An Inconvenient Truth:

Payments fraud and cyberattacks rising at alarming rates in the public sector

Your presenter

Lynn is a member of Wells Fargo's Treasury Management & Payments Solution team, responsible for providing customized treasury consulting to government entities in Central, West Central, Panhandle and North Florida regions, including the State of Florida and its various agencies throughout the State. She is dedicated to helping these organizations implement and maintain efficient and cost-effective cash management programs while also keeping them abreast of new and enhanced treasury services and trends.

She has worked in Treasury Management serving government clients for over 23 years, and joined Wells Fargo in mid-2008 after 12 years at Bank of America.

Lynn has a B.S. in Marketing and a Masters in Business Administration from the University of Central Florida. She has been designated a Certified Treasury Professional (CTP) by the Association of Financial Professionals (AFP) and is a member of the Florida Government Finance Officers Association (FGFOA).

Lynn resides in Wesley Chapel with her husband Carlos and their two adorable basset hounds, Minnie Precious and Daisy Sunshine.

Lynn Nieves, MBA, CTP

Senior Vice President

Treasury Management & Payment Solutions

Government Banking

Public sector threat landscape

By the numbers

"Agencies currently fail to comply with basic cybersecurity standards."

— U.S. Senate report, 2019[1]

Email-based threats remain prevalent with email/phishing continuing to be a highly-targeted attack vector[2]

Cyber incidents reported by federal agencies from 2006 – 2015

↑1300%

Cyber incidents reported by federal agencies in 2017

35,277[1]

Public sector breaches are

>2.5x more likely

to be undiscovered **for years**[3]

50+

# of cities and towns suffering ransomware attacks in 2019 to date[4]

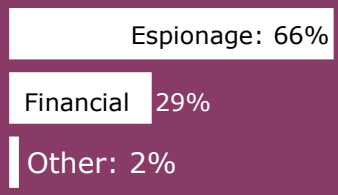
22+ million

# of security clearance files ex-filtrated from the Office of Personnel Management (2015)[1]

Cyber espionage

is rampant in the public sector

Actor motives



79% of all external breaches involve State-affiliated actors[4]

Sources:

[1]U.S. Senate, *Federal cybersecurity: America's data at risk* (June 2019), https://www.hsgac.senate.gov/imo/media/doc/2019-06-25%20PSI%20Staff%20Report%20-%20Federal%20Cybersecurity%20Updated.pdf

[2]FISMA, *Annual report to Congress* (2018), https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf

[3]Verizon's *2019 Data Breach Report*, https://enterprise.verizon.com/resources/reports/dbir/2019/public-administration/

[4]Barracuda Networks, *Threat spotlight: Government ransomware attacks*, https://blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/

Imagine for a moment that you receive a call from one of your direct reports. The general contractor for a large project called inquiring about a substantial payment they were expecting last month.

Your team conducts research and confirms the payment was made by ACH three weeks ago. It’s also discovered that a few weeks prior, the vendor requested to change the destination bank account.

Now imagine the next phone call you have to make...

Who would you call?

What would you say?

