Fighting Commercial Fraud in 2023

TN Government Finance Officers Association

Jeffrey Taylor, CTP
Senior Vice President – Corporate Banking Group Fraud Forensics

September 28, 2023

REGIONS

Disclaimer:

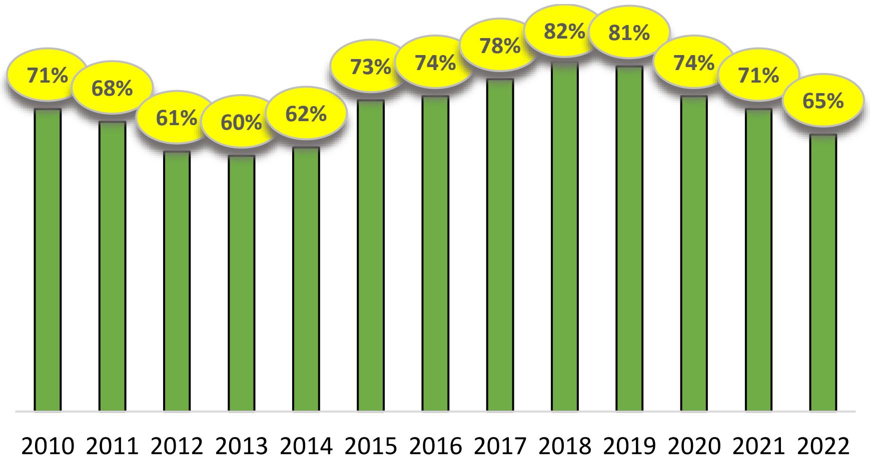
The opinions expressed in the presentation are statements of the speaker’s opinion, are intended only for informational purposes, and are not formal opinions of, nor binding on Regions Bank, its parent company, Regions Financial Corporation and their subsidiaries, and any representation to the contrary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

