Shared Responsibility in Cybersecurity: Protecting Retirement Plans in the Digital Age

NAGDCA
2024 ANNUAL CONFERENCE
PHOENIX • SEPTEMBER 15 - 18

1

Speakers

Doug Peterson
Empower
Moderator

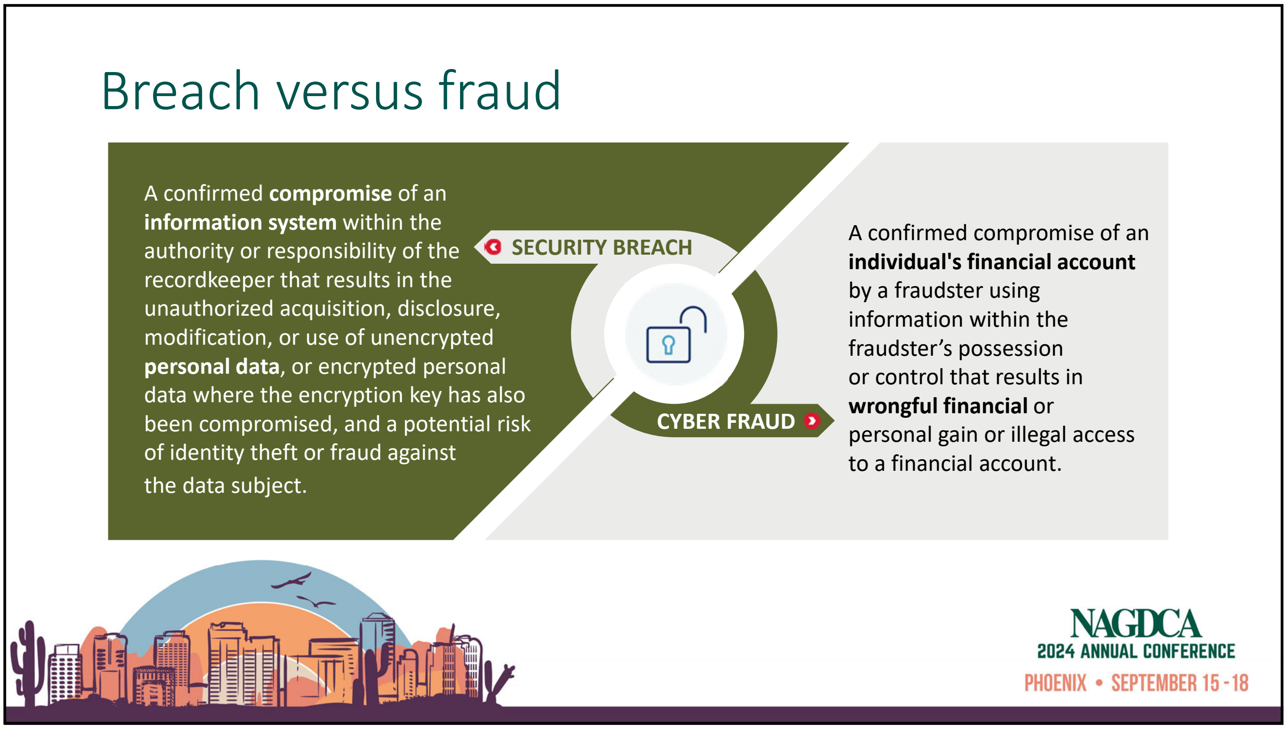
Duke Alden
Alight
Panelist

Robert Boehmer
Nevada Public Employees' Deferred Compensation Program
Panelist

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

2

2



Breach versus fraud

SECURITY BREACH

A confirmed **compromise** of an **information system** within the authority or responsibility of the recordkeeper that results in the unauthorized acquisition, disclosure, modification, or use of unencrypted **personal data**, or encrypted personal data where the encryption key has also been compromised, and a potential risk of identity theft or fraud against the data subject.