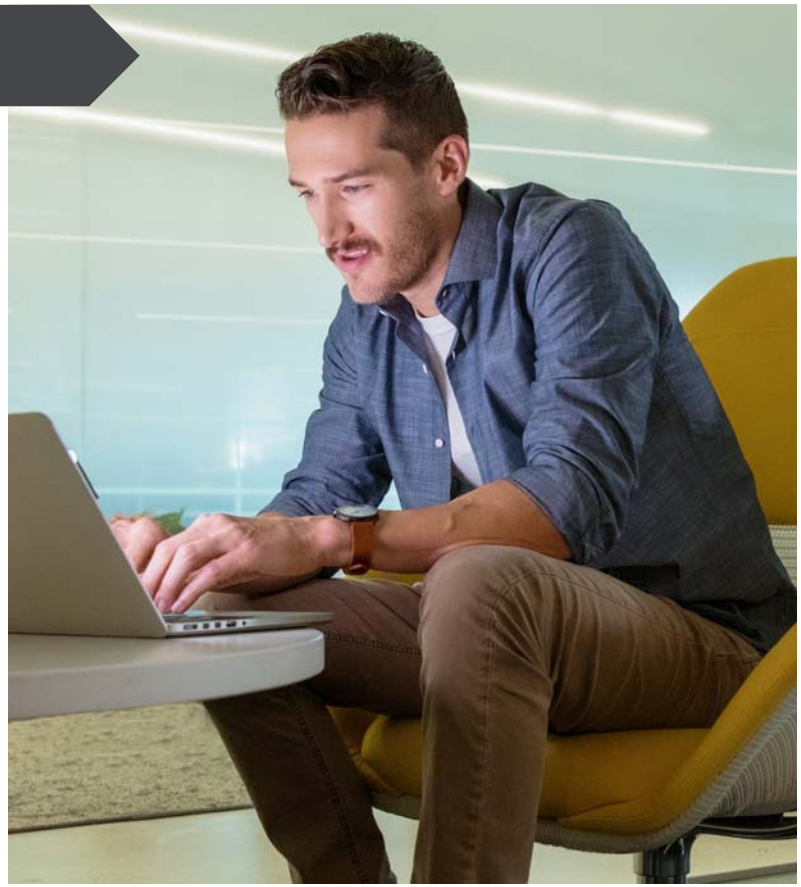
What questions might **they ask**?

Important questions to ask yourself

Face it…you are a target

Fraudsters are actively…

- Taking advantage of the public sector by leveraging government transparency to commit fraud
- Monitoring government entity board meeting minutes and looking for large upcoming vendor payments being discussed/disclosed (often construction vendors)
- Following governmental entities' process and submitting the required forms to conduct change of payment method



Ransomware

Attacks happen regardless of size

In the first nine months of 2019, at least 621 government entities, healthcare service providers and school districts, colleges and universities were affected by ransomware

Source: *State of Ransomware in the U.S.: 2019 Report for Q1 to Q3*, Emsisoft

Business email compromise (BEC)

BEC continues to hinder companies

80%

Companies impacted by Business email compromise **increased to 80% in 2018**

Source: 2019 AFP Payments Fraud and Control Survey report

An inconvenient truth

"As more than 90 percent of targeted attacks start with email, it is critical that federal agencies consider their employees as their last line of defense and craft a **security strategy** that **prioritizes training users on how to spot and report malicious emails.**"[1]

Bhagwat Swaroop, EVP
Proofpoint

Because most municipalities don't have millions to spend on cybersecurity the way big corporations do, they can be easy prey. 1:4 will fall to ransomware.[2]

Lou Romero
Cybersecurity expert

1. "Cybersecurity Training for Government Moves Up the FedRAMP," Government Technology website, https://www.govtech.com/biz/Cybersecurity-Training-for-Government-Moves-Up-the-FedRAMP.html ,accessed December 13, 2019
2. Michaelle Bond, "Ransomware attacks are hitting local governments. Here's how they can fight back.", *The Philadelphia Inquirer*, September 9, 2019