REGIONS

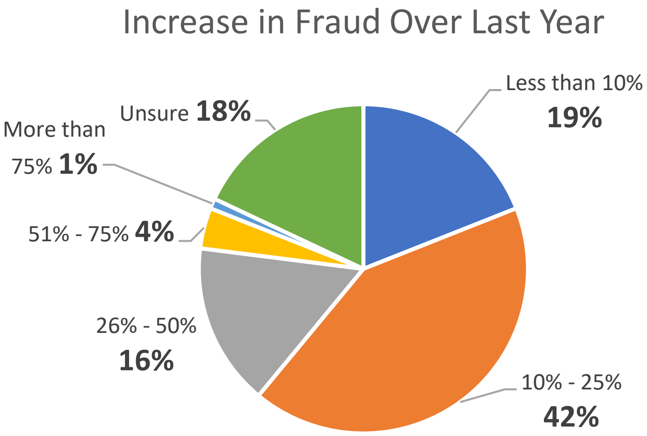
Agenda

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

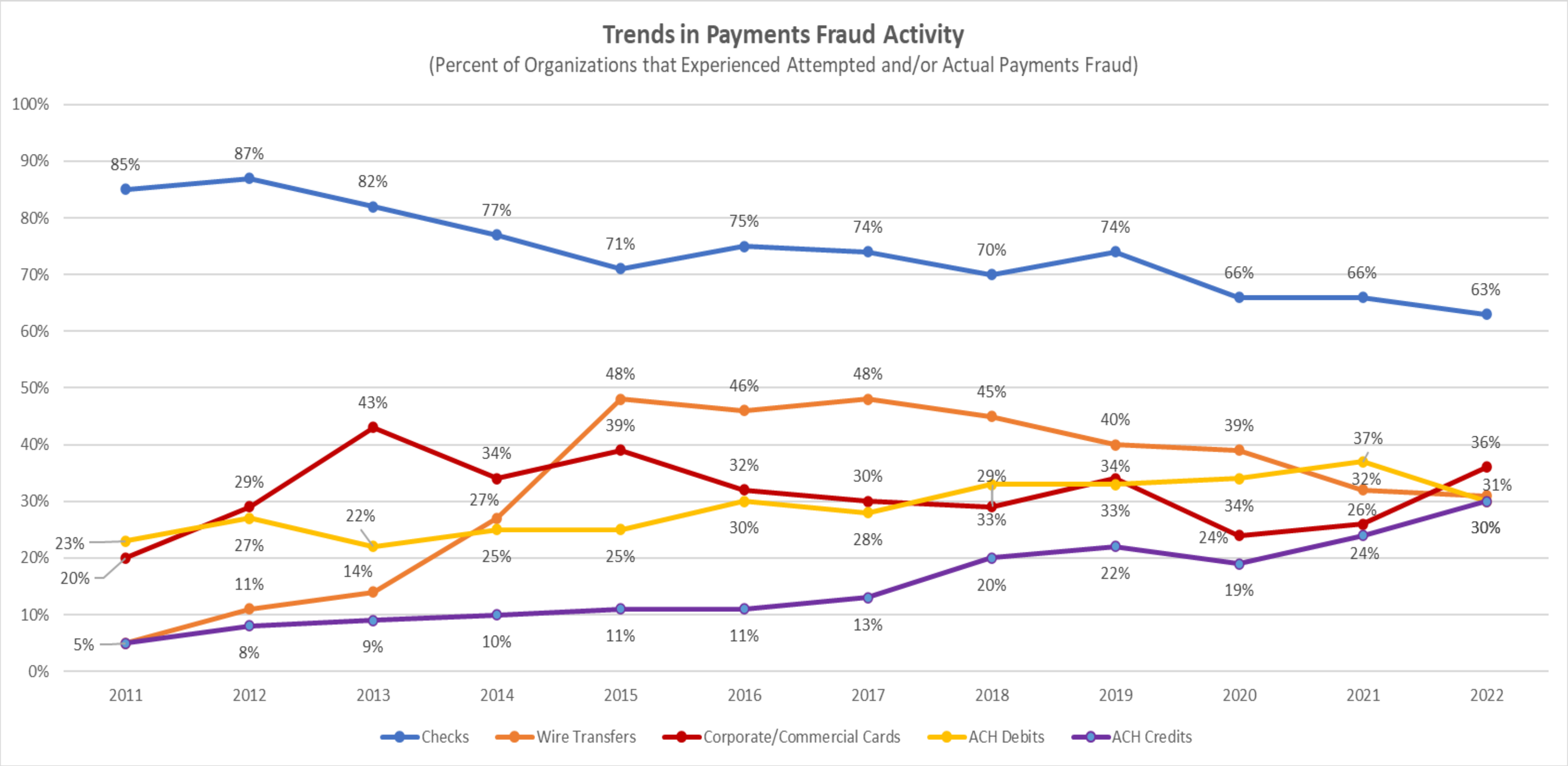
Payment Fraud and Control Survey Highlights



- Steady decline since 2018, but remains an issue
- Overall attacks have decreased?
- 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



Trends in Payments Fraud Activity

(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)

