NonProfit 360

Session 13: Fraud & Abuse in Banking Industry

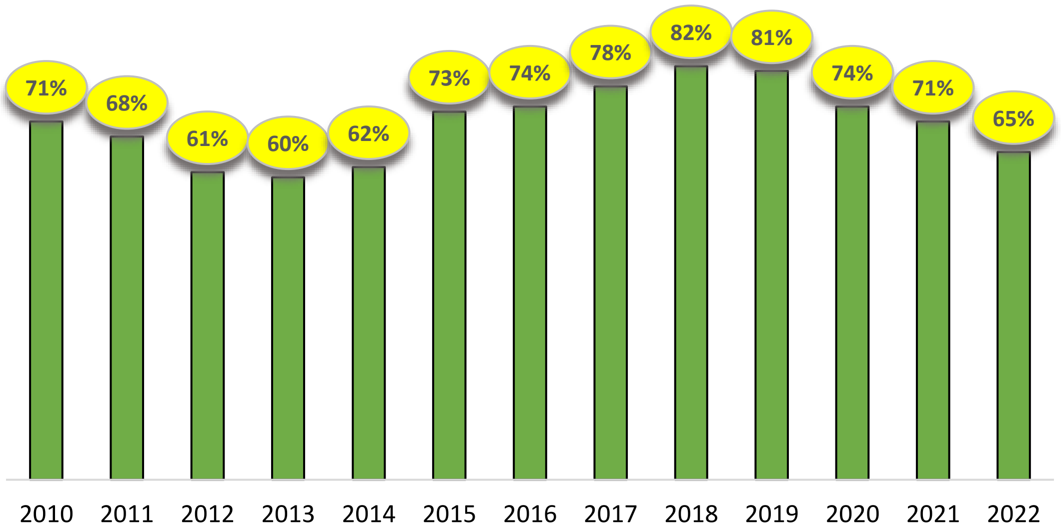
Disclaimer:

The opinions expressed in the presentation are statements of the speaker’s opinion, are intended only for informational purposes, and are not formal opinions of, nor binding on Regions Bank, its parent company, Regions Financial Corporation and their subsidiaries, and
any representation to the contrary is expressly disclaimed.

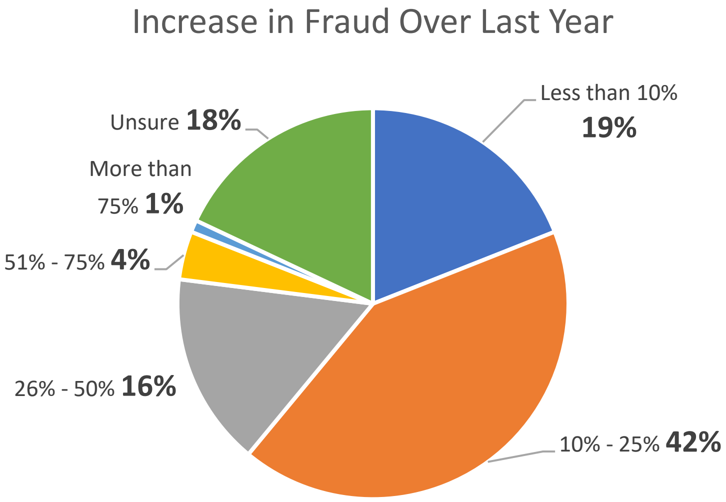
Course Objectives:

- AFP Payment Fraud Highlights
- Fraud Schemes - Recaps
- Industry Suggested Practices
- Resources
- Questions