Fraud is on the rise

1,300%

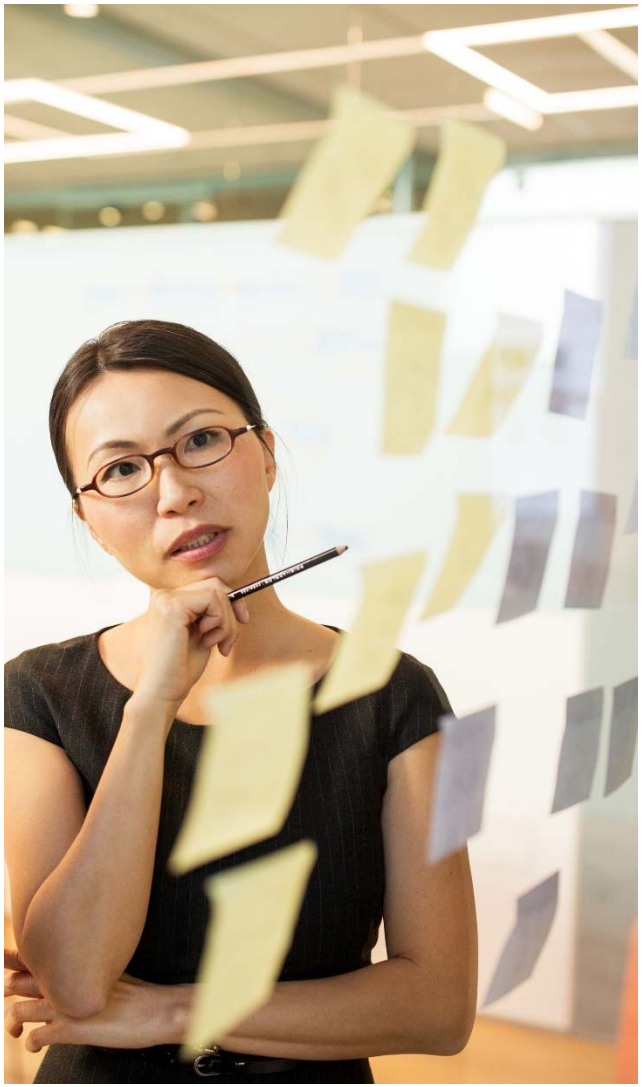
jump in email scams in the space of **one year**[1]

82%

of organizations were targets of payment fraud in 2018[2]

Who is held responsible for financial losses stemming from a breach?

1. Federal Bureau of Investigation, "Cyber-Enabled Financial Fraud on the Rise Globally," 2017
2. 2019 AFP Fraud and Control Survey report



Whose job is it anyway?

IT

Accounting

Treasury

Controller

Risk


Where are you positioned now?
Where do you want to be?

“

That’s been one of my mantras – focus and simplicity. Simple can be harder than complex: You have to work hard to get your thinking clean to make it simple.

- *Steve Jobs*

”

Essential elements of an effective strategy

You have an opportunity...


Align your vision
Collaborate
with key disbursement functions of your organization

Preparation guide

1. Policy and procedures

Do you have policy and procedural documentation that specifically addresses payment changes?

- Is it specific?
- Is it published and understandable?
- How are employees trained?
- Does it include an audit procedure?

