Corporate Finance Fraud, Prevention and Awareness

Randy C. Wilborn, CTP – Vice President, Regions Bank Treasury Management Products and Services

January 20, 2021
AASBO – Alabama Association of School Business Officials
Monthly Webinar Series

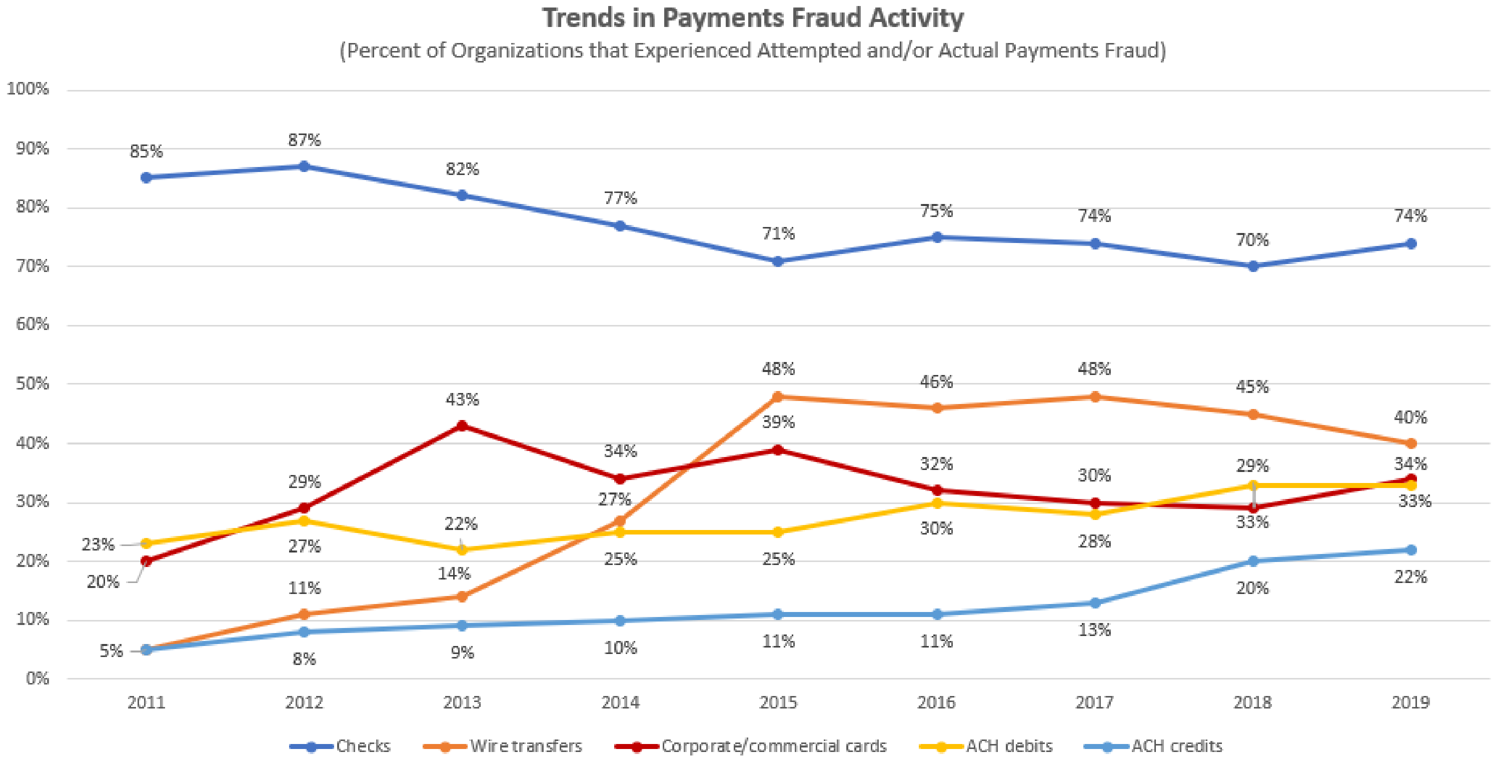
REGIONS

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.

Agenda

- Background
- Payments Fraud Schemes
  - Bookkeeper Fraud
  - Business E-mail Compromise
  - Ransomware
  - Cyber Fraud
  - Check Fraud
  - Electronic Payments Fraud
- Fraud Prevention Solutions
- Questions