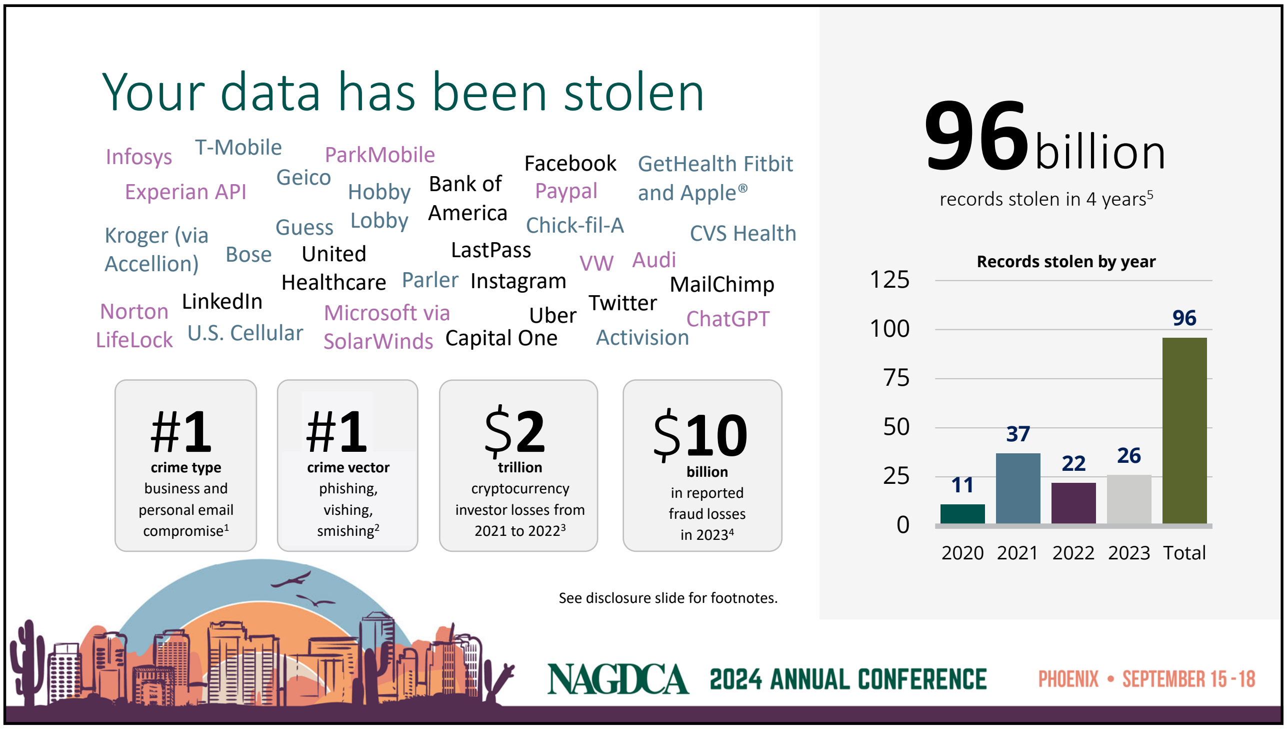
CYBER FRAUD

A confirmed compromise of an **individual's financial account** by a fraudster using information within the fraudster's possession or control that results in **wrongful financial** or personal gain or illegal access to a financial account.

NAGDCA 2024 ANNUAL CONFERENCE

PHOENIX • SEPTEMBER 15 - 18

3



Your data has been stolen

Infosys T-Mobile ParkMobile Geico Experian API Hobby Lobby Bank of America Facebook GetHealth Fitbit and Apple® Paypal Kroger (via Accellion) Guess Bose United Healthcare LastPass Chick-fil-A CVS Health VW Audi Parler Instagram MailChimp Norton LifeLock LinkedIn U.S. Cellular Microsoft via SolarWinds Capital One Uber Twitter Activision ChatGPT

#1 crime type
business and personal email compromise[1]

#1 crime vector
phishing, vishing, smishing[2]

$2 trillion
cryptocurrency investor losses from 2021 to 2022[3]

$10 billion
in reported fraud losses in 2023[4]

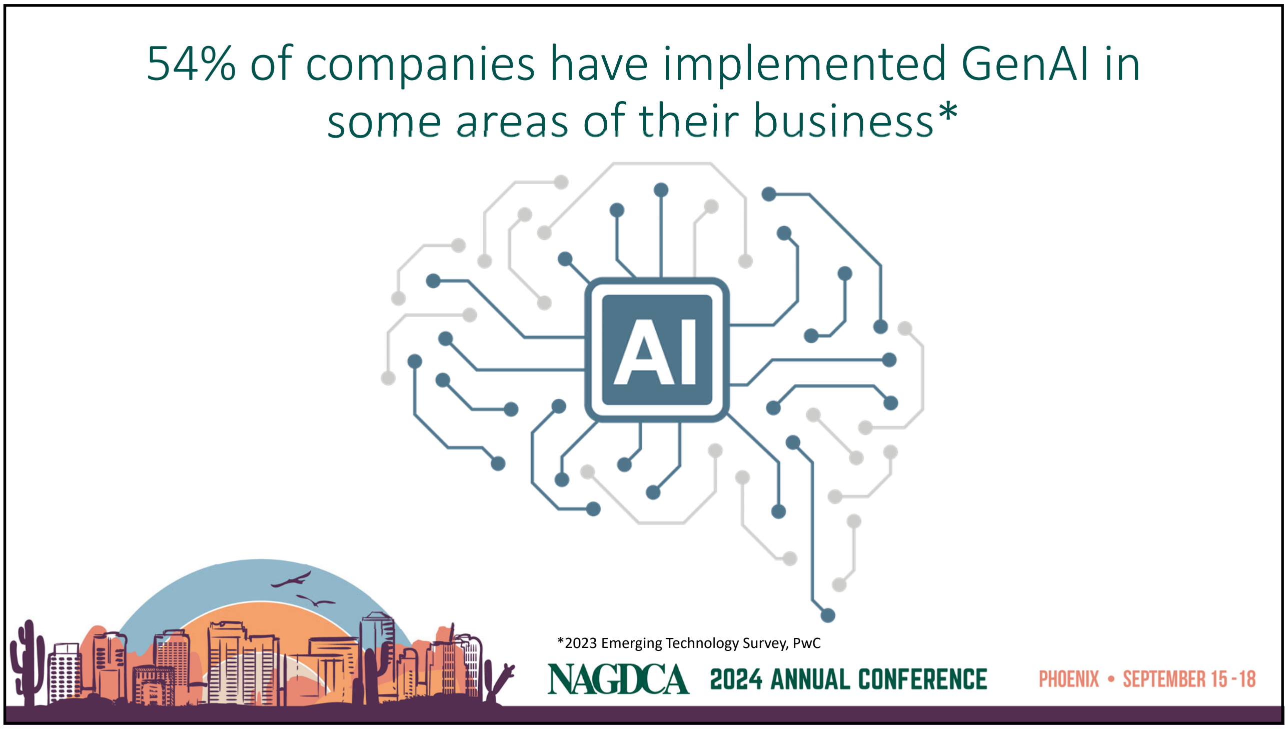
See disclosure slide for footnotes.