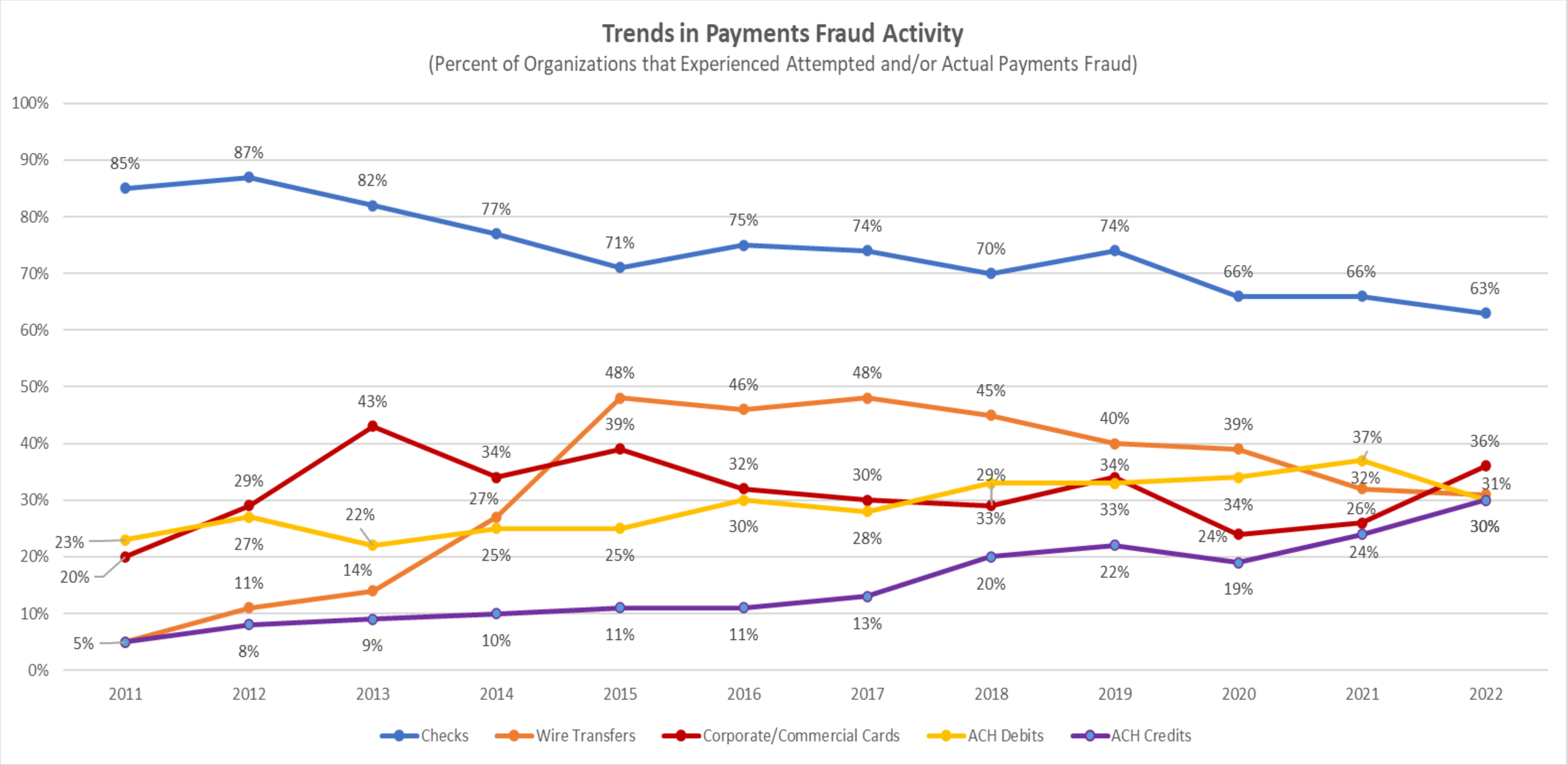
Payment Fraud and Control Survey Highlights