Payment Fraud Trends



Trends in Payments Fraud Activity

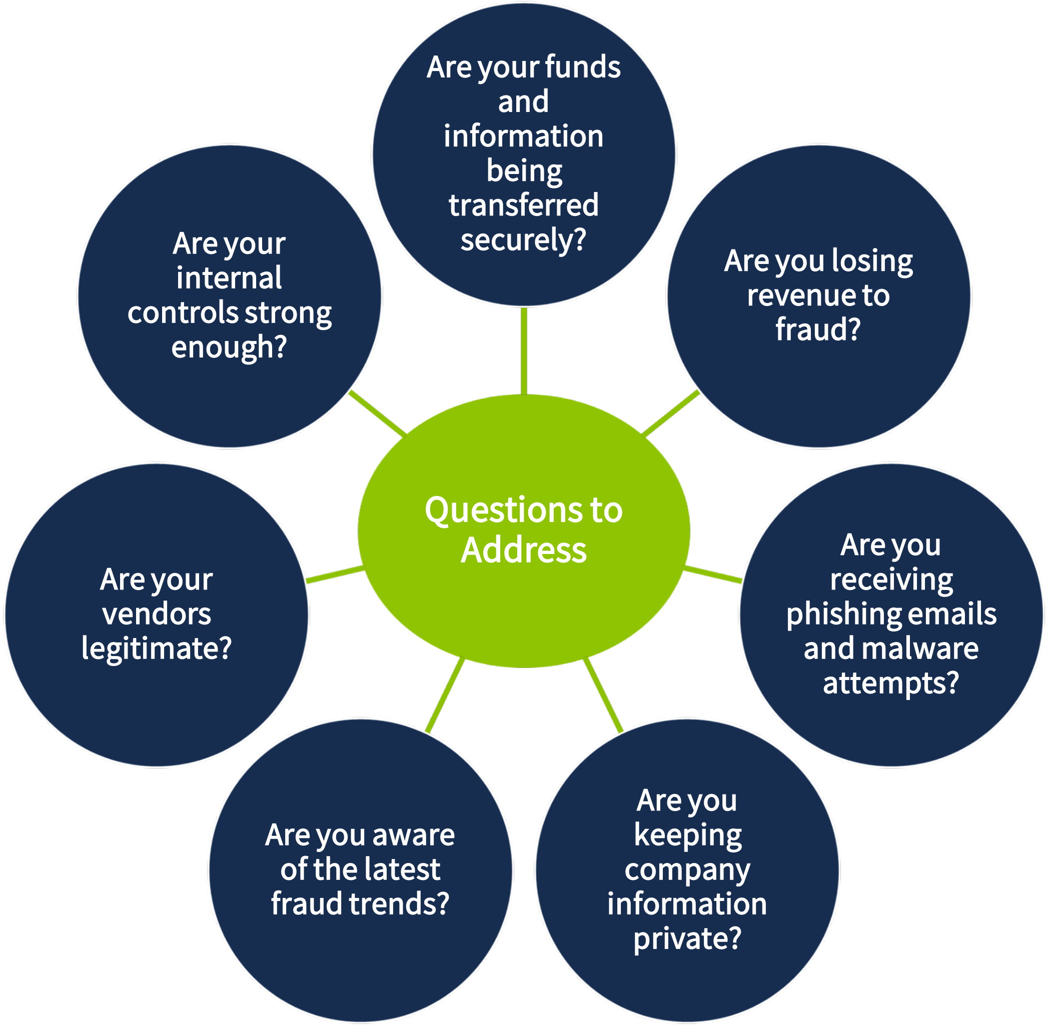
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)

Source: 2020 AFP Payments Fraud & Control Survey

Why target commercial accounts?

- High dollar balances in checking accounts
- Can move money quickly
  - Real-time using Wire Transfer
  - “Near” real-time using ACH
- Commercial computers represent a target rich environment for other corporate information

Education and Awareness are Key to Prevention



Questions to Address

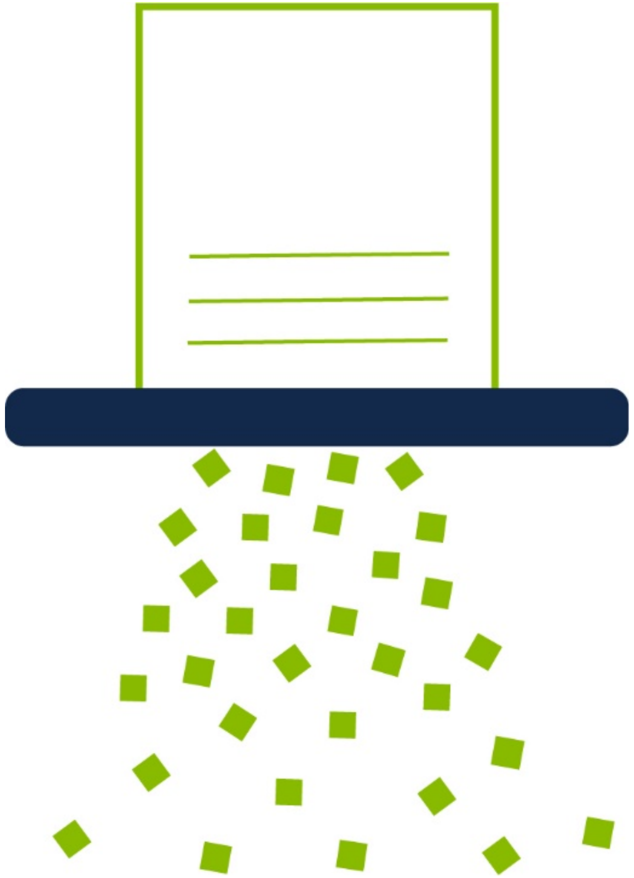
- Are your funds and information being transferred securely?
- Are you losing revenue to fraud?
- Are you receiving phishing emails and malware attempts?
- Are you keeping company information private?
- Are you aware of the latest fraud trends?
- Are your vendors legitimate?
- Are your internal controls strong enough?