2. Validation recommendations

These are tailored based on your organization

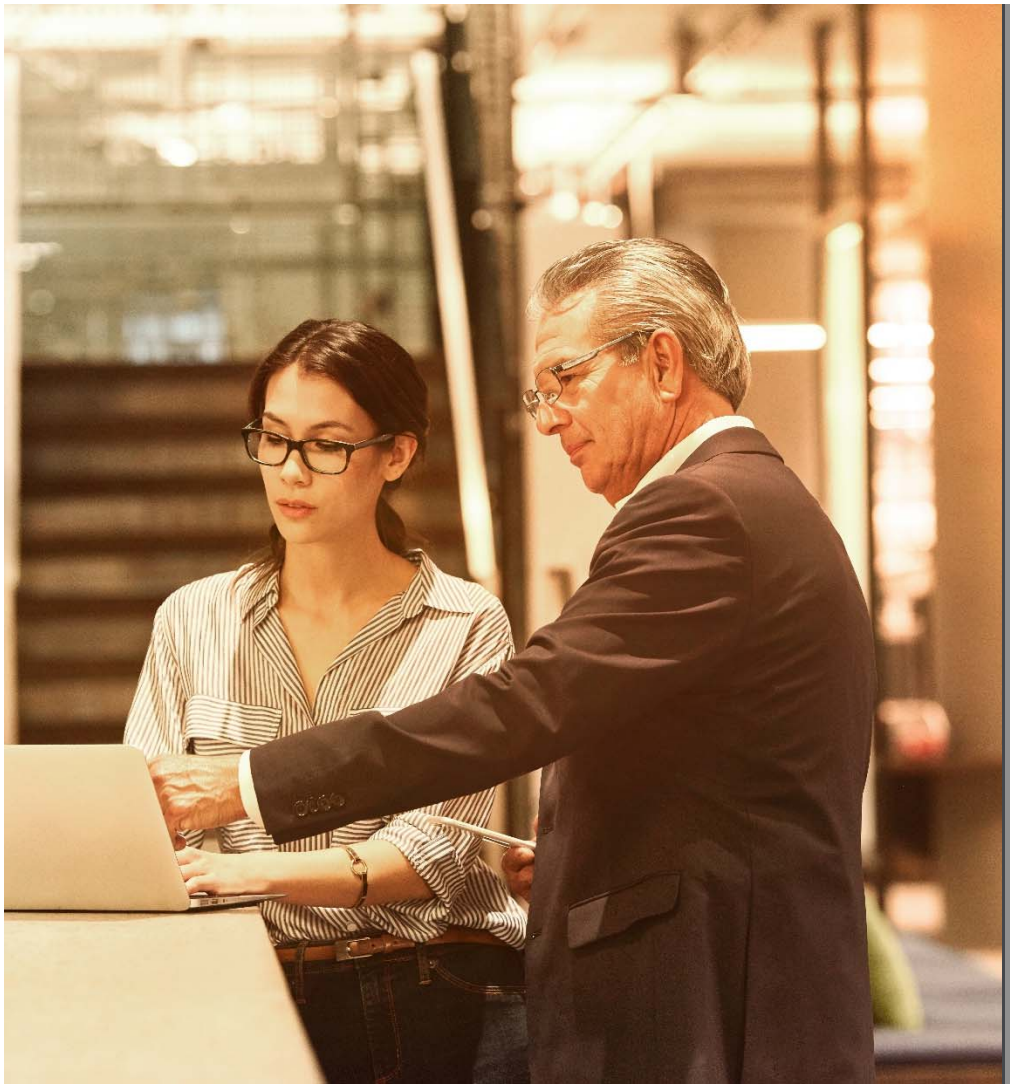
- Validate **all** changes
- Call general phone # at supplier and be routed to specific AR contact person
- Consider adding multifactor authentication:
  - Past payment data or invoice details
- Verify account ownership

3. Implement dual custody

Dual custody requires two employees review and approve changes. This serves as a second chance to spot a fraudulent payment before it goes out the door.

- Confirm all changes have been verified before approving
- Consider auditing a certain # of changes

Never a rubber stamp



Imagine you and your team are putting the finishing touches on next year’s budget when…

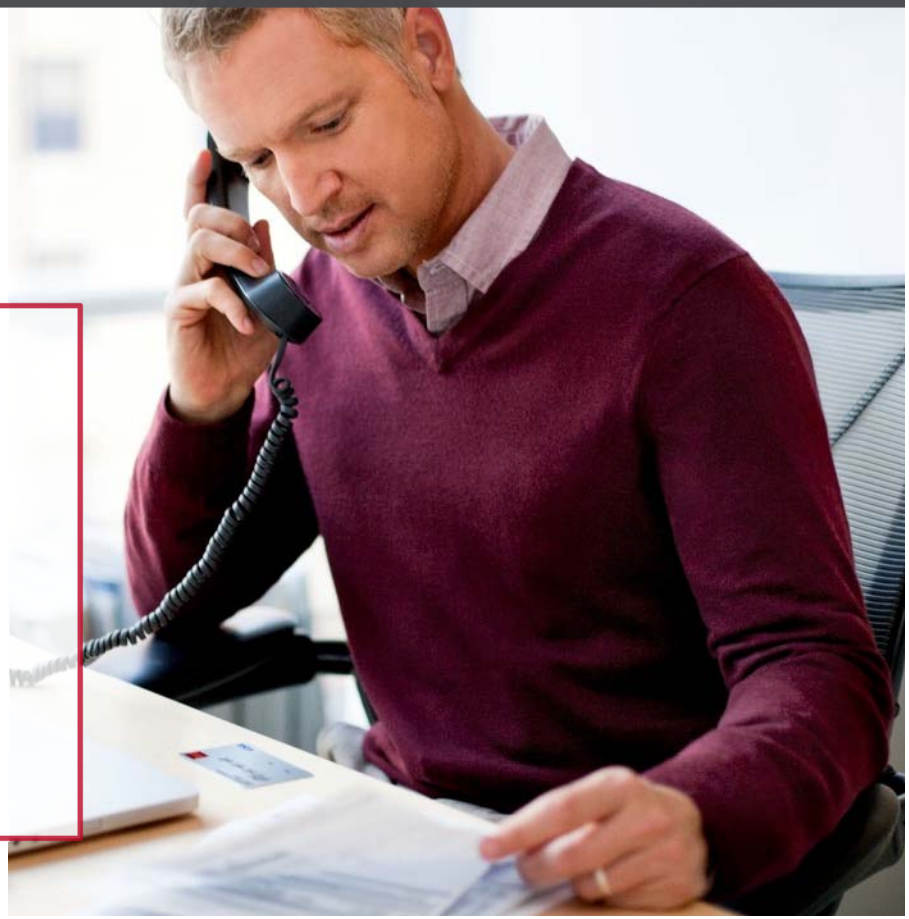
…your computer screen goes completely dark and a message appears stating your organization is the newest member of the ransomware club.

