2024Commercial Fraud Risk Update

Alabama Association of School Board Officials

Randy Wilborn, CTP, CFE
Vice President - Product Manager, Treasury Management Fraud Solutions

May 23, 2024
Webinar

Disclaimer:

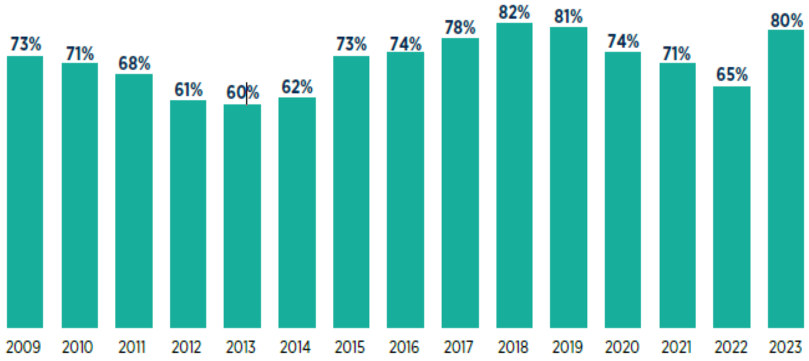
The opinions expressed in the presentation are statements of the speaker's opinion, are intended only for informational purposes, and are not formal opinions of, nor binding on Regions Bank, its parent company, Regions Financial Corporation and their subsidiaries, and any representation to the contrary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

REGIONS

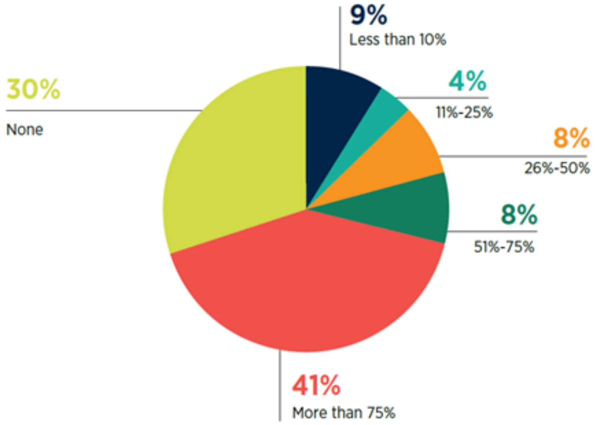
Agenda

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

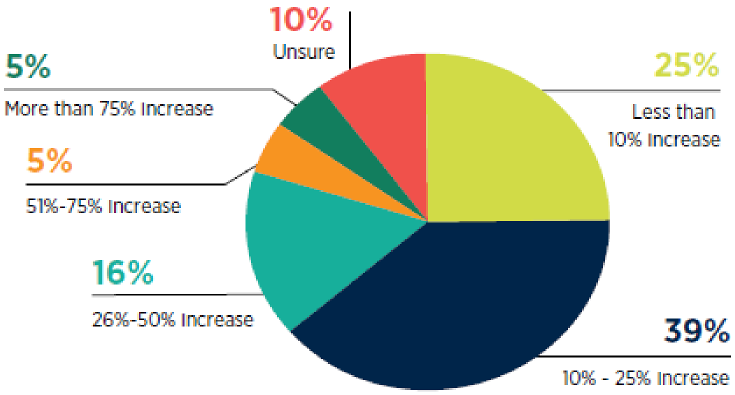
AFP Payment Fraud and Control Survey Highlights