Document Protection

- To help avoid embarrassment and/or fraud loss, confidential trash must be handled and destroyed properly

- Business wide process needs to be implemented and enforced

- In house process or outsourced vendor can both work



Payments Fraud Schemes

- Bookkeeper Fraud
- Business E-mail Compromise
- Ransomware
- Cyber Fraud
- Check Fraud
- Electronic Payments Fraud

Bookkeeper Fraud

Bookkeeper Fraud

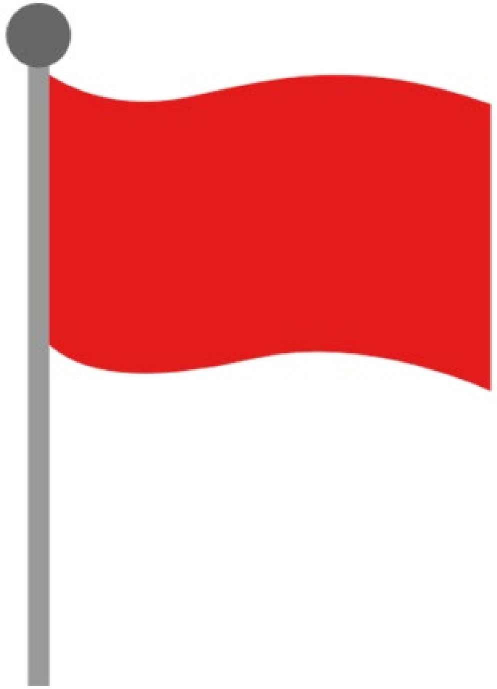
- Arises when full authority has been given to a single employee to issue and reconcile payments, especially associated with checks
- 85% of all fraud is perpetrated by a trusted employee
- Creates bogus accounts payable/vendors and generates payments
- Opens bank account in similar name to business 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

Business Email Compromise (BEC)

Business Email Compromise (BEC)

- Fraudster targets employees with access to company finances
- Tricks them into making wire transfers to bank accounts thought to belong to trusted partners
- The money ends up in accounts controlled by the criminals

BEC Iterations

1. **Executive email intrusion:** email compromise resulting in a fraudulent payment request from a company executive
2. **Vendor email intrusion:** email compromise that results in a fraudulent request to change payment terms or criteria
3. **Employee email intrusion:** email compromise resulting in fraudulent payment requests being sent to vendors involving a change in payment criteria

BEC – Means of Deception

- **Phishing** – bogus emails prompt victims to reveal confidential information
- **Social Engineering** – phone calls/conversations to gain trust
- **Identity Theft** – deliberate use of someone’s identity for financial gain
- **E-mail Spoofing** – slight variations on legitimate email addresses
- **Malware** – infiltration of networks

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

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.

Ransomware - Means of Deception

- Infected software applications
- Infected external storage devices
- Compromised websites

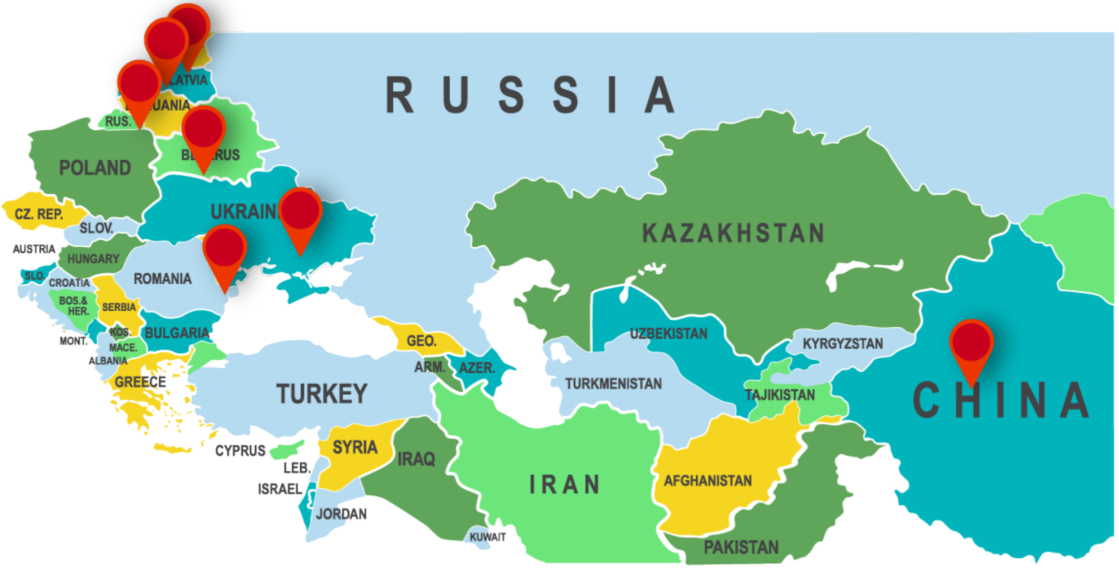
Ransomware - Helpful Practices to Avoid these Schemes

- Frequently back up data
- Remove unnecessary programs
- Update security software including antivirus software
- Avoid clicking on email links from strangers