Now imagine the new reality you'll be operating in…

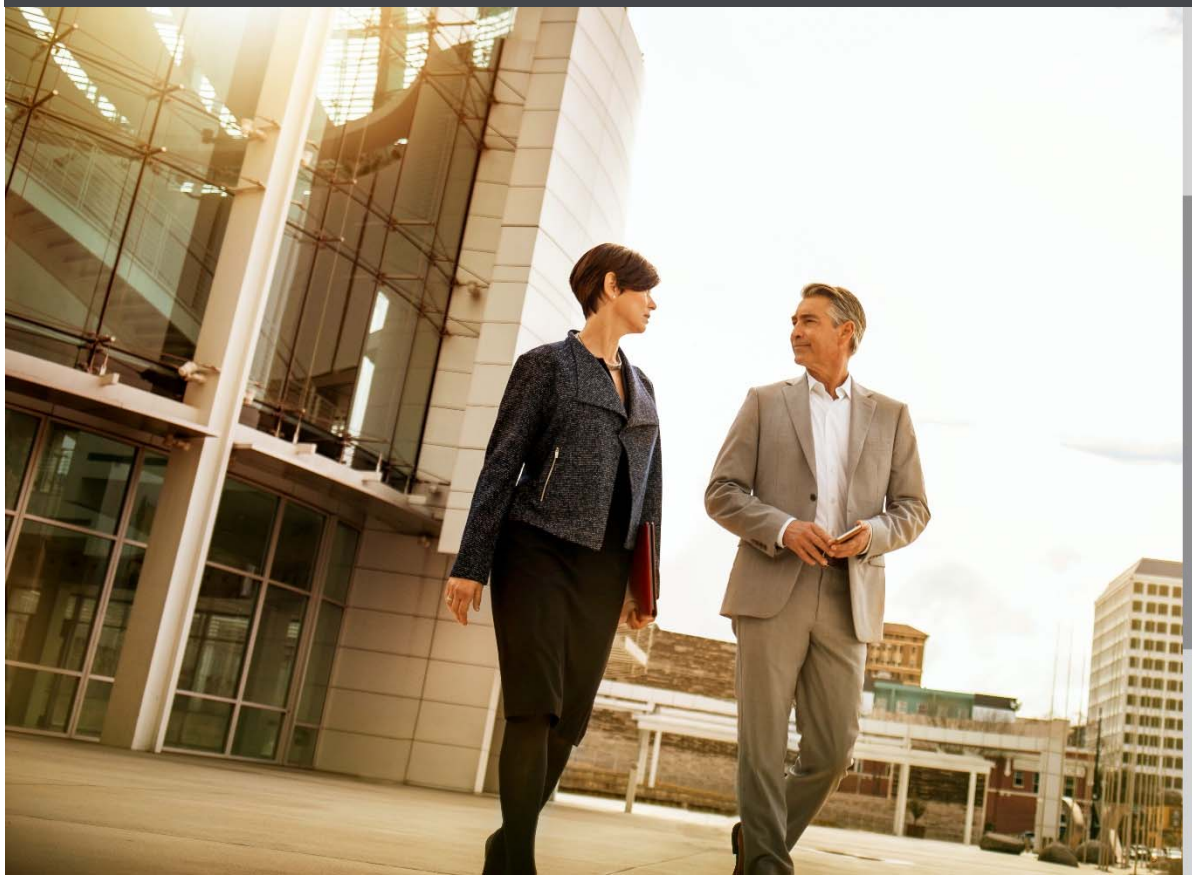
What data can you access?