Percentage of Lost Funds Recovered



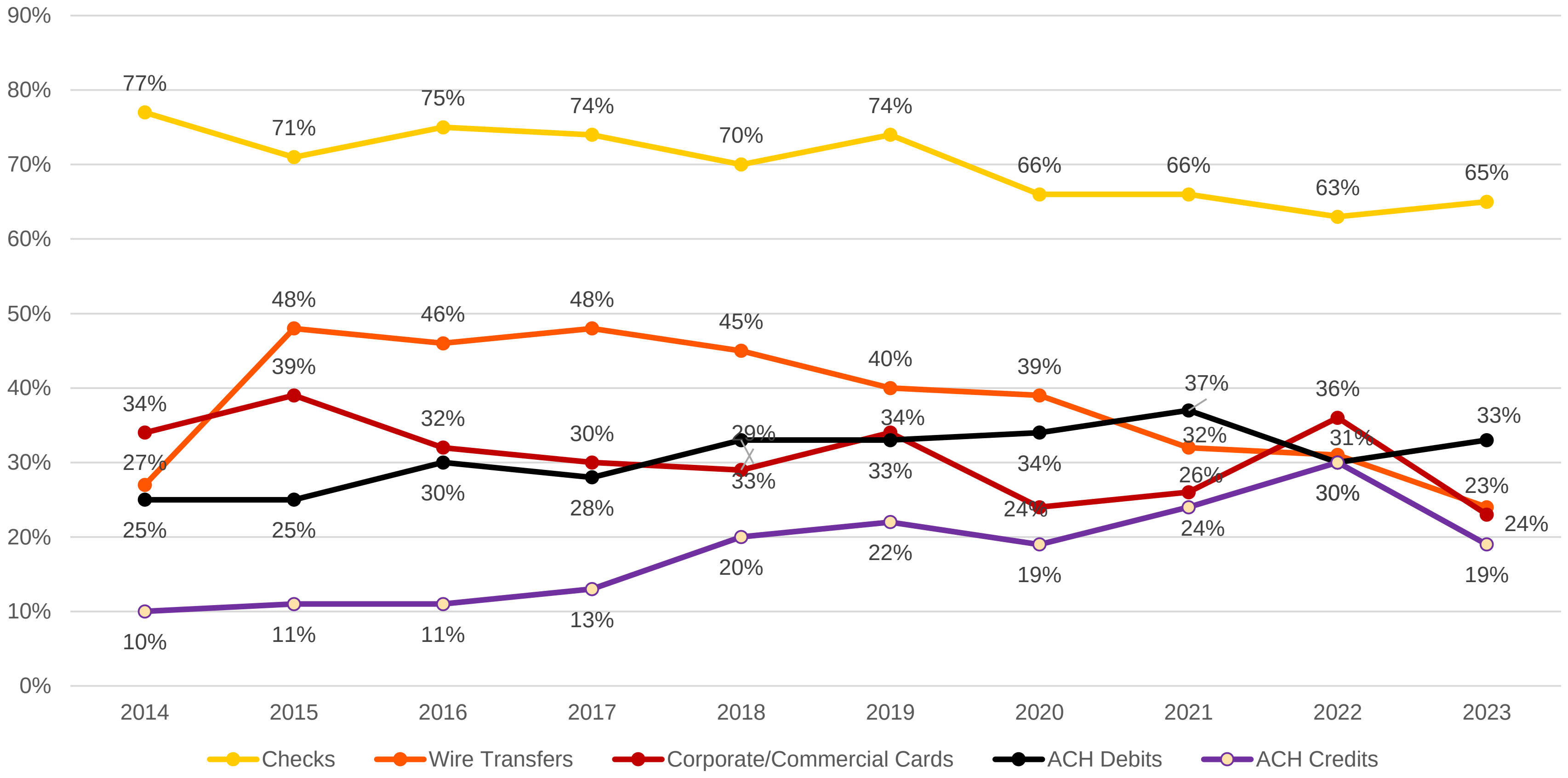
Increase in Fraud over Last Year



80% of organizations were reported targets in 2023
15% increase over 2022
Two out of three continue to be victims
Larger organizations targeted more frequently (83%)
Smaller organizations (74%)
39% indicate fraud has increased 10% - 25% over 2022