Cyber Fraud

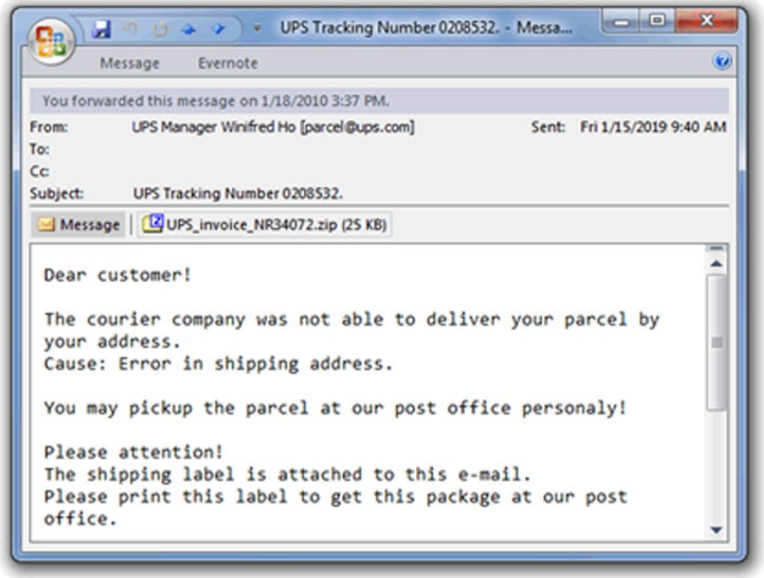
Cyber Fraud - Where are the bad guys?

- Ringleaders and Malware authors are in Russia and Ukraine
- Software is for sale on the Darknet (underground internet) – DHS/FBI says darknet is 90% of the Internet
- Command and Control servers along with botnet servers are for rent
- These are used to disperse the malware
- The actual thief may be in the house or office next door



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 directl
- Immediate goal may be ransomware or theft of intellectual proper



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

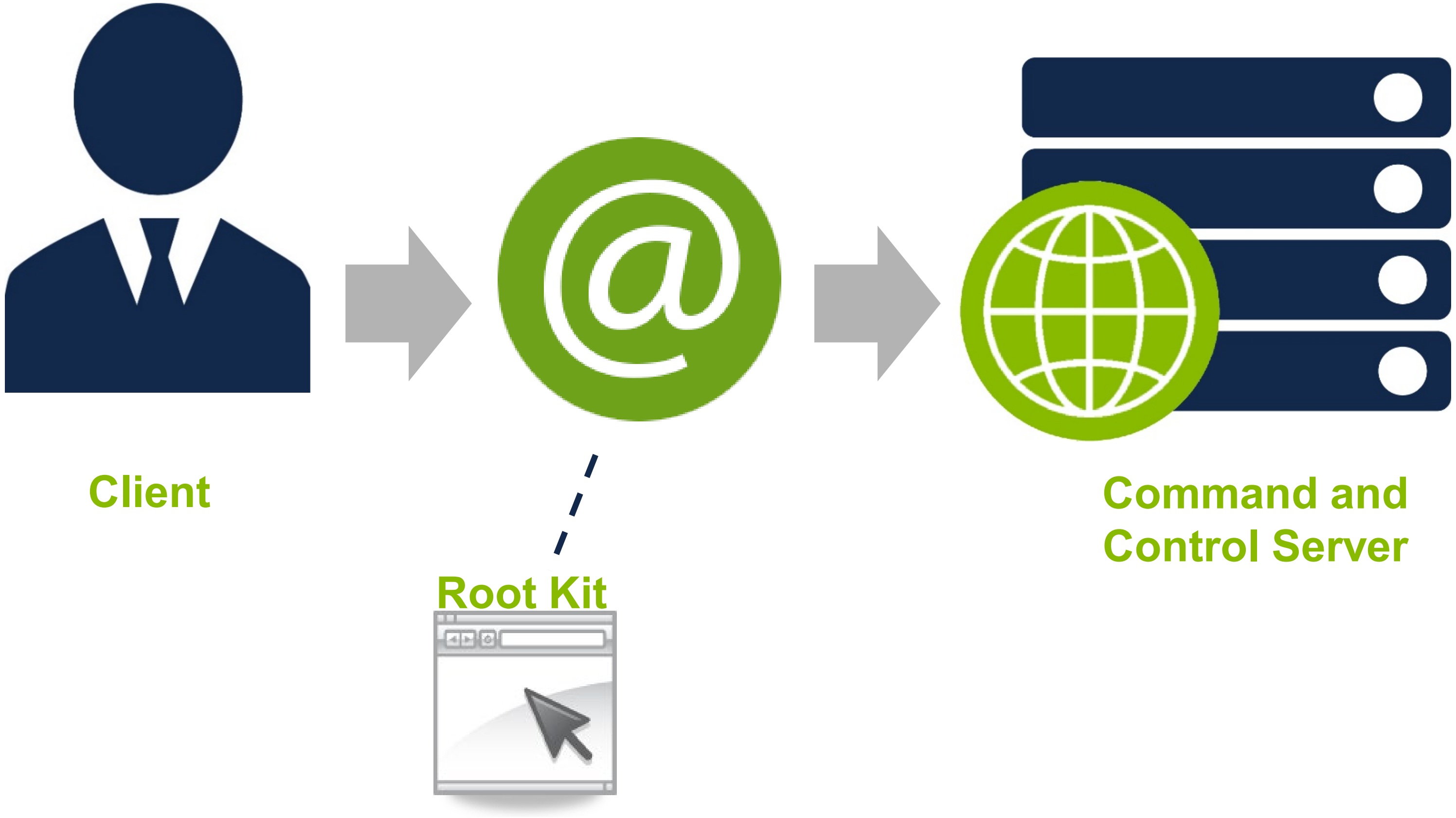
From: UPS Manager Winifred Ho [parcel@ups.com] Sent: Fri 1/15/2019 9:40 AM
To:
Cc:
Subject: UPS Tracking Number 0208532.