96 billion
records stolen in 4 years[5]

Records stolen by year

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

4

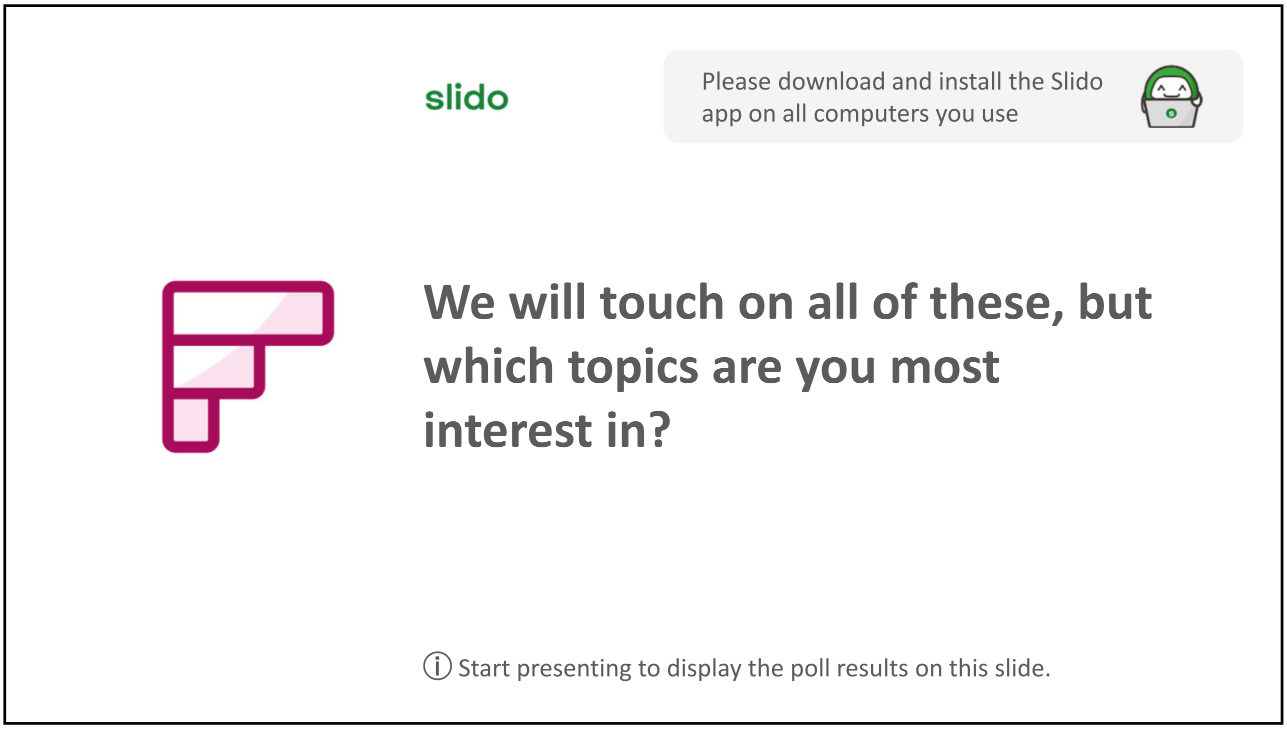


54% of companies have implemented GenAI in some areas of their business*

*2023 Emerging Technology Survey, PwC

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

5



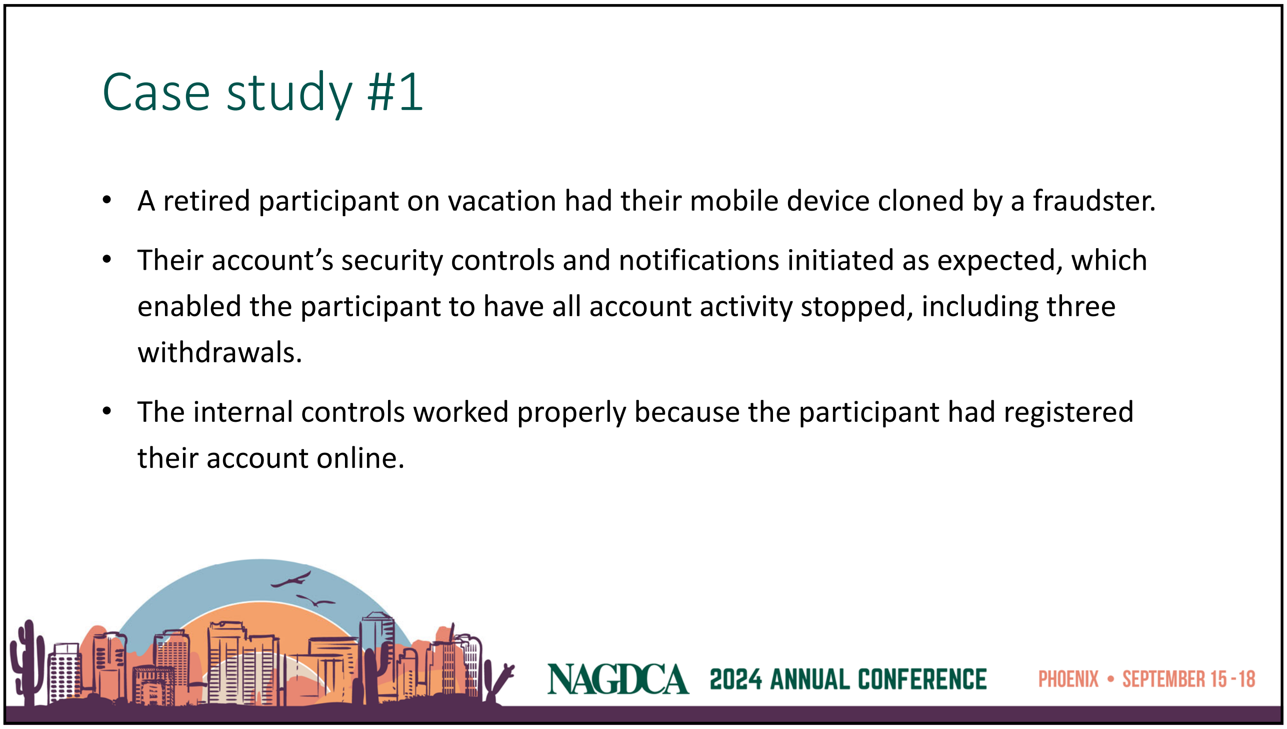
slido

Please download and install the Slido app on all computers you use

We will touch on all of these, but which topics are you most interest in?