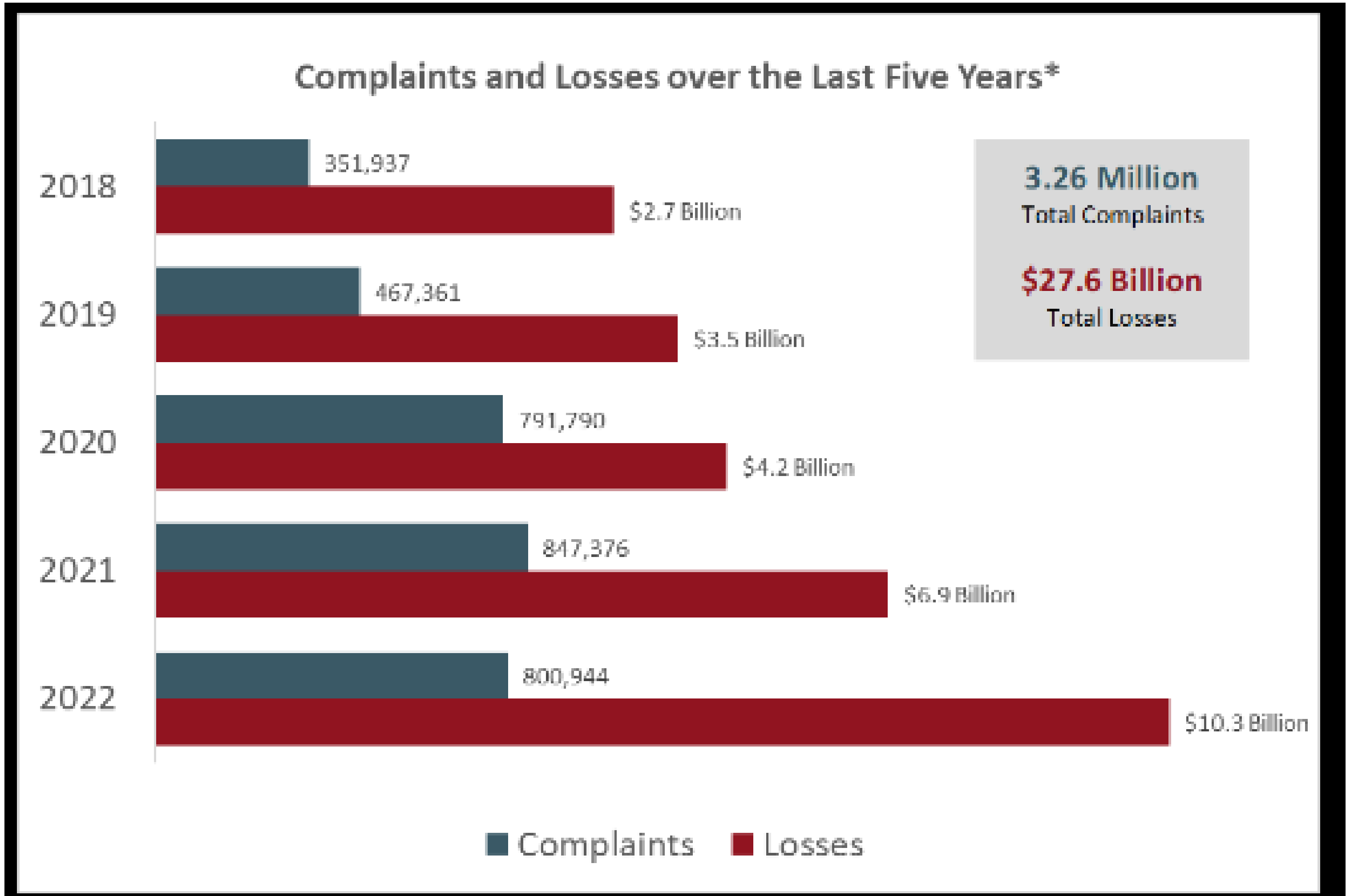
- Remains an issue despite decline
- Two out of Three continue to be victims
- Larger organizations targeted more frequently (78%)
- Smaller organizations (60%)
- 58% indicate fraud has increased 10% - 50% over 2021



2023 AFP® Payments Fraud and Control Survey Report: Highlights | www.AFPonline.org



Source: 2023 AFP® Payments Fraud and Control Survey Report: Highlights | www.AFPonline.org



Complaints and Losses over the Last Five Years*

Chart includes yearly and aggregate data for complaints and losses over the years 2018 to 2022. Over that time, IC3 received a total of 3.26 million complaints, reporting a loss of $27.6 billion.