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.
```

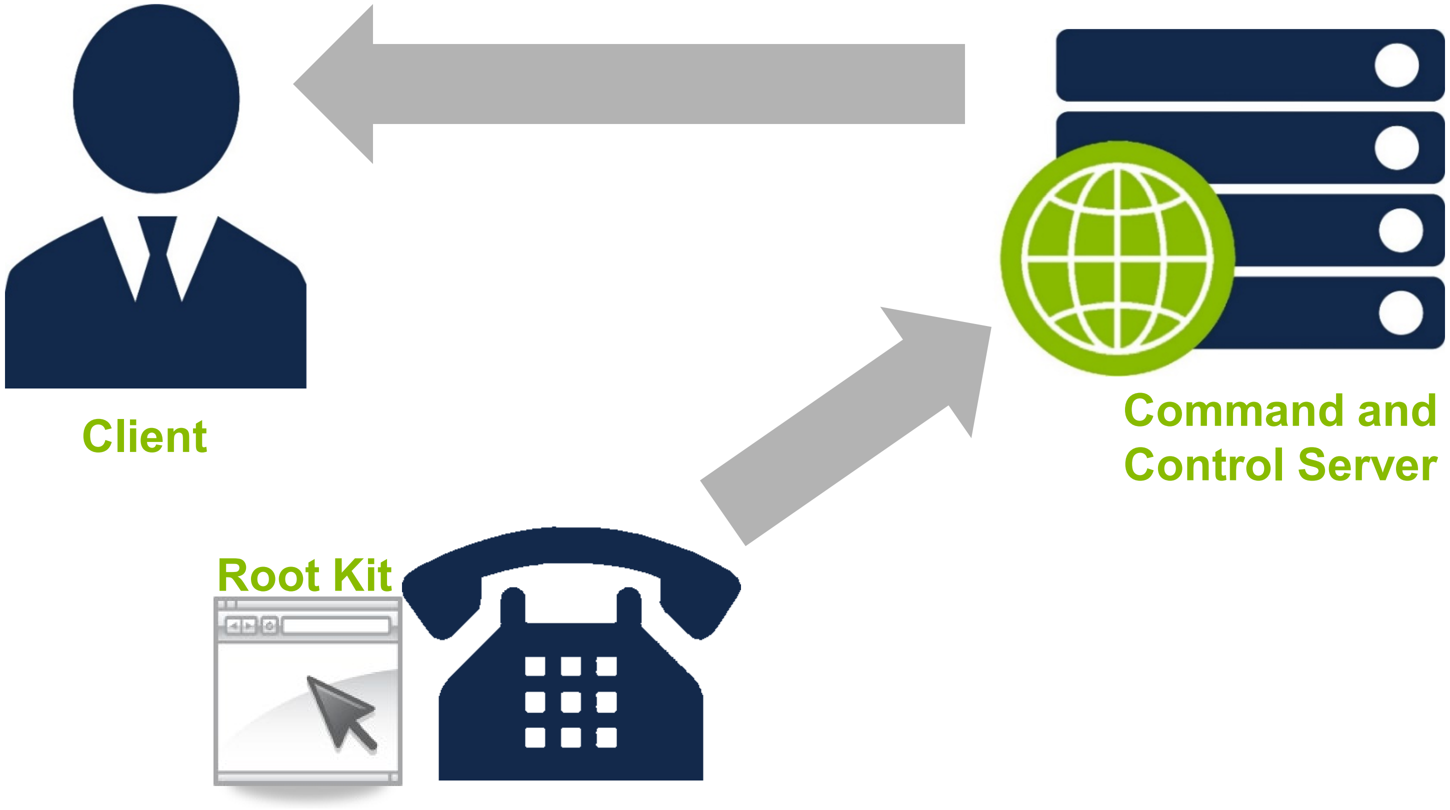
Cyber Fraud – Means of Deception

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



Cyber Fraud – Means of Deception

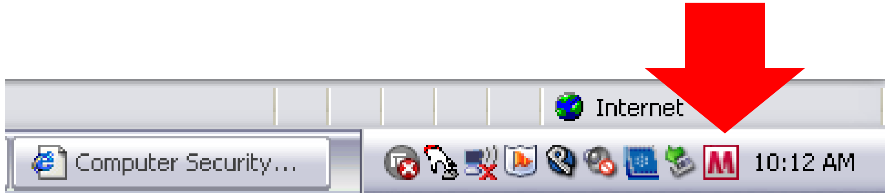
- Root kit installs itself deep within the client's operating system.
- Root kit "phones home" across the internet to a Command and Control server. It tells the Command and Control server "I am here. Send me the rest of the malware payload."



Cyber Fraud – Means of Deception

- Malware disables anti-virus software. (The indicator in the system tray isn't necessarily affected, so the user doesn't know that anti-virus has been disabled.)

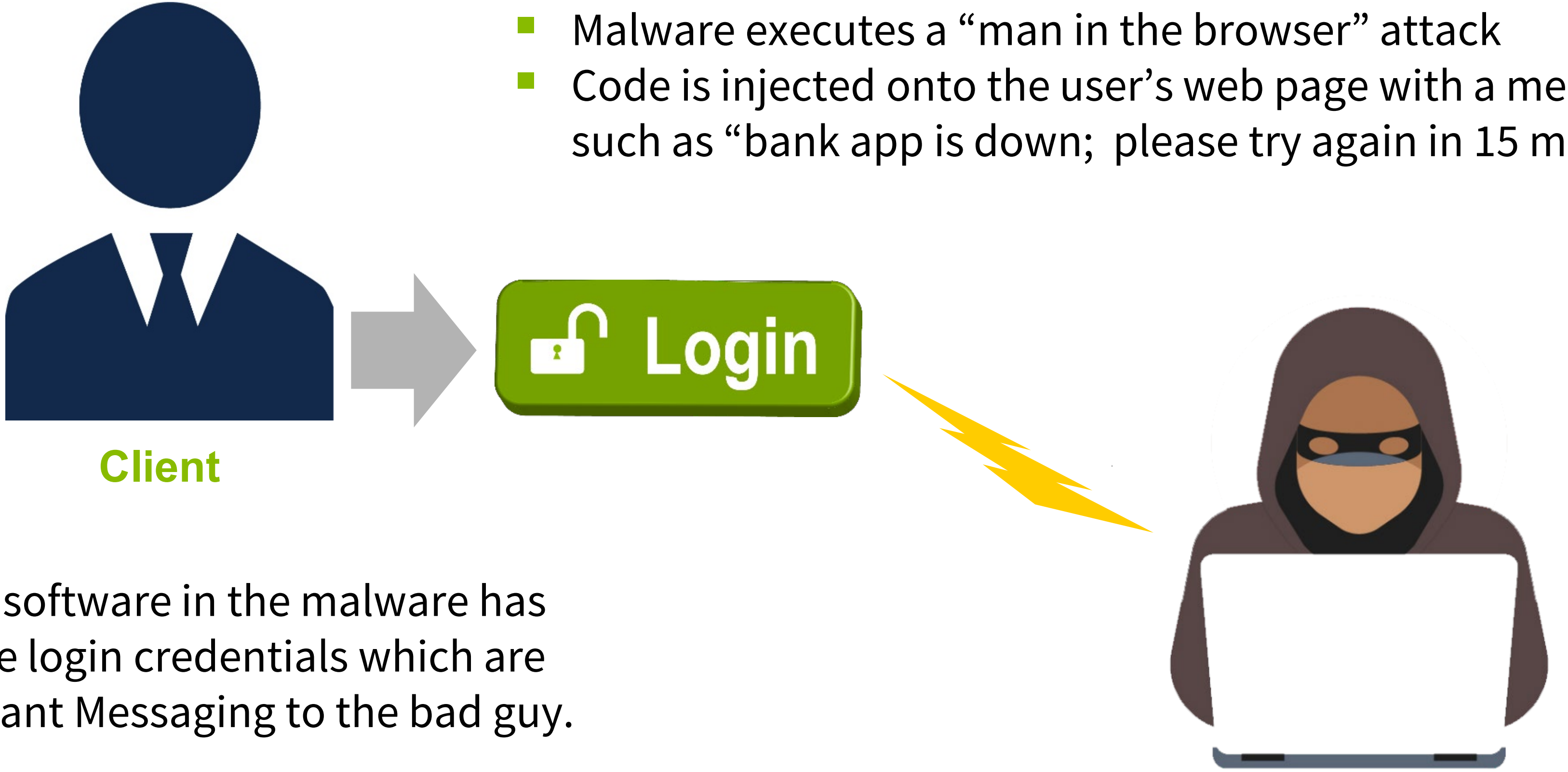
Client



Cyber Fraud – Means of Deception

- The malware waits for the user to connect to a financial institution. As soon as that happens, an instant message is sent out to the criminal, alerting him that the user is online.

- User enters login credentials and token pin if used
- Malware executes a “man in the browser” attack
- Code is injected onto the user’s web page with a message such as “bank app is down; please try again in 15 minutes”

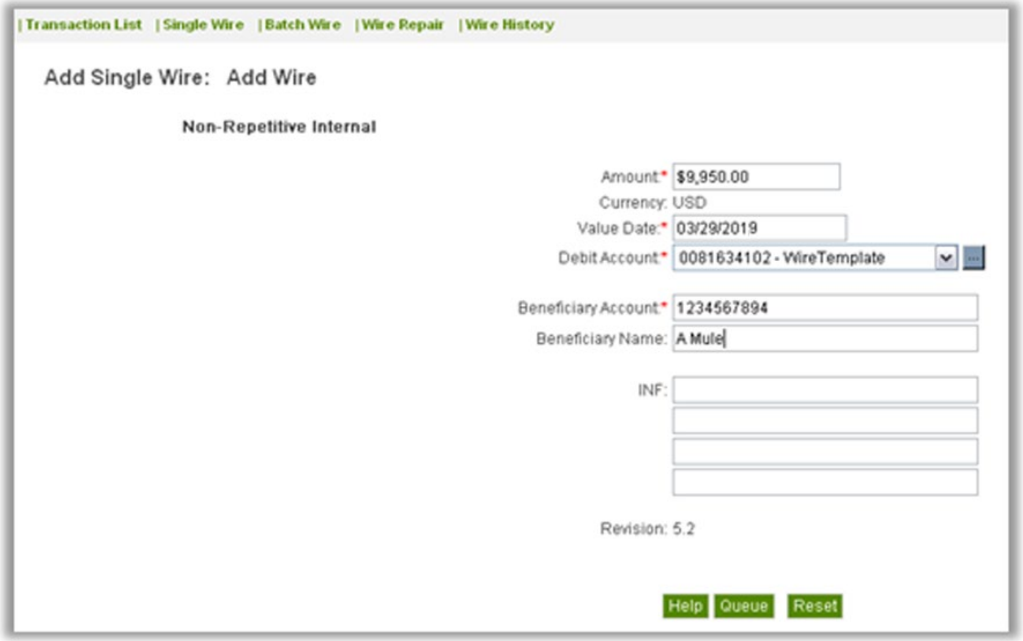


- Key logging software in the malware has captured the login credentials which are sent via Instant Messaging to the bad guy.

Cyber Fraud – Means of Deception

- Before the 60 second expiration of the one time token pass code, the criminal logs on to the banking app.