ⓘ Start presenting to display the poll results on this slide.

6

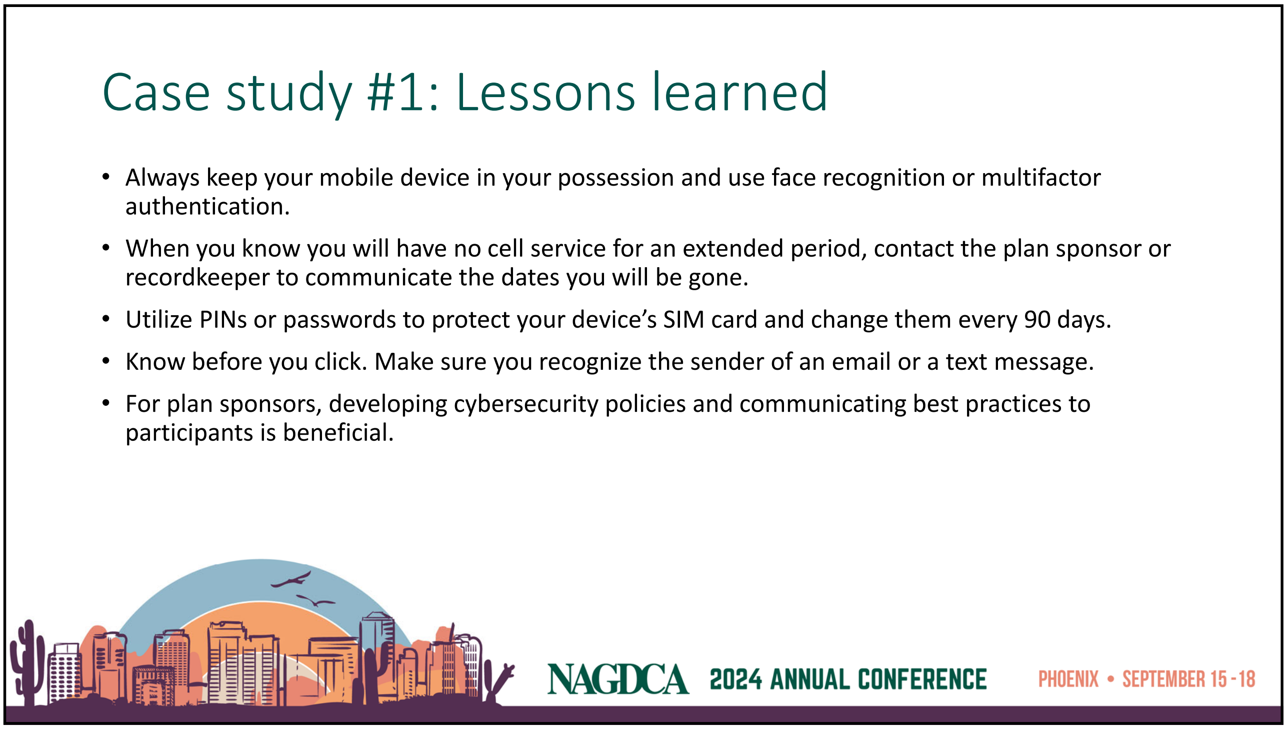


Case study #1

- A retired participant on vacation had their mobile device cloned by a fraudster.
- Their account's security controls and notifications initiated as expected, which enabled the participant to have all account activity stopped, including three withdrawals.
- The internal controls worked properly because the participant had registered their account online.

