U.S. Customs and Border Protection (CBP) aims to approach supply chain security comprehensively. To that end, CTPAT added requirements to help address the most prevalent and evolving security threats. The new and updated criteria are related to **cybersecurity**, the protection against agricultural contaminants, **the prevention of money laundering** and terrorism financing, and the expansion of security technology.

# Cyber Security Awareness Briefing

Are You Prepared?

May 2019

# For Your Information

This presentation is for informational purposes only. We recommend that your business also obtain data security and anti-fraud advice from experts who are familiar with your business' information security controls. While this presentation will provide you with suggestions on controls, best practices, and risk management, these recommendations cannot replace the services of dedicated data security and anti-fraud experts with an in-depth understanding of your business and operational infrastructure.

Nothing in this presentation should be considered legal, accounting or tax advice.

# Cyber-Attacks Are Hitting Home

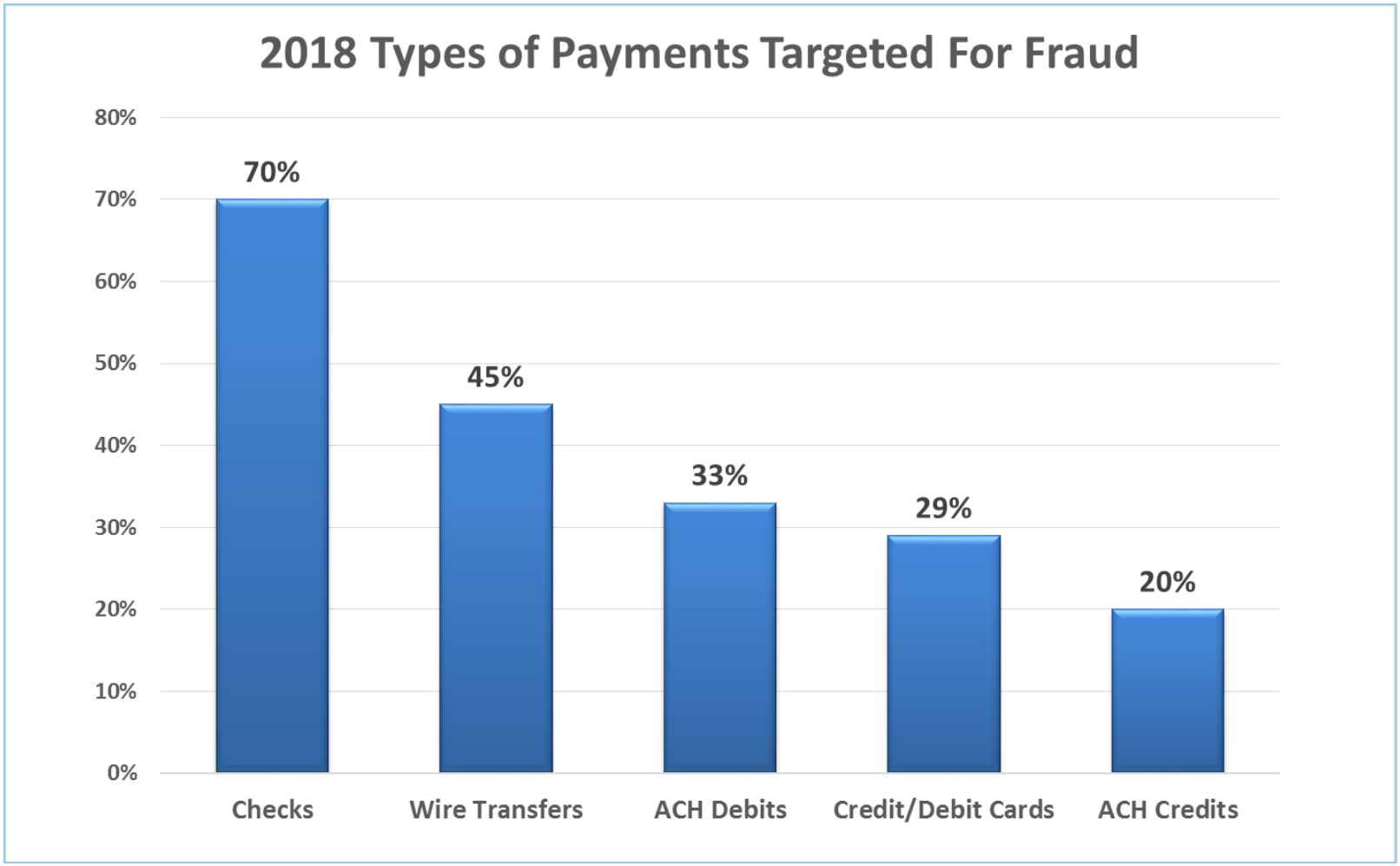
## Business executives expect B2B payments fraud scams to grow