Trends in Payments Fraud Activity

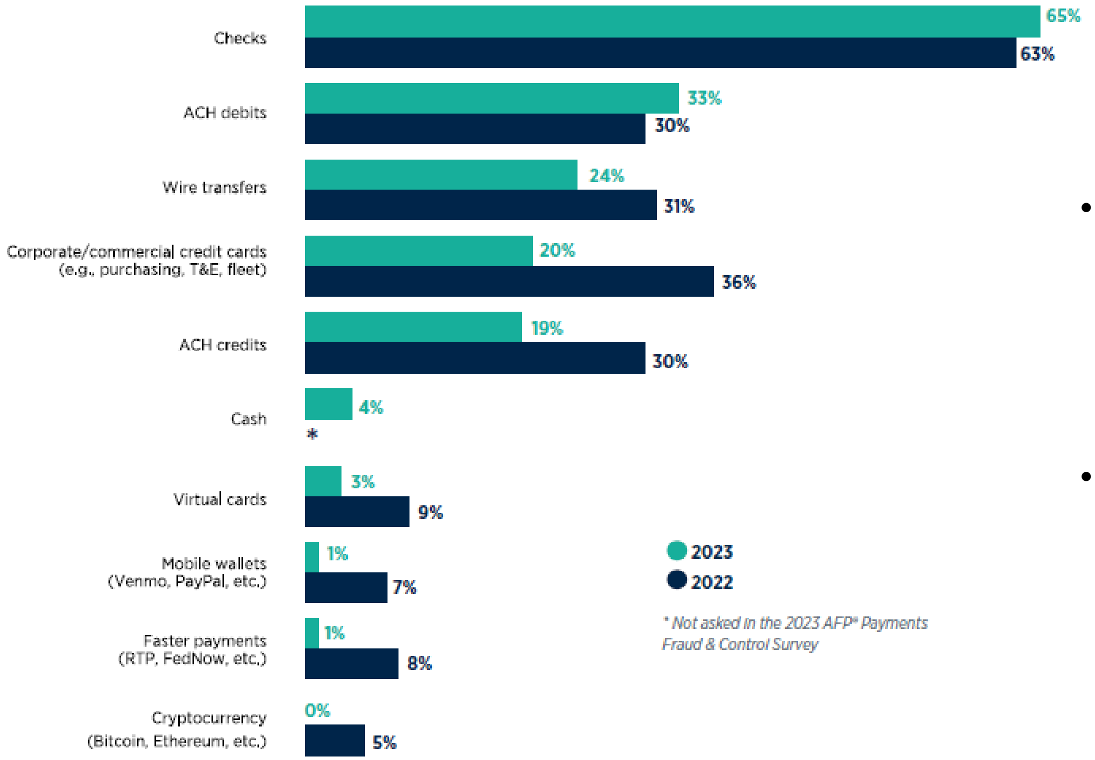
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)



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

AFP Payment Fraud and Control Survey Highlights

Payment Methods Subject to Attempted/Actual Payments Fraud



** Not asked in the 2023 AFP® Payments Fraud & Control Survey*

- 2023 increases in check and ACH debit fraud (increase likely due to check fraud- creation of ACH debit with stolen check information)

- Wire transfer, ACH credits and commercial card/virtual card/mobile wallet has gone down

Source: 2024 AFP® Payments Fraud and Control Survey Report: Highlights | www.AFPonline.org

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

Check Fraud - Helpful Practices to Avoid these Schemes

Positive Pay detects fraudulent checks by comparing check serial number, amount, and payee name.

- **Positive Pay Options**
  - Reverse Positive Pay
  - Next Day Positive Pay
  - Same Day Positive Pay
  - Payee Name Verification
  - No Check Positive Pay

- **Account Reconcilement**
  - Full Reconcilement
  - Partial Reconcilement
  - Deposit Reconcilement

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.

“Bookkeeper” Fraud

Bookkeeper Fraud

REGIONS

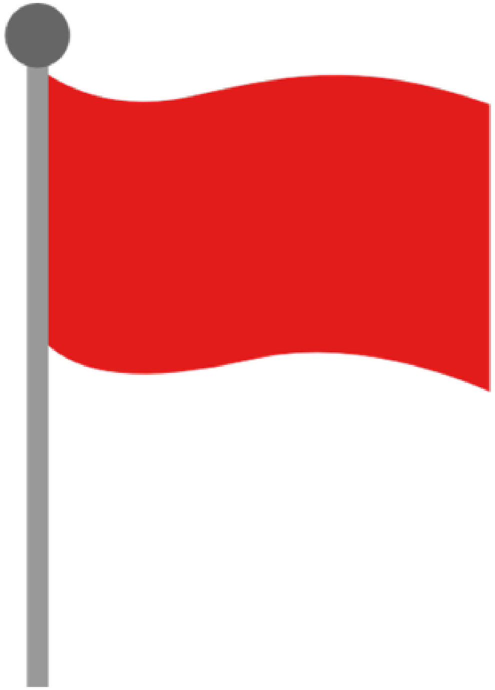
- Arises when full authority has been given to a single employee to issue and reconcile payments, especially associated with checks
- 85% of all fraud is perpetrated by a trusted employee
- Creates bogus accounts payable/vendors and generates payments
- Opens bank account in similar name to business and diverts legitimate checks meant for business
- Obtains blank signed company checks and fills in inappropriate payees
- May also be associated with investment schemes, sales schemes or identity theft

Bookkeeper Fraud - Example

- Company payroll was outsourced to CPA firm
- One employee at the firm was assigned to administer it
- She created employee status for herself with the company
- Regular payroll checks were made payable to her
- Over a five year period a loss of $250k occurred
- Suspect was prosecuted and sentenced to federal prison

