penetration Testing

e+

Global Leaders in Multi-Factor Authentication:

RSA ➡ Internal
Twilio ➡External

RSA

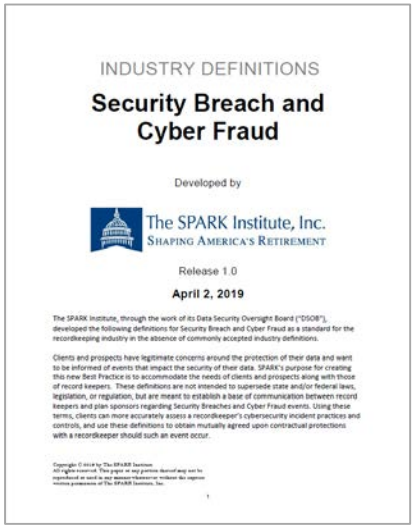
Mandatory Employee CyberSecurity Training & Phishing Testing

Global Leader in DDoS, WAF and Data Center Perimeter Protections

Global Leader in Managed Cybersecurity Monitoring Services, AI-Based Analytics and Alerts

Establishing Standard Industry Definitions

- **The SPARK Institute, Inc.**
- **Data Security Oversight Board**
- **Newport Group**



INDUSTRY DEFINITIONS

Security Breach and Cyber Fraud

Developed by

The SPARK Institute, Inc.
Shaping America's Retirement

Release 1.0

April 2, 2019

The SPARK Institute, through the work of its Data Security Oversight Board ("DSOB"), developed the following definitions for Security Breach and Cyber Fraud as a standard for the recordkeeping industry in the absence of commonly accepted industry definitions.

Clients and prospects have legitimate concerns around the protection of their data and want to be informed of events that impact the security of their data. SPARK's purpose for creating this new Best Practice is to accommodate the needs of clients and prospects along with those of record keepers. These definitions are not intended to supersede state and/or federal laws, legislation, or regulation, but are meant to establish a base of communication between record keepers and plan sponsors regarding Security Breaches and Cyber Fraud events. Using these terms, clients can more accurately assess a recordkeeper's cybersecurity incident practices and controls, and use these definitions to obtain mutually agreed upon contractual protections with a recordkeeper should such an event occur.

- **Security breach** is a confirmed compromise of a system or process
- **Cyber fraud & identity theft** are confirmed compromises of a participant account using data or processes.
- **Remember the poll question at the beginning of today's webinar? The answer was….**

Comprehensive Fraud Prevention Architecture

Helping to protect and secure our client data

- Enhanced Authentication Procedures:
  - Mandatory Two-Factor Authentication (2FA)
  - Mandatory Security Questions - *established by the participants*
  - Strong Password Requirements
  - Mobile Biometric Authentication (fingerprint)
  - Call Center Authentication Tools (call recordings, LexisNexis, etc.)
- Two-Tiered Firewall Protection (environment + database)
- Military-Grade Data Encryption (in transit + at rest)
- Access Logs & Audit Trails (all user types + proxy)
- IP Address Tracking & Cross Referencing
- Transaction + Address/eMail Change Confirmations
- AI-Based Fraud Protection (monitoring high-risk scenarios/activities)

And If I Never Sign In?

Failure to personalize your account may result in Newport Group asking you additional security questions over the phone to confirm your identity.

The questions may be personal in nature, like a former address, a city you've lived, or a car you've owned.

Protocols and Considerations to Prevent Fraudulent Activity

Presented by:

Scott Pollack – EVP, Client Services
Newport Group

What Does Fraud In the Retirement Industry Look Like?

A few examples:

- A fraudulent caller to the call center trying to access a participant account
- False distribution paperwork received from the participant
- Email received that looks like it is coming from a known plan sponsor or contact:
  - Fake distribution request
  - Fake email
- Fraudulent bank accounts established

Who is most at risk?

- Participants Age 59 ½ and older
- Terminated or retired employees
- Those who have never logged in (account set to defaults)
- High profile participants with public biographies
- Plan Sponsor and Plan Administrator listed on the 5500

Newport Group's Proactive Approach

Established Security Committee	• Committee is responsible for investigating reported fraud attempt occurrences
Continuously Updating Procedures	• Participant Service Center processes • Electronic payment protocols (wires / ACH transfers)
Internal Training	• Company-wide awareness training to all employees • Specific application training to operational and client service staff
Third Party Interaction	•Privacy Policy •Newport Group only uses participant information for the administration of client's plans.

Consider these items in mitigating your risk …

- Elimination of electronic payments
- Encouragement of participants to sign in to accounts and establish personal security settings
- Continue to protect sensitive data including— at rest data and secure email and data transfer
- Establishing internal protocols on steps to take should an incident arise

Questions?

Contact Us:
www.newportgroup.com

Notice of Confidentiality and Disclosure

The attached material was prepared by Newport Group. The format and substance of the material contained in this report were developed by and constitute the work product of Newport Group. This report is for informational and educational purposes only.

20190723-906981-2733499


NEWPORT
GROUP™