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

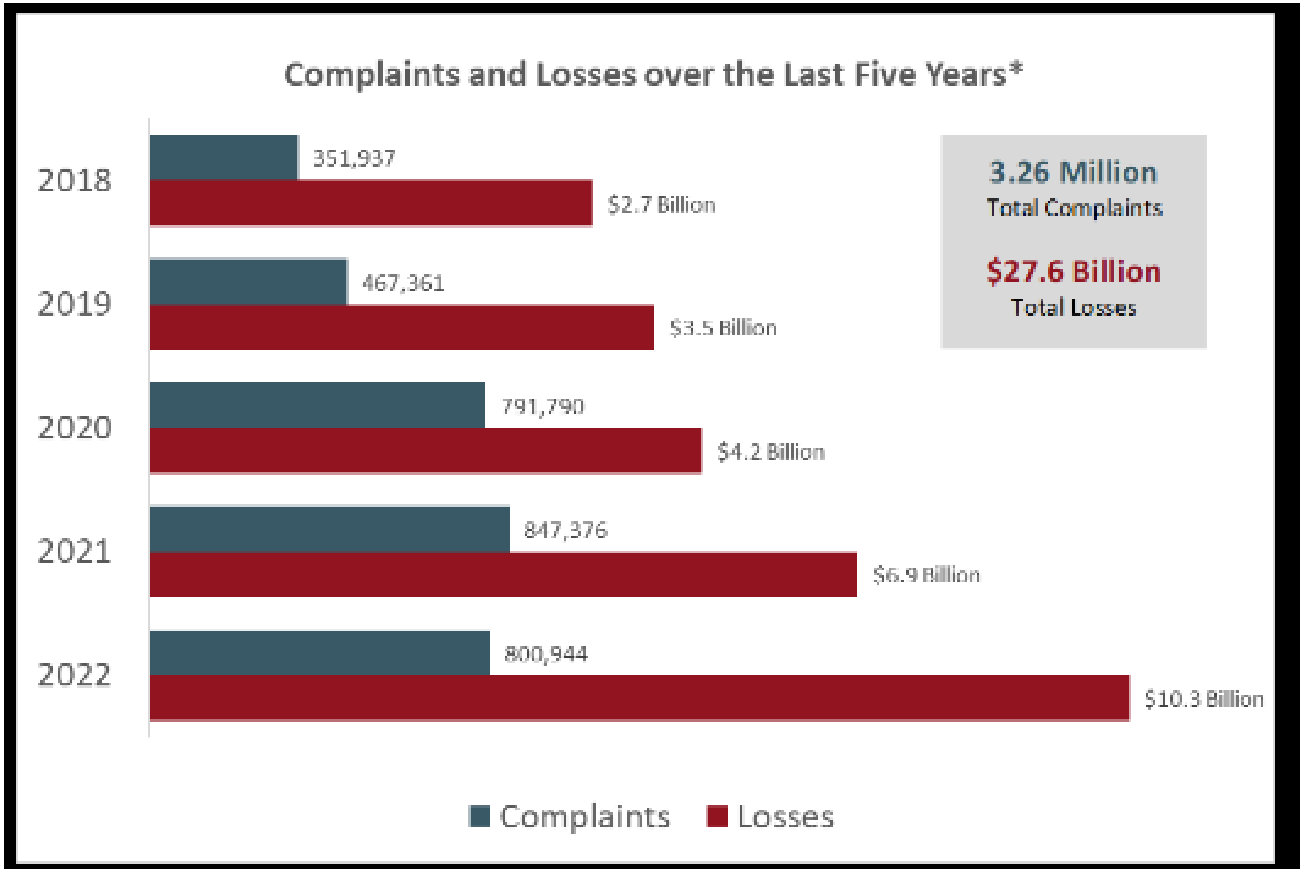


Chart includes yearly and aggregate data for complaints and losses over the years 2018 to 2022. Over that time, IC3 received a total of 3.26 million complaints, reporting a loss of $27.6 billion.

Source: www.ic3.gov

Check Fraud

Traditional Check Fraud - Recap

Check Fraud

1. **Alteration**
   - Change to face or back of checks
   - Results in non-conforming
2. **Counterfeit**
   - Illegal, unauthorized printing of checks
3. **Forgery**
   - Unauthorized maker's signature – produced manually or via fax
   - Unauthorized endorsements/payee claims
   - payments instructions/endorsements
4. **Improper/missing endorsements**
   - Endorsement is missing or doesn't conform to the way check was drawn
5. **Non-negotiable check copy**
   - Photocopy of check processed as an original check

