• Largest retirement system in Iowa
• $32 billion trust fund
• 355,000 total members
• 117,000 retirees
  – Over 95 percent use direct deposit
• Annual payroll is $2 billion
Our pension system software features an online portal called *My Account*

*My Account* allows members to make updates to contact information, direct deposit information and view other information
By definition, IPERS was not “hacked”

- Criminals possessed Social Security numbers, date of birth records, etc.
- This allowed them to establish an online account via the My Account portal
- Once established, email, street address, bank information was changed
IPERS’ cyber attack is *not* considered a data breach.

- Personally identifiable information (PII) was not obtained from IPERS
- Criminals stole PII from outside source
  - Such as Equifax
- Stolen information used to take over accounts
- Considered an “account takeover”
Situation Unfolds

Morning of October 31, 2017

- IPERS receives a phone call from a member reporting that his monthly check was not deposited

- System shows member changed financial institutions two weeks earlier on October 18

- Member denies that he made the change
Immediate Investigation

System check reveals that up to 115 accounts had changes to direct deposit information

- Later confirmed that 103 accounts were hijacked
- The fraudsters changed the contact information after establishing the accounts to prevent the members from receiving communications about changes from IPERS
The criminals were able to change the member’s:

- Email address
- Phone number
- Street address
- Bank account
The bank account information for direct deposit changed, redirecting the funds

- New bank accounts were then accessible only to the criminals
  - Each fraudulent bank account number was unique
- Funds were drained immediately after the benefit payment was deposit
Authorities Contacted

Immediately, IPERS notified:

- FBI
- Iowa Dept. of Criminal Investigation
- OCIO
- Attorney General
Affected members

- Contacted by phone within 8 hours
- Within 24 hours, accounts were restored and payments in process
- Encouraged to monitor all accounts

Involved banks and credit unions

- IPERS has recovered some of the stolen funds
IPERS got out in front of the story:

- Alert posted on website and social media
- CEO interviewed with local news station
- Talking points published by various media
- Updates provided on our website
• Educating the public on “account takeover” vs. data breach
• Helping members understand how to protect their IPERS account
• Owning the problem; not passing the buck
Talking Points Published

• Today IPERS learned that some retiree accounts were compromised on October 18 through the online member self-service.

• Hackers had your social security number and your birth date and were able to change your direct deposit account information, redirecting IPERS to deposit the monthly benefit payments to a different financial institution.

• Right now, IPERS is working to reverse these deposits and get the payments to their rightful owners.

• The Department of Criminal Investigation has been notified and IPERS intends to pursue full prosecution against the criminals.
Subsequent Steps

1. Online account access was removed until the scope of the incident was determined.

2. Removed the ability to change direct deposit information through online access.

3. Option to use Social Security number for online access was removed.
4. IPERS improved its internal review of activity on the online access and monitors all returned emails.

5. IPERS now requires notifications of address changes to be sent to member's new address and old address.
Going Forward

• **Two-factor authentication**
  • To launch with pension system upgrade by the end of 2018

• **Enhanced authentication step**
  • Currently evaluating for those actions with the greatest risk for fraud
Current messaging to members:

• Avoid account takeover by establishing access to My Account

In the coming months:

• Targeted mail campaign to members
  • IPERS to provide new credentials
  • Opt out is available

• New members will be directed to name a beneficiary using My Account
• Transparency in government is important, but it cannot come at the expense of compromising citizens’ personally identifiable information.

• State government websites publish names, addresses, salaries, taxes, etc. that can be downloaded and cross-referenced with data stolen from other security breaches.

• Steps should be taken to eliminate this exposure.
For additional information:

Judy Akre, Director of Communications
judy.akre@ipers.org

Rick Hindman, Chief Information Officer
rick.hindman@ipers.org

800-622-3849    www.ipers.org