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

7

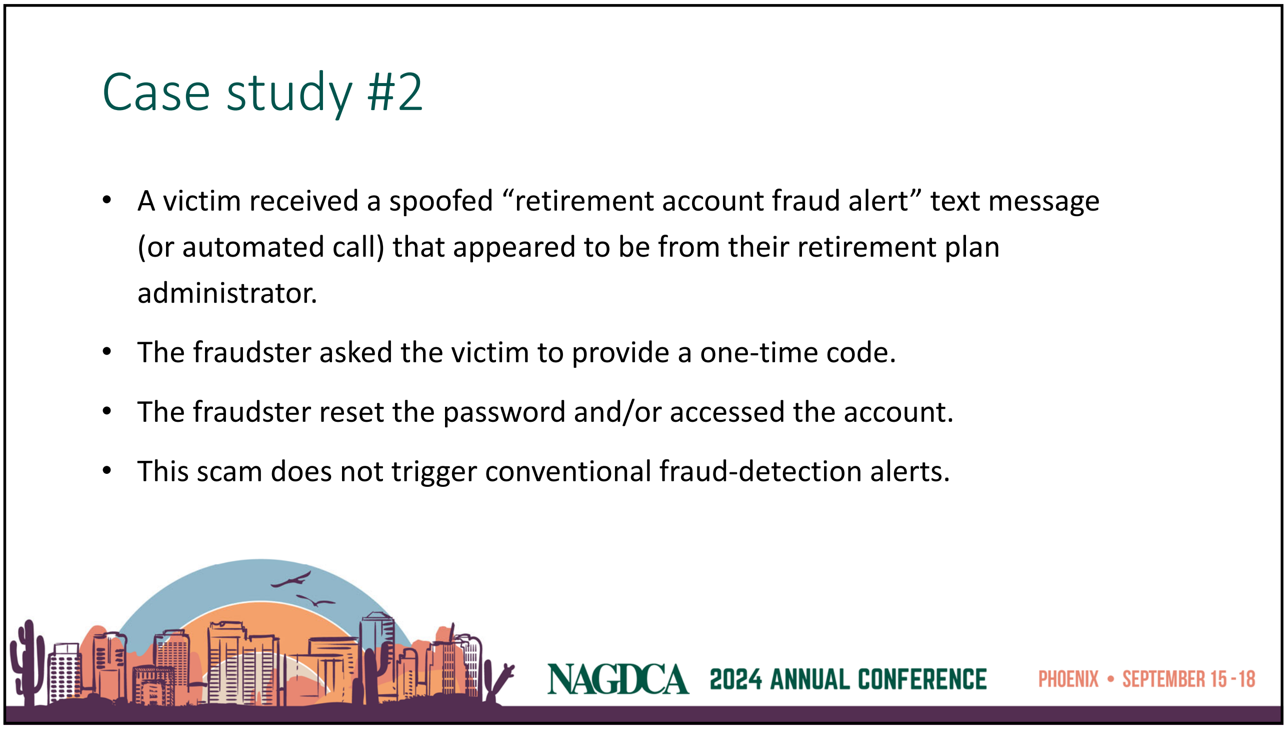


Case study #1: Lessons learned

- Always keep your mobile device in your possession and use face recognition or multifactor authentication.
- When you know you will have no cell service for an extended period, contact the plan sponsor or recordkeeper to communicate the dates you will be gone.
- Utilize PINs or passwords to protect your device's SIM card and change them every 90 days.
- Know before you click. Make sure you recognize the sender of an email or a text message.
- For plan sponsors, developing cybersecurity policies and communicating best practices to participants is beneficial.

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

8

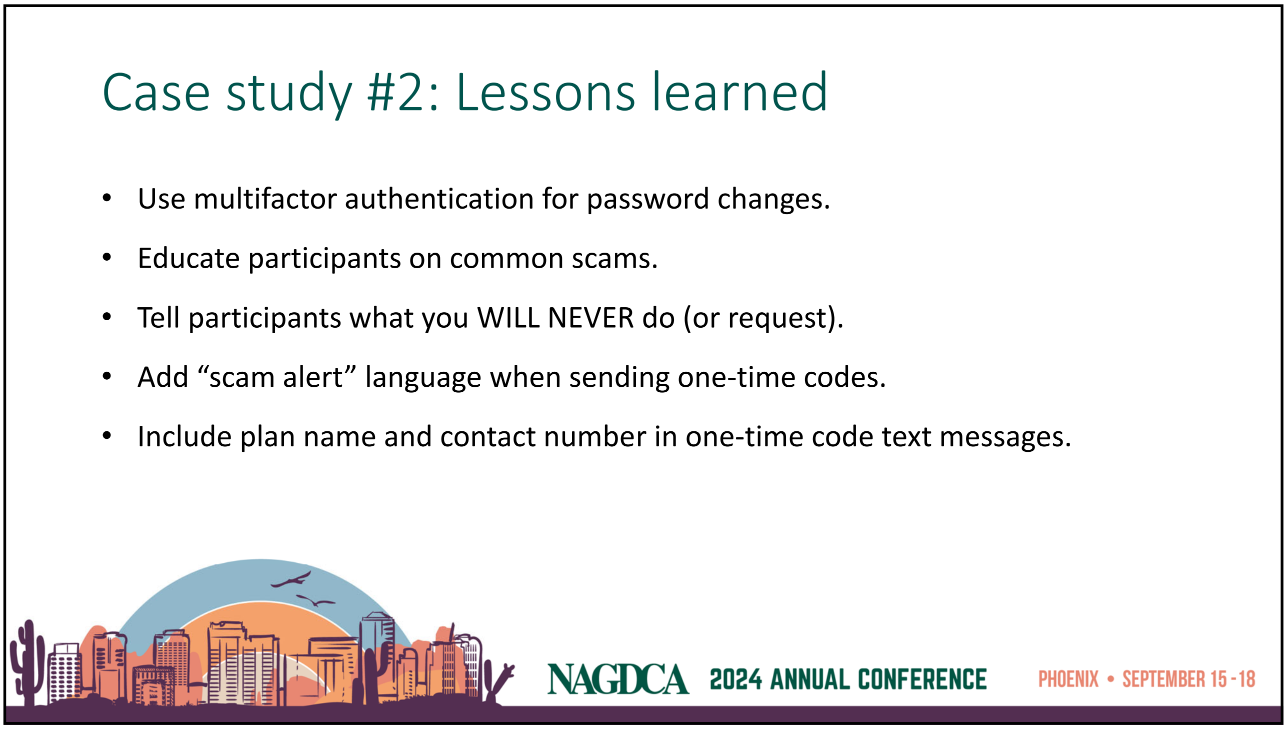


Case study #2

- A victim received a spoofed “retirement account fraud alert” text message (or automated call) that appeared to be from their retirement plan administrator.
- The fraudster asked the victim to provide a one-time code.
- The fraudster reset the password and/or accessed the account.
- This scam does not trigger conventional fraud-detection alerts.