Source: www.ic3.gov

Check Fraud

Traditional Check Fraud - Recap

Check Fraud

1. **Alteration**
   - Change to face or back of checks
   - Payee name or amount

2. **Counterfeit**
   - Illegal, unauthorized printing of checks

3. **Forgery**
   - Unauthorized maker's signature – produced manually or via fax
   - Unauthorized endorsements/payees

BEST PRACTICES

1 Reconcile to spot abnormal activity

- Reconcile your accounts in a timely manner.
- Segregate your accounts by purpose, type, and/or payment method.

2 Place stop payments on any checks that have been lost or stolen

3 Convert paper payments to electronic payments

For Employees

- Use Automated Clearing House (ACH).
- If an employee does not have a bank account, offer to deposit their pay directly to a payroll card that allows them to use it like a bank debit card.

For Vendors

- Pay via ACH or purchasing card.
- Use wire transfers for high-value or time sensitive payments as well.

4 Securely store check stock, deposit slips and bank statements, then destroy securely

5 Use Positive Pay

This powerful tool allows you to send information to your bank about the checks you've written so that when checks come in to pay, they are matched to what you've told them. Positive Pay is also available for ACH. If you've authorized a supplier or other partner to draft money from your account you can pre-approve these transactions.

Ransomware

Ransomware

- Fraudsters target an organization by placing malware on the organization’s computer system and locking the system with encryption.
- Payment (ransom) is demanded before the fraudster releases the code to unlock the system.
- Fraudsters access the computer system through:
  - Phishing & social engineering
  - Infected software applications
  - Infected documents and files
  - Infected external storage devices
  - Compromised websites

Examples of ransomware in Non-Profit sector

- ❖ A breach was detected when unusual activity in an employee’s email account was spotted by a security contractor. The criminal compromised the personal computer of an employee working remotely and stole $7.5 million from the organization’s endowment funds.
- ❖ A cybersecurity incident when a hacker gang infiltrated their systems. The attack resulted in the compromise of 6.8 terabytes of sensitive data, including HR files, personal information, and financial records.
- ❖ Insider fraud resulted in the compromise of donor financial data.

- www.ic3.gov received 2,385 complaints
- States have recently passed legislation prohibiting government agencies from paying or negotiating a ransom (NC & FL)
- Government, education, financial services, and vulnerable organizations are targets
- Ransomware-as-a-Service

https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf

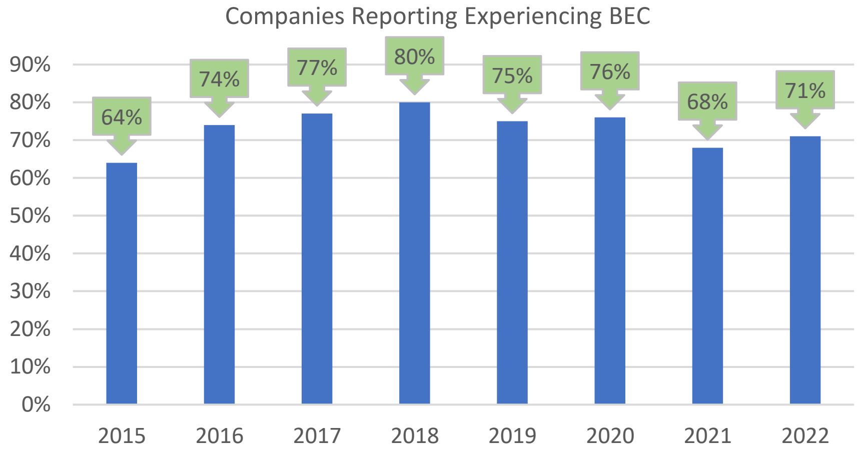
When fraud occurs, what are the industry suggested next steps?