Bookkeeper Fraud – Red Flags

- Living beyond their means
- Financial difficulties
- Unusually close association with vendors or customers
- Excessive control issues
- Little vacation taken



Bookkeeper Fraud - Helpful Practices to Avoid these Schemes

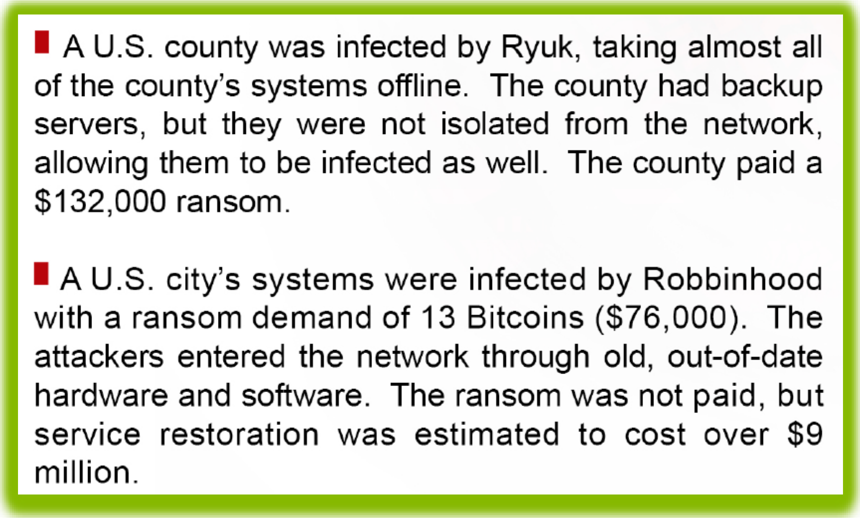
- Never sign blank checks
- Establish dual control for check issuance and account reconciliation tasks
- Make sure all employees are aware of and adhere to internal controls and financial reporting
- Restrict employee access to accounting systems and online functions; audit periodically
- Implement an approval process for new vendors

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

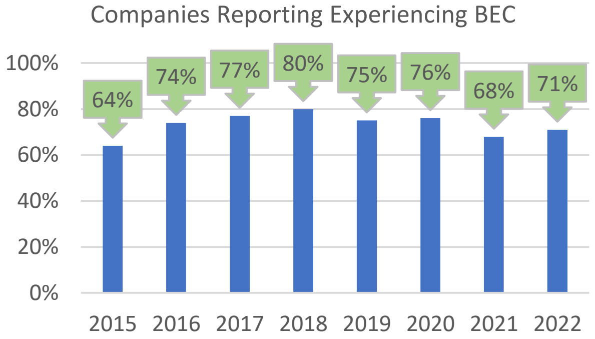
Contact the impacted parties

- *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

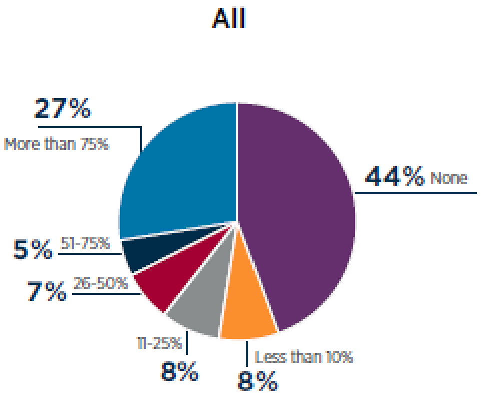
Iterations Over Time:

- **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



BEC – Means of Deception

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

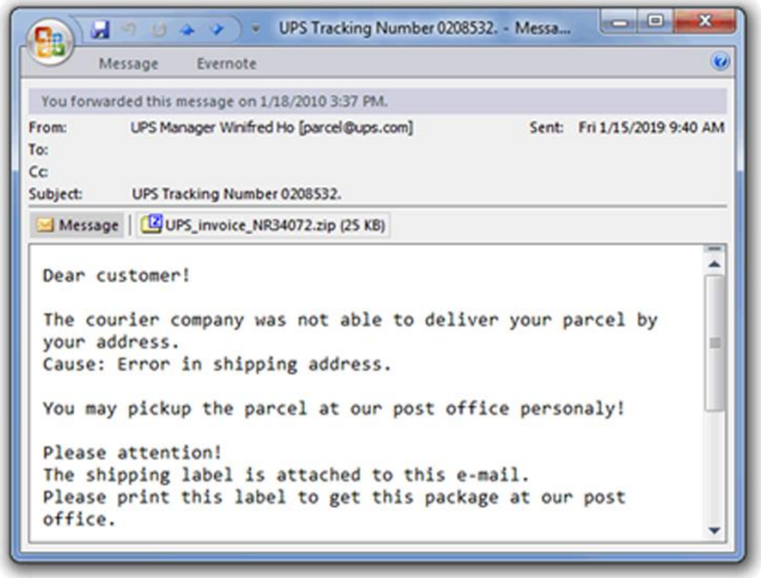
BEC - Helpful Practices to Avoid these Schemes