- He now has the ability to do everything that the user is entitled to do.



Add Single Wire: Add Wire

Non-Repetitive Internal

Amount:* $9,950.00
Currency: USD
Value Date:* 03/29/2019
Debit Account:* 0081634102 - WireTemplate

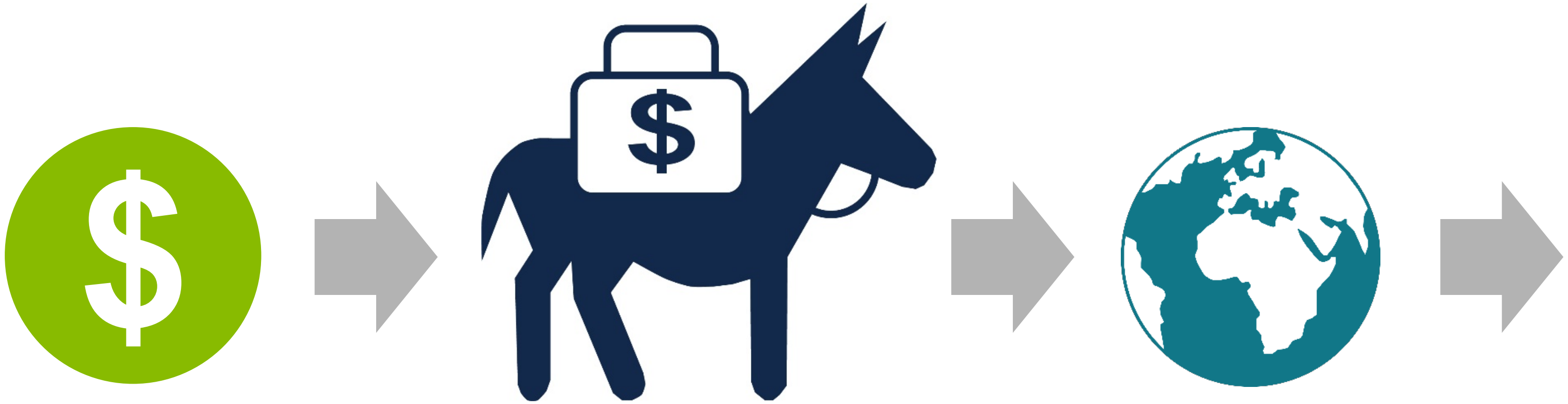
Beneficiary Account:* 1234567894
Beneficiary Name: A Mule

INF:

Revision: 5.2

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

Check Fraud

Check Fraud – Means of Deception

Counterfeit checks are by far the most prevalent check fraud mechanism

- **Forgery**
  - Unauthorized maker's signature – produced manually or via fax
  - Unauthorized endorsements/payee claims
- **Alteration**
  - Change to face or back of checks
  - Results in non-conforming payments instructions/endorsements
- **Counterfeit**
  - Illegal, unauthorized printing of checks
- **Improper/missing endorsements**
  - Endorsement is missing or doesn't confirm to the way check was drawn
- **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

Paper Payments Helpful Practices

- Convert paper payments to electronic.
- Securely store check stock, deposit slips and bank statements then destroy securely.
- Place stop payments on any check that are outstanding over a period of time.
- Utilize Positive Pay services for checks and ACH
- Employee Education

Electronic Payments Fraud

Electronic Payments Fraud

ACH Fraud

- On-line or verbally initiated single act – Fraudulent debit of an unknowing party's account to credit a secondary party. Examples: Bill pay, Payroll Scam, etc.