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

9

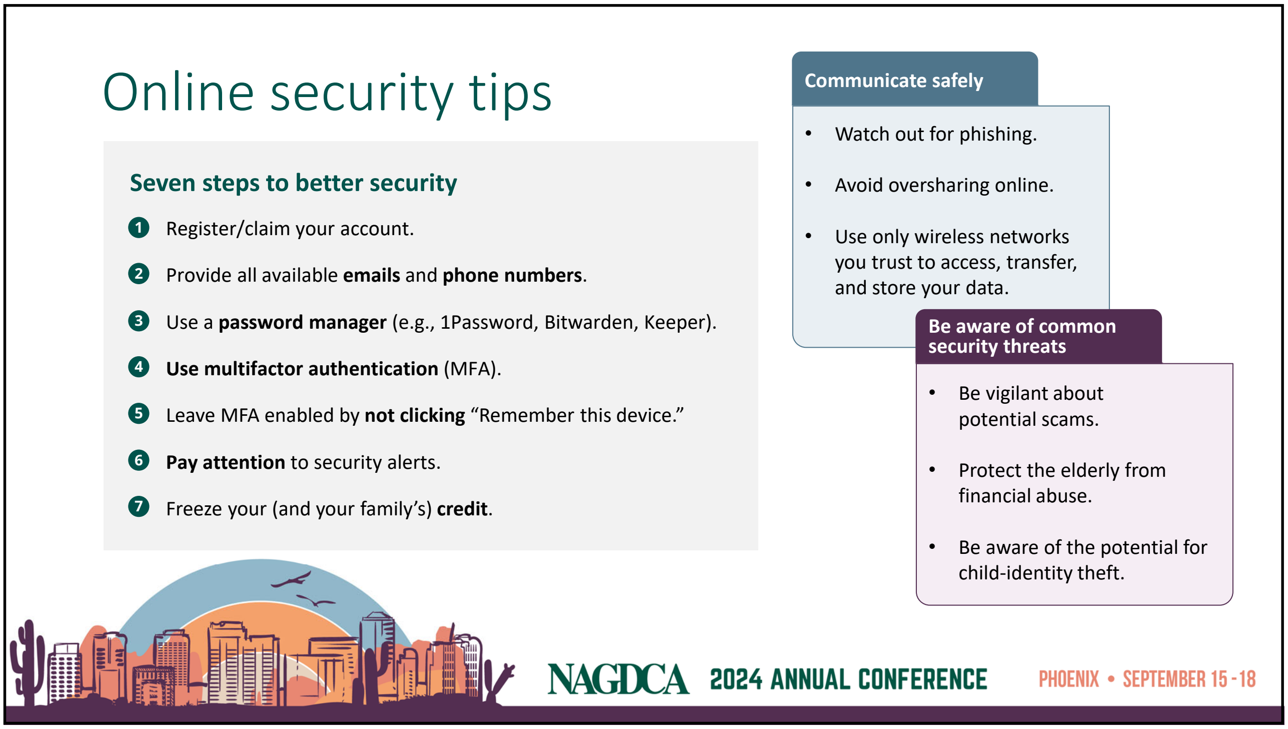


Case study #2: Lessons learned

- Use multifactor authentication for password changes.
- Educate participants on common scams.
- Tell participants what you WILL NEVER do (or request).
- Add “scam alert” language when sending one-time codes.
- Include plan name and contact number in one-time code text messages.

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

10



Online security tips

Seven steps to better security

1. Register/claim your account.
2. Provide all available **emails** and **phone numbers**.
3. Use a **password manager** (e.g., 1Password, Bitwarden, Keeper).
4. **Use multifactor authentication** (MFA).
5. Leave MFA enabled by **not clicking** "Remember this device."
6. **Pay attention** to security alerts.
7. Freeze your (and your family's) **credit**.

Communicate safely

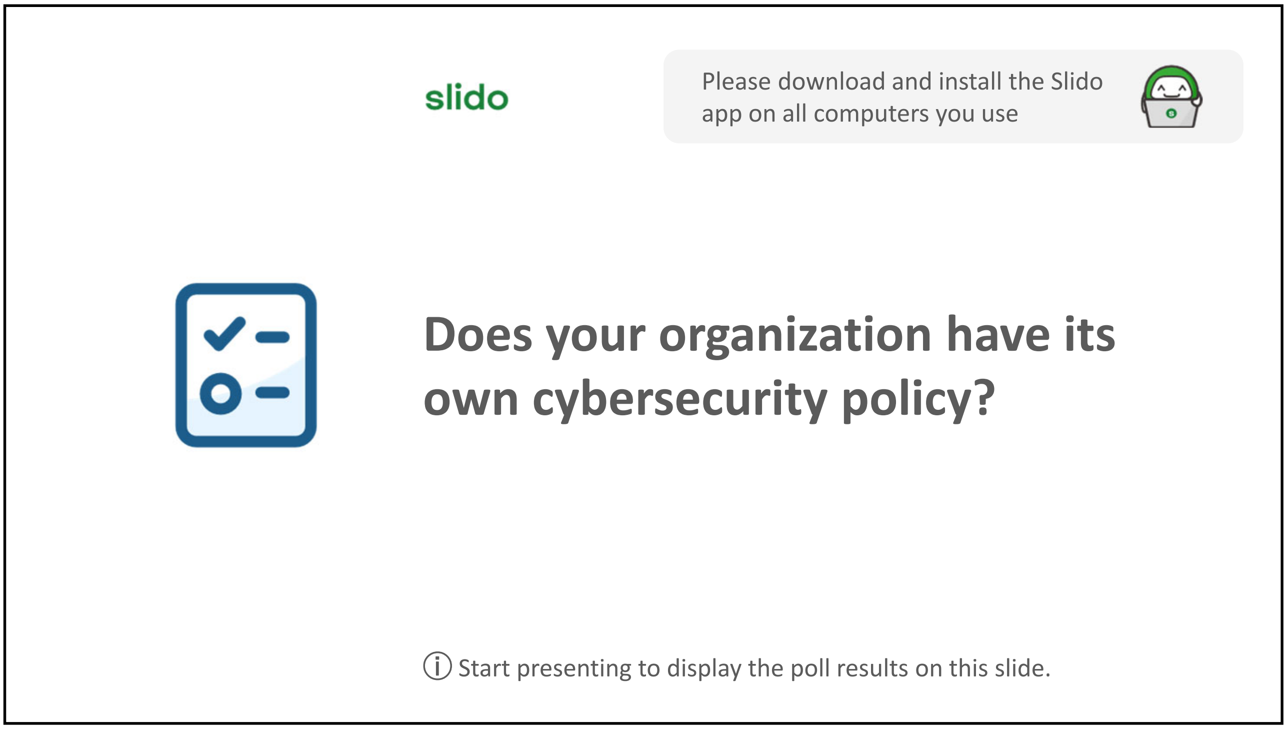
- Watch out for phishing.
- Avoid oversharing online.
- Use only wireless networks you trust to access, transfer, and store your data.