Can key processes **continue**?

Will employees get **paid on-time**?



Another inconvenient truth…



Many organizations' business continuity plans (BCP) are heavily focused on weathering a natural disaster vs. one that is man made

Business continuity/continuation of operations

Critical processes

Critical payments

Critical stakeholders and departments

Critical timing

Critical approvals

“

Truth is ever to be found in simplicity,
and not in the multiplicity and confusion
of things.

- *Isaac Newton*

”

It is alarming that the rate of payments fraud has reached a record high despite repeated warnings.

In addition to being extremely vigilant, treasury and finance professionals will need to anticipate scams and be prepared to deter these attacks.

- AFP President and CEO Jim Kaitz

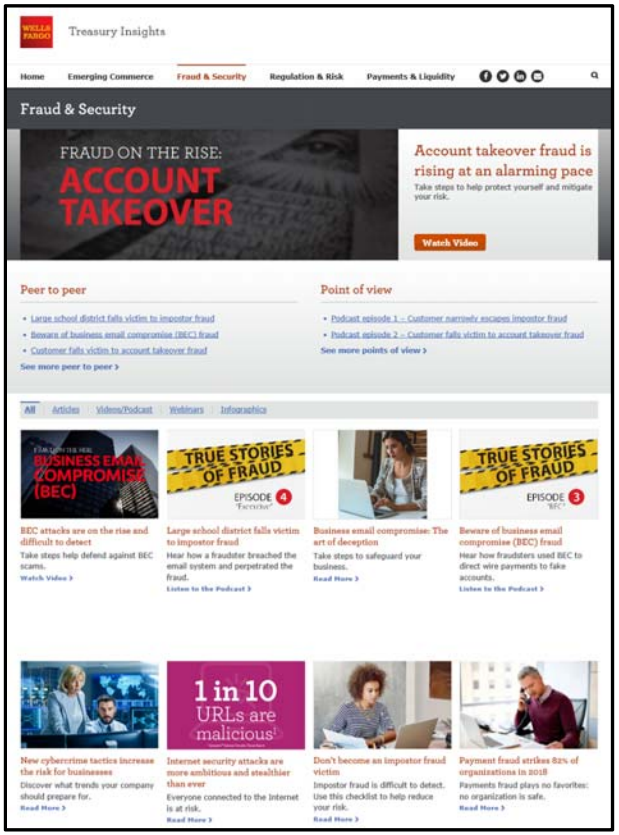
Resources for more fraud protection information

Fraud websites for additional fraud assets

- Treasury Insights Fraud & Security page
  - https://digital.wf.com/treasuryinsights/fraud-security/)
- Wellsfargo.com fraud page
  - https://www.wellsfargo.com/com/fraud

Fraud checklists

- 3 steps to combat impostor fraud checklist
  - https://digital.wf.com/treasuryinsights/portfolio-items/tm3232/
  - Triumph over account takeover checklist
  - https://digital.wf.com/treasuryinsights/portfolio-items/tm3167/



Note: to use the links, highlight the link, right click and select "Open Hyperlink" – if reading hard copy, enter the https address on your browser.

Thank you