- Mass targeted scams – Manipulation of individuals into generating transactions themselves, to benefit a secondary party.
- Account takeover – Attempts in which a victim's electronic credentials are compromised and used to initiate unauthorized transactions.

Wire Fraud

- **Hacking/ Account Takeover** – Attempts in which a victim's electronic credentials are compromised and used to initiate unauthorized transactions.
- **Identity Theft –** Utilizing unauthorized identity documents to validate or initiate a fraudulent transaction.
- **Embezzlement –** Unauthorized movement of funds or property by a person in a position of trust.
- **Wire Scam –** Placement of illegally obtained funds with a legitimate party with the intent of using the legitimate party to move funds to a secondary party.

Electronic Payments Fraud- Helpful Practices to Avoid these Schemes

Wire Fraud Risk

- Use of dedicated PC – strict access
- Dual control/Segregation of duties
- Reduce number of non-repetitive wire transfers
- Review current day reporting from banks
- Subsequent daily review using prior day reporting

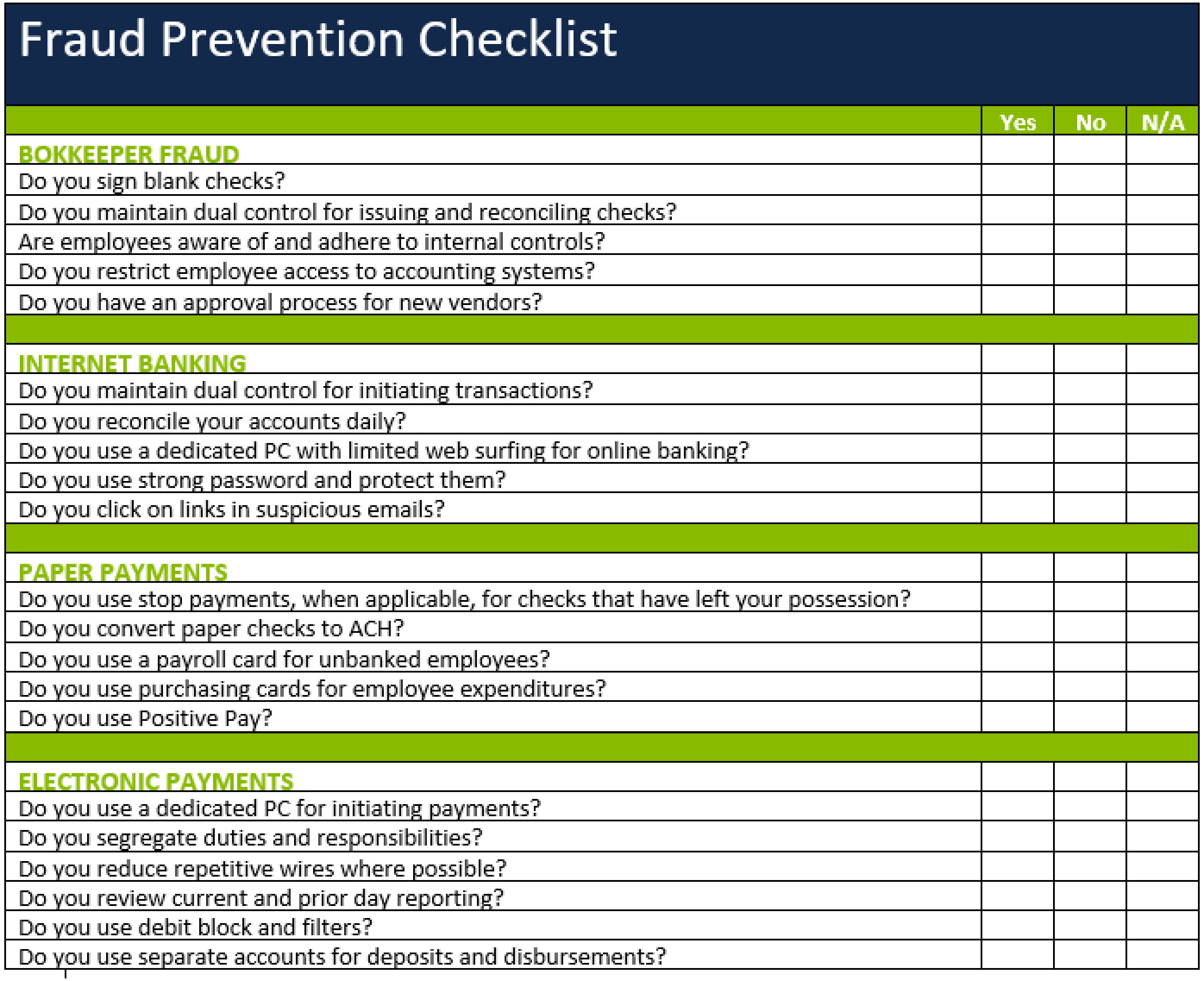
ACH Fraud Risk

- Use of debit blocks and debit filters
- Use of separate accounts for deposits versus disbursement
- ACH Positive Pay and decision capability

Purchasing Cards

- Use MCC Groups
- Set monthly, daily, and single transaction limits
- Limit online maintenance access

Fraud Prevention Checklist



Fraud Prevention Checklist

	Yes	No	N/A
BOKKEEPER FRAUD			
Do you sign blank checks?			
Do you maintain dual control for issuing and reconciling checks?			
Are employees aware of and adhere to internal controls?			
Do you restrict employee access to accounting systems?			
Do you have an approval process for new vendors?			
INTERNET BANKING			
Do you maintain dual control for initiating transactions?			
Do you reconcile your accounts daily?			
Do you use a dedicated PC with limited web surfing for online banking?			
Do you use strong password and protect them?			
Do you click on links in suspicious emails?			
PAPER PAYMENTS			
Do you use stop payments, when applicable, for checks that have left your possession?			
Do you convert paper checks to ACH?			
Do you use a payroll card for unbanked employees?			
Do you use purchasing cards for employee expenditures?			
Do you use Positive Pay?			
ELECTRONIC PAYMENTS			
Do you use a dedicated PC for initiating payments?			
Do you segregate duties and responsibilities?			
Do you reduce repetitive wires where possible?			
Do you review current and prior day reporting?			
Do you use debit block and filters?			
Do you use separate accounts for deposits and disbursements?			

Questions?

The information presented is general in nature. Regions reminds its customers that they should be vigilant about fraud and security and that 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 that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit regions.com/stopfraud, or speak with your Treasury Management Officer for further information on how you can help prevent fraud.

REGIONS