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

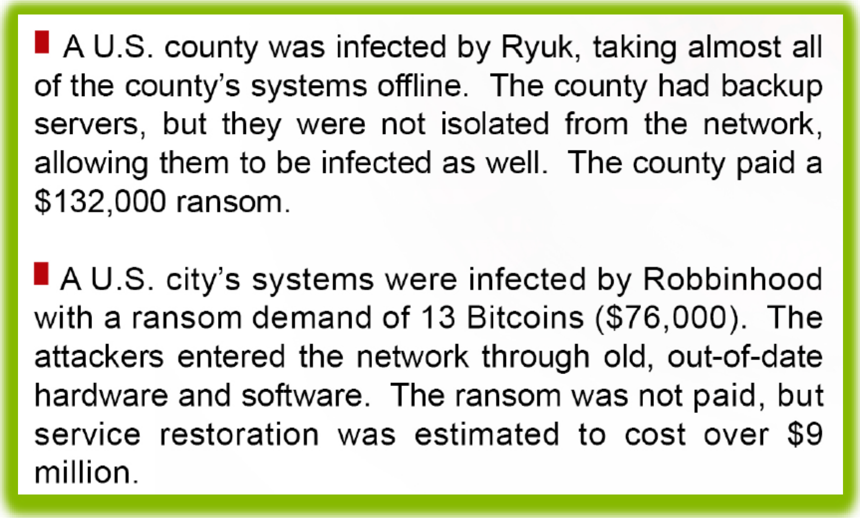
This powerful tool allows you to send information to your bank about the checks you've written so that when checks come in to pay, they are matched to what you've told them. Positive Pay is also available for ACH. If you've authorized a supplier or other partner to draft money from your account you can 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:
  - Infected software applications
  - Infected documents and files
  - Infected external storage devices
  - Compromised websites

Examples or ransomware in the public sector



- A U.S. county was infected by Ryuk, taking almost all of the county's systems offline. The county had backup servers, but they were not isolated from the network, allowing them to be infected as well. The county paid a $132,000 ransom.

- A U.S. city's systems were infected by Robbinhood with a ransom demand of 13 Bitcoins ($76,000). The attackers entered the network through old, out-of-date hardware and software. The ransom was not paid, but service restoration was estimated to cost over $9 million.

- www.ic3.gov received 2,385 complaints
- States have recently passed legislation prohibiting government agencies from paying or negotiating a ransom (NC & FL)
- Critical infrastructure organizations are targets
- Need for adequate back up plans

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

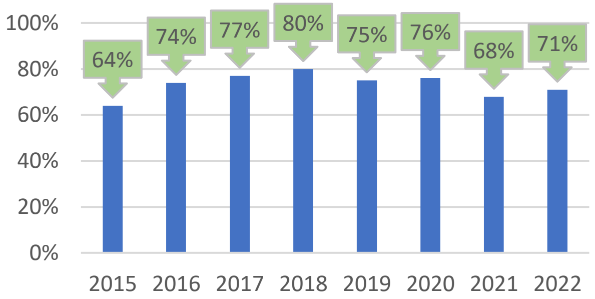
- *Communicate the details needed for all impacted parties to take necessary action*

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
- Target employees with access to company finances and money movement capability – 60% indicate Accts Payable

Companies Reporting Experiencing BEC



Iterations Over Time:

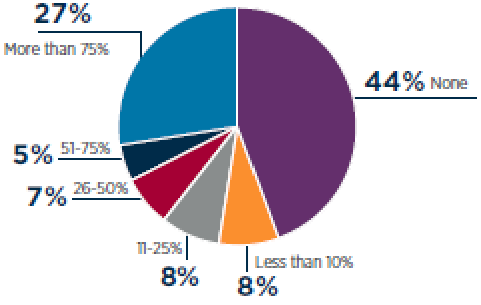
- **Executive email intrusion:** criminal impersonates senior executive requesting payment or order to purchase gift cards
- **Vendor email intrusion:** criminal impersonates vendor requesting the company to change payment remittance information
- **Employee email intrusion:** criminal impersonates an employee requesting the vendor to send payment account information or requesting the company change employee's direct deposit information

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

All



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

Scaries

1. **AI Generated Impersonations**
   - Deep fake video and audio

2. **AI Infused Scams**
   - AI (ChatGTP) generated communications

3. **Trusted Partner/Imposter scam**
   - Spoofed phone numbers and text messages

4. **Business Email Compromise**
   - Relies on human interaction & participation
   - Merges with the trusted partner scam