1. **Disconnect infected computers/devices**
   - *Remove the connections to the network immediately*
2. **Engage your IT team**
   - *Let your IT team know immediately so they can begin remediation*
3. **Contact the impacted parties**
   - *Communicate the details needed for all impacted parties to take necessary action*

Business Email Compromise (BEC) -

Business Email Compromise - Recap

- 71% of companies experienced BEC (2023 AFP survey)
- www.ic3.gov received 21,832 BEC reports, representing $2.7 Billion in losses in 2022
- All industry segments at risk
- Target employees with access to company finances and money movement capability – 60% indicate Accts Payable

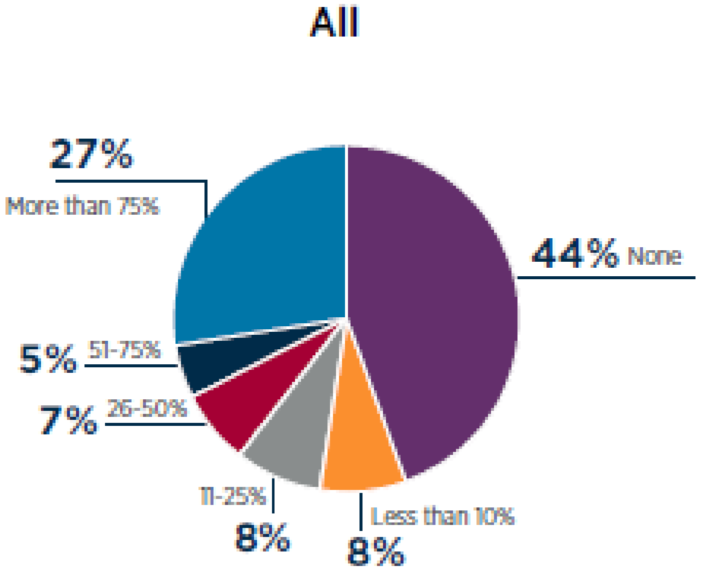

Companies Reporting Experiencing BEC

Iterations Over Time:

- **Executive email intrusion**
- **Vendor email intrusion**
- **Employee email intrusion**

Recoup of Funds After a Successful Fraud Attempt
(Percentage Distribution of Organizations that Experienced Fraud)

60% of victimized companies recovered less than 25% of funds



2023 AFP® Payments Fraud and Control Survey Report: Highlights | www.AFPonline.org

BEC – Means of Deception

- **Phishing** – bogus emails prompt victims to reveal confidential information
- **E-mail Spoofing** – slight variations on legitimate email addresses (73%)
- **Domain lookalike –** slight variations of the legitimate domain address (57%)
- **Legitimate email taken over by fraudster** (54%)
- **Social Engineering** – phone calls/conversations to gain trust

Importance to Non-Profit Organizations

1. **Board Responsibilities**
   - ➢Communicating and reporting for Board awareness
   - ➢Protection of your contribution platform
   - ➢Development of a response plan

2. **AI Generated Impersonations & infused scams**
   - ➢Deep fake video and audio
   - ➢AI (ChatGPT) generated communications

3. **Trusted Partner/Imposter scam**
   - ➢Spoofed phone numbers and text messages
   - ➢Spoofed websites and search engine ads

4. **Business Email Compromise**
   - ➢Relies on human interaction & participation
   - ➢Difficult to detect

NonProfit 360

Education and Awareness are Key to Prevention

- Are your **internal controls** strong enough?
- Over the past 18 months, have you experienced a **financial loss** related to fraud?
- Is access to your **networks and data** secure?
- Do you have a strong **vendor management program?**
- Do you have software in place to detect and stop **phishing & malware?**
- Do you have a **cybersecurity employee education & awareness program?**
- Do you have a **cybersecurity action & governance plan?**

NonProfit 360

Guard Your House 1

- Conduct an IT vulnerability assessment
- Work with your IT vendor to create effective firewall protocols that protect your systems and confidential information
- Regularly patch and update security systems and back up critical data offline
- Require secure passwords and multi-factor authentication
- Leverage fraud prevention tools - Positive Pay, ACH Positive Pay & Account Reconcilement

Create a Training Program 2

- Utilize the videos and information to educate critical payment stream positions. Resources include: **www.regions.com/stopfraud** and **www.regions.com/fraudprevention**
- Perform regular phishing testing
- Encourage Associates to be aware of potential points of compromise
- Don’t click on links or attachments from unknown sources
- Encourage a fraud awareness mindset