Be aware of common security threats

- Be vigilant about potential scams.
- Protect the elderly from financial abuse.
- Be aware of the potential for child-identity theft.

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

11



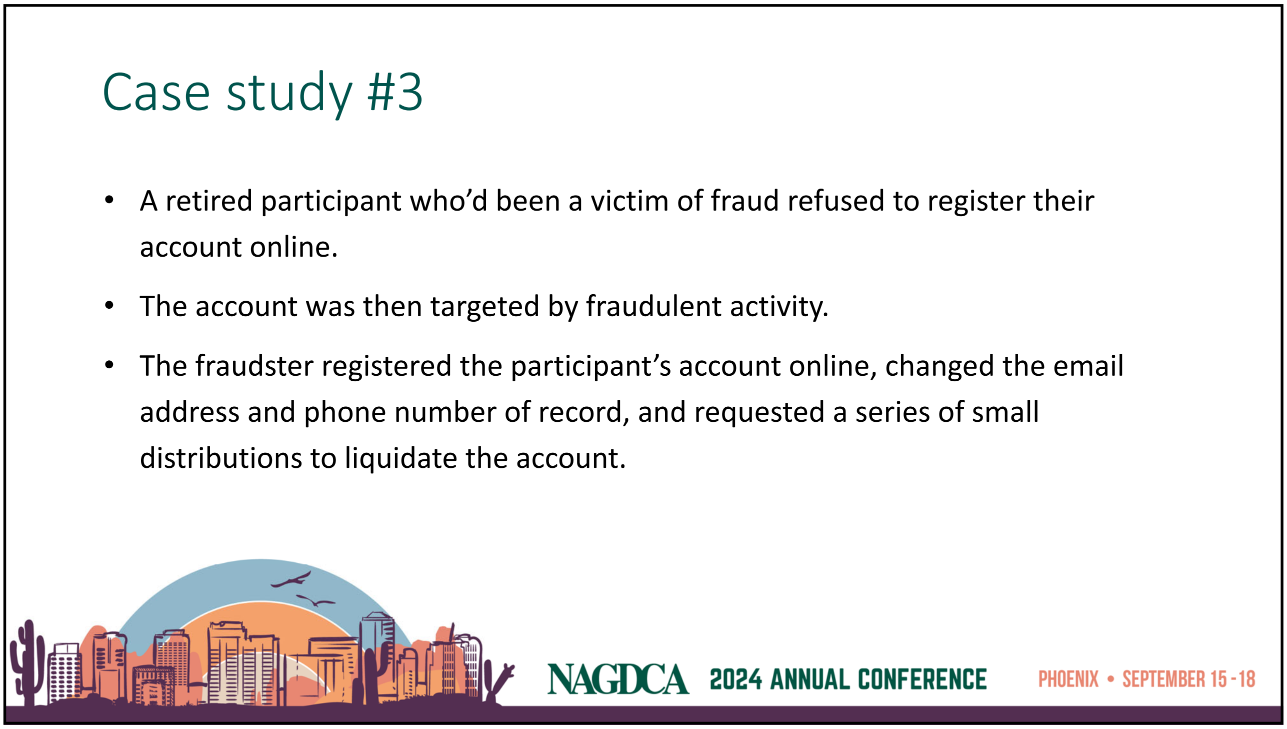
slido

Please download and install the Slido app on all computers you use

Does your organization have its own cybersecurity policy?

ⓘ Start presenting to display the poll results on this slide.