- Create email rules to identify suspicious emails
- Implement two factor authorization for payment changes
- Phone verification for transfer requests
- Provide employee training and awareness
- Use ‘Forward’ instead of ‘Reply’
- DON’T RELY ON E-MAIL ALONE

Cyber Fraud

Cyber Fraud – Means of Deception

- Phishing emails with malicious links or attachments – Spear Phishing in BEC, shipping documents to compromise e-mail system
- Banner ads on prominent surf engines and news sites – "Malvertising." Increased 200% to 209,000 incidents, 12.4 billion malicious advertisements
- Social networking sites (your friends may not be your friends)
- Probing for un-patched, vulnerable machines and attacking directly
- Immediate goal may be ransomware or theft of intellectual property



You forwarded this message on 1/18/2010 3:37 PM.

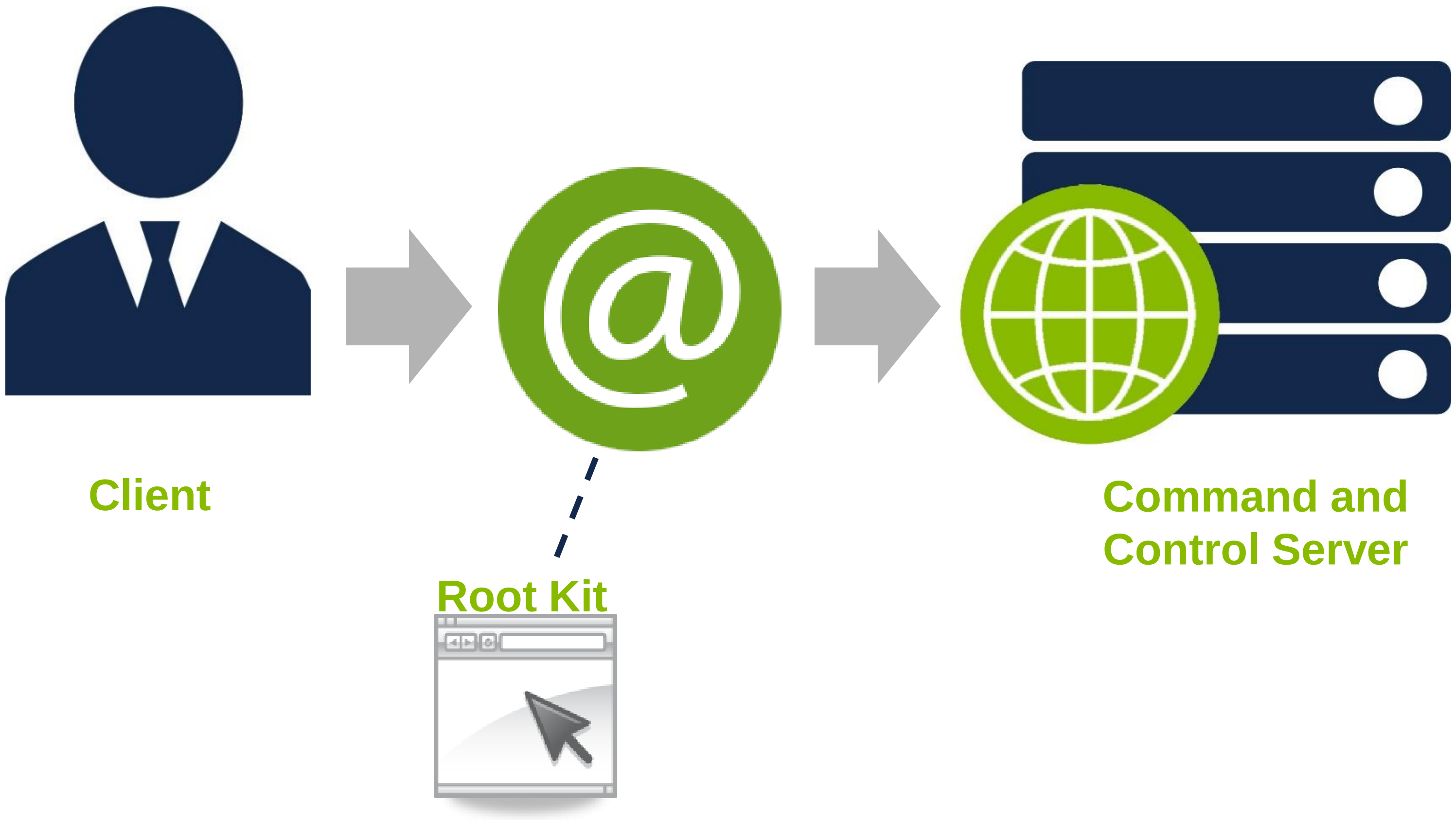
From: UPS Manager Winifred Ho [parcel@ups.com] Sent: Fri 1/15/2019 9:40 AM
To:
Cc:
Subject: UPS Tracking Number 0208532.