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?**

Three Industry Suggested Practices

Guard Your House 1

- Conduct a thorough IT vulnerability assessment
- Work with your IT Department to create efficient and effective firewall protocols that guard and protect your systems and confidential information
- Regularly patch and update security systems and back up critical data offline
- Require the use of secure passwords or pass phrases
- Leverage fraud prevention tools - Positive Pay, ACH Positive Pay & Account Reconcilement

Create an Associate Training Program 2

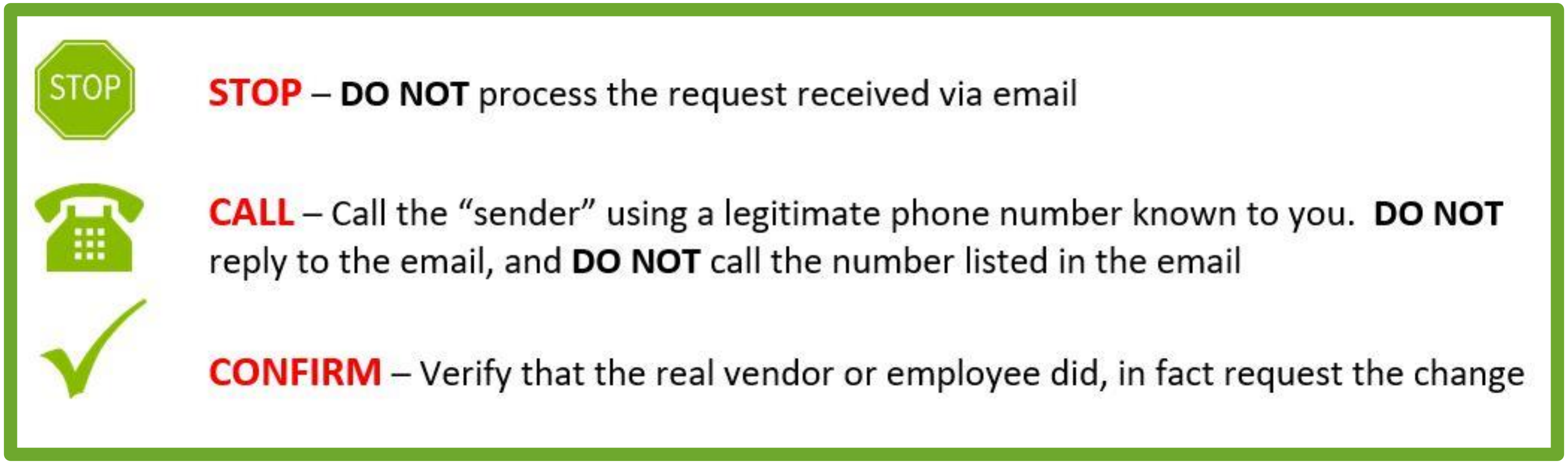
- Utilize the videos and information to educate critical payment stream positions. Resources include: www.regions.com/stopfraud and www.regions.com/fraud_prevention
- Perform regular phishing testing on Associates
- Encourage Associates to be aware of potential points of compromise
- Don’t click on links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

Create a Fraud and Risk Governance Plan 3

- Identify and document risk tolerance
- Create a robust vendor management program
- Document a detailed fraud response plan
- Establish internal controls like a call-back procedure for changes in payments

Call Back Control

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



STOP **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

REGIONS

Additional Website Information

Federal Government		
	Internet Crime Complaint Center	j wr uŝőőy y y ſkeı ſi qx
	Federal Bureau of Investigation	j wr uŝőőy y y ſhdkſi qx
	Cybersecurity & Infrastructure Security Agency	j wr uŝőőy y y ſEKUCſi qx
	Federal Trade Commission	https://www.ftc.gov
	National Security Agency	j wr uŝőőy y y ſpucſi qx
	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

QUESTIONS

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**.**

The information presented is general in nature. Presentation material sourced from the Association for Financial Professionals, and the Department of Homeland Security are noted. Regions reminds its customers to be vigilant about fraud and security, and they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices, as the threat evolves daily. There is no guarantee all fraudulent transactions will be prevented or that related financial losses will not occur.

REGIONS