12

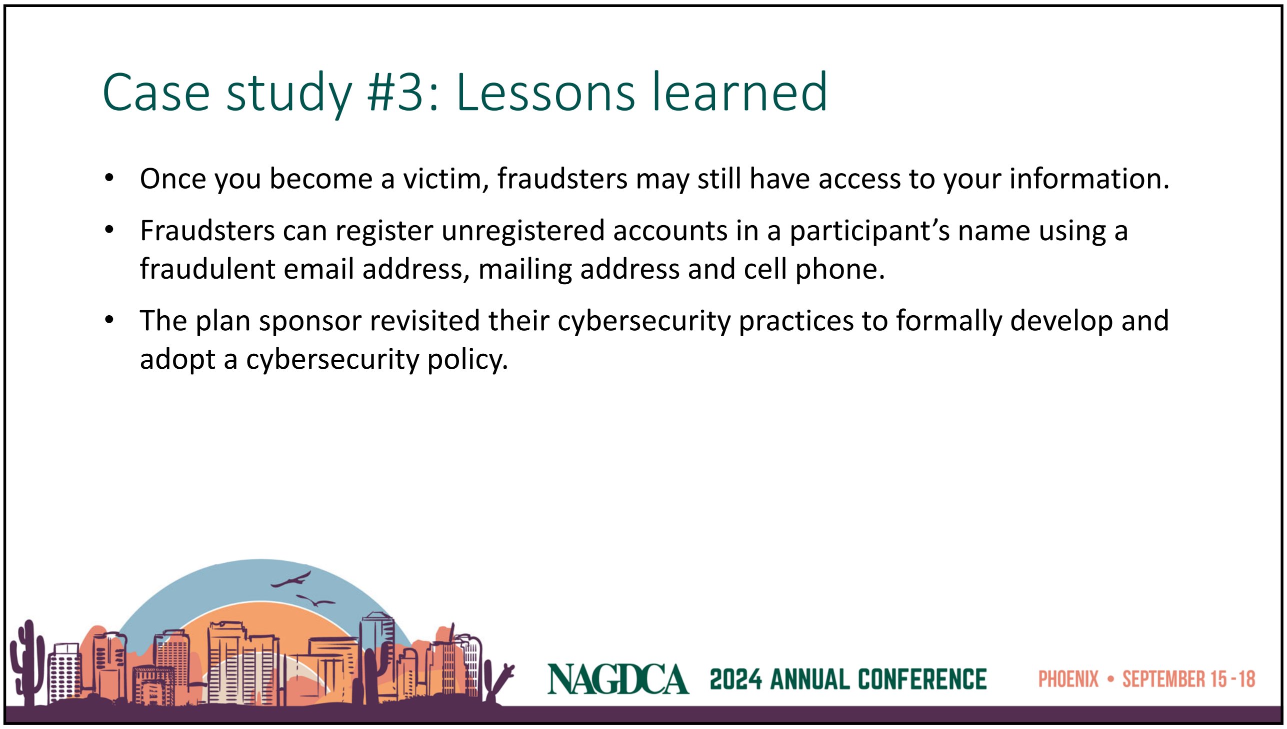


Case study #3

- A retired participant who'd been a victim of fraud refused to register their account online.
- The account was then targeted by fraudulent activity.
- The fraudster registered the participant's account online, changed the email address and phone number of record, and requested a series of small distributions to liquidate the account.

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

13



Case study #3: Lessons learned

- Once you become a victim, fraudsters may still have access to your information.
- Fraudsters can register unregistered accounts in a participant's name using a fraudulent email address, mailing address and cell phone.
- The plan sponsor revisited their cybersecurity practices to formally develop and adopt a cybersecurity policy.

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

14

Creating and adopting a cybersecurity policy

Components to consider:

- Purpose
- Key definitions
- Account security tips and guidance
- Minimum requirements
- Recordkeeper cyber policies and procedures
- Cybersecurity incident response
- Internal controls to evaluate and audit the existing policy: This includes reviewing quarterly reports, conducting vulnerability and penetration testing, reviewing the recordkeeper’s SOC1 Report, and utilizing MFA and unique non-SSN login IDs.
- Reports and checklists needed to manage an incident or threat
- Coordinated requirements across your recordkeeper, investment consultant, internal risk management, and IT support/information security officer (ISO): Gather input to support creating, executing, managing, testing, and amending the cybersecurity policy.

Current scams to watch out for

Romance scams: Scammers create fake online profiles and attempt to build phony emotional attachments until a potential victim is comfortable sending them money. (Now also featuring AI chatbots!)

Employment scams: Scammers collect your personal information from your employment forms or tell you to buy equipment or training.

Cryptocurrency scams: Criminals lure victims to download fraudulent investing apps while building trust and convincing them to invest in cryptocurrency platforms. The fraudsters control the platforms and eventually take all the money and vanish.

Voiceprint scams: Thieves capture a recording of your voice and use a software program to generate an imitation “deepfake” version that can be used to impersonate you.

Questions?

1. In the conference app, select this session from the schedule.
2. Select "External QA/Survey."
3. Type your question and tap send.

CONTINUING EDUCATION CODE:

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

17

Disclosures

1 Federal Bureau of Investigation – Internet Crime Complaint Center Releases 2022 Statistics — FBI
2 2021_IC3Report.pdf.
3 $2 trillion: SEC Warns Investors Crypto Assets Are at Risk of 'Significant' Losses (businessinsider.com). March 2023.
4 Federal Trade Commission: As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public | Federal Trade Commission, February 2024
5 IT Governance UK 2020; Risk-Based Security, "New Research: No. of Records Exposed Increased 141% in 2020," 2021, and "Data Breach Report: 2021 Year End," 2022. 2024 Statista number of data breaches worldwide.

Empower Retirement, LLC and its affiliates are not affiliated with Duke, Alight, Robert Boehmer or Nevada Public Employees' Deferred Compensation Program and are not responsible for the third-party content provided.

Empower refers to the products and services offered by Empower Annuity Insurance Company of America and its subsidiaries. This material is for informational purposes only and is not intended to provide investment, legal, or tax recommendations or advice.

"EMPOWER" and all associated logos and product names are trademarks of Empower Annuity Insurance Company of America.

WSA-EEV-WF-3584216-0924 RO3821004-0924

NAGDCA 2024 ANNUAL CONFERENCE PHOENIX • SEPTEMBER 15 - 18

18