Message | UPS_invoice_NR34072.zip (25 KB)

```
Dear customer!

The courier company was not able to deliver your parcel by
your address.
Cause: Error in shipping address.

You may pickup the parcel at our post office personaly!

Please attention!
The shipping label is attached to this e-mail.
Please print this label to get this package at our post
office.
```

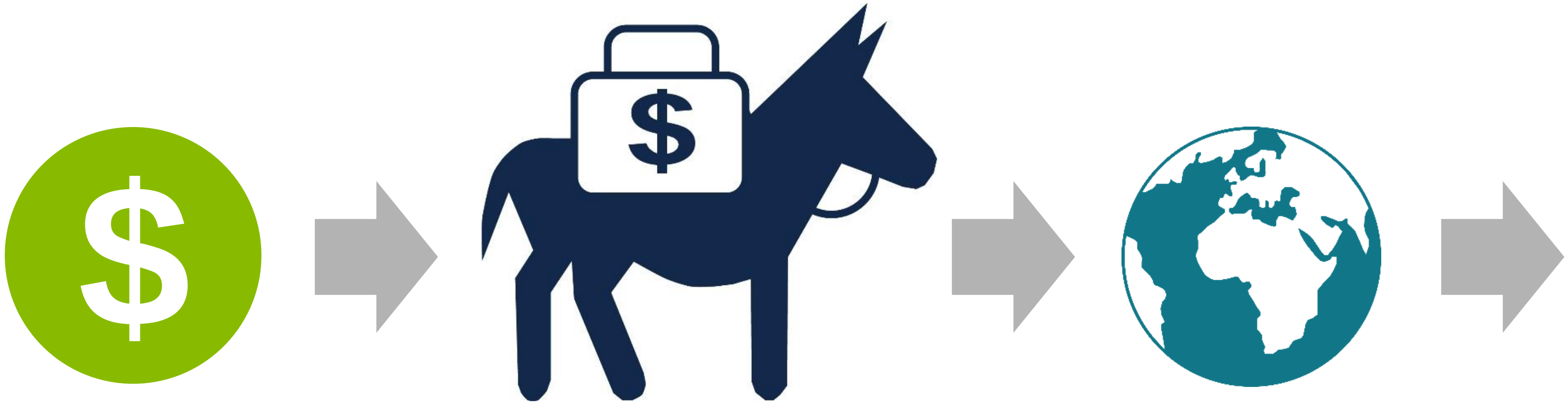
Cyber Fraud – Means of Deception

- User opens email or clicks banner ad and the malware's root kit is installed.



Cyber Fraud – Means of Deception

- Money is usually sent to mules, who are recruited to accept Wire Transfers and/or ACH payments. The mules then withdraw the funds and wire the money outside the US.



Cyber Fraud - Helpful Practices to Avoid these Schemes

- Dual Control for transaction initiation
  - Wire and ACH
  - E-mail Alerts for Approvals
- Daily Reconcilement
- Secure Environment
  - Dedicated PC and/or limit web surfing
  - Firewall, Anti-virus, Anti-malware, Anti-spyware
- Use strong passwords and protect them
  - No birthdays or pet names
  - Change every 60 days
- Don't click on links in suspicious e-mails

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
- Review cybersecurity insurance coverage
- Create a robust vendor management program
- Document a detailed fraud response plan
- Establish internal controls like a call-back procedure for changes in payments

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 (Stop Ransomware)	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

REGIONS

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