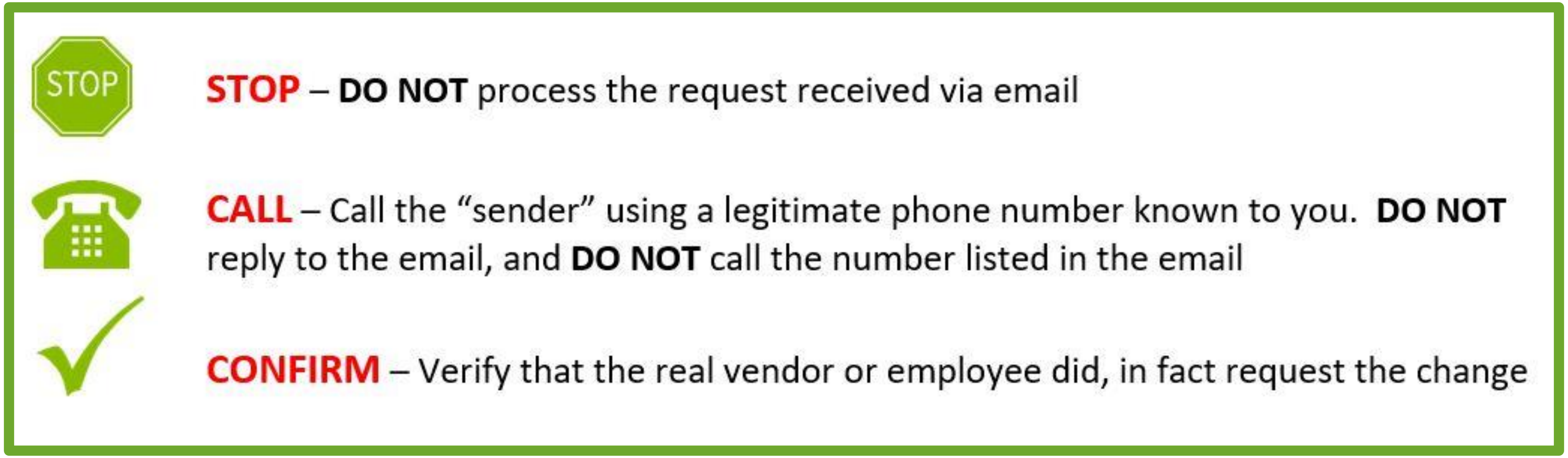
Create a Fraud and Risk Governance Plan 3

- Identify and document risk tolerance
- Divide financial responsibilities
- Create a robust vendor management program
- Document a detailed fraud response plan
- Review cybersecurity insurance coverage
- Review and establish internal controls like least privilege access and a call-back procedure for changes in payments

NonProfit 360

Call Back Control

If you receive an email requesting a change to the account number for payments:



STOP – **DO NOT** process the request received via email

CALL – Call the "sender" using a legitimate phone number known to you. **DO NOT** reply to the email, and **DO NOT** call the number listed in the email

CONFIRM – Verify that the real vendor or employee did, in fact request the change

Additional Website Information

Federal Government	Internet Crime Complaint Center	https://www.ic3.gov
	Federal Bureau of Investigation	https://www.fbi.gov
	Cybersecurity & Infrastructure Security Agency	https://www.CISA.gov
	Federal Trade Commission	https://www.ftc.gov
	National Security Agency	https://www.nsa.gov
	CISA, Homeland Security & Secret Service	https://www.stopransomware.gov
	US Postal Inspectors Service	https://www.uspis.gov
Regions	Stop Fraud	https://www.regions.com/stopfraud
	Doing More Today	https://www.doingmoretoday.com/
	Fraud Prevention	https://www.regions.com/fraudprevention

Presenter & Contact Information

Sam Woodring	**Commercial Banking**	**636-387-2012**	**sam.woodring@regions.com**
Brenden Finnerty	Commercial Banking	618-581-3965	brenden.Finnerty@regions.com
Drew Gress	Nonprofit Banking	636-627-8550	andrew.gress@regions.com

NonProfit 360