- **FBI: #1 Cybercrime is Business Email Compromise**
  - Business Email Compromise (BEC) fraud doubled to $1.2 billion
- **82% of businesses were exposed to a payment fraud attack**
  - After checks, wire transfer was the 2nd most popular method of payments fraud
- **ACH is the fastest growing payments fraud**
  - 33% of organizations had ACH debit fraud and 20% had ACH credit fraud, each up several percentage points from the prior year

Sources FBI IC3 Statistics
AFP 2019 Payments Fraud and Control Survey Report

# Payment Fraud Activity Continues To Grow

82% of businesses had attempted or actual payment fraud



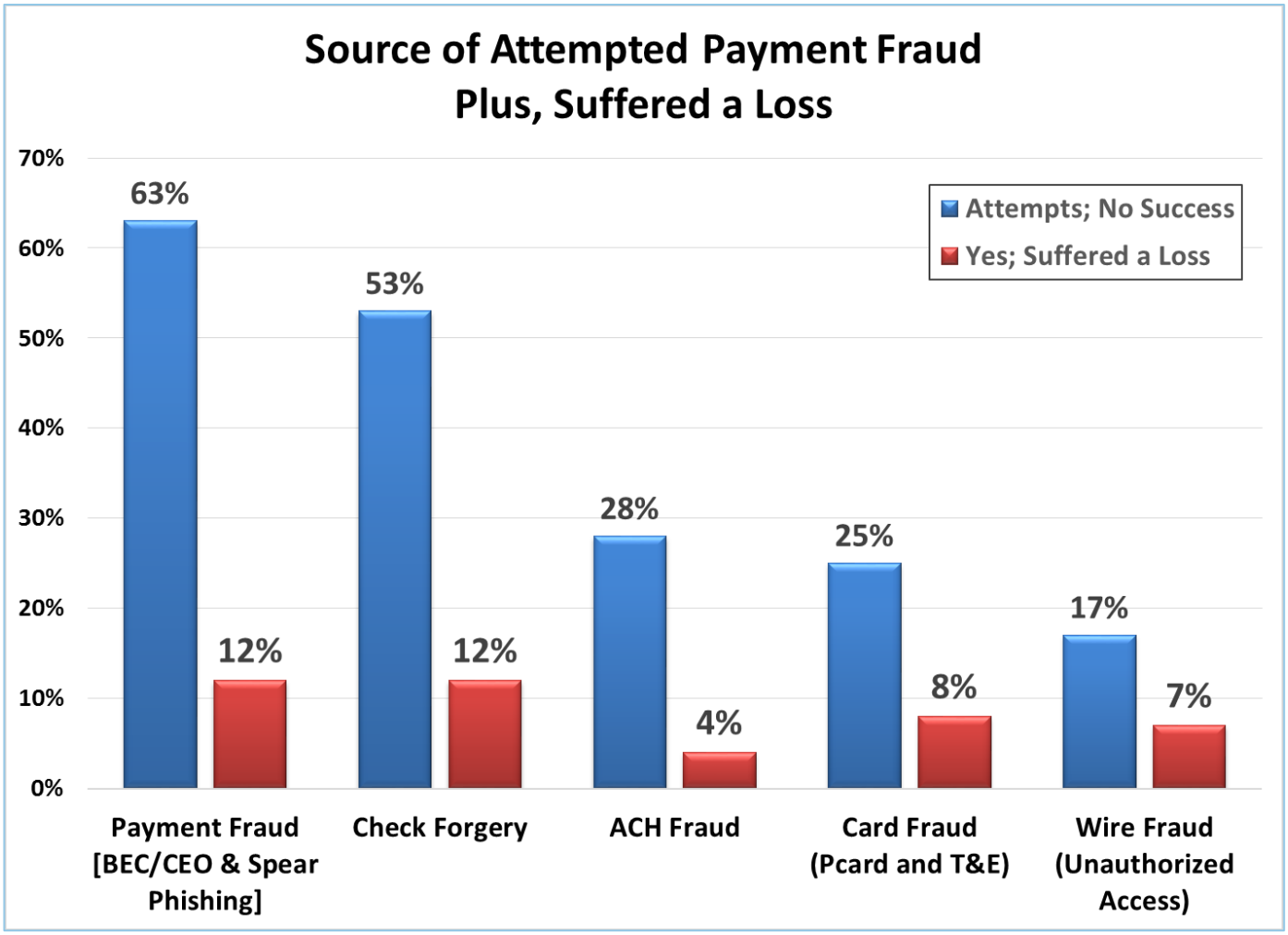

Source: AFP 2019 Payments Fraud and Control Survey Report



HANCOCK WHITNEY

# Top Fraud Targets

Payment fraud in the last two years




[1] Source: Strategic Treasurer, Fraud & Security in 2018



HANCOCK WHITNEY

# The Threats Are Real

Corporates are very aware that cybercrime risk is growing

- **84%** of corporates indicate the threat of cyber & payment fraud has *increased* in the past year.
- **41%** of corporates plan to invest in security controls for *payment operations* in 2019.
- **33%** of firms were hit with at least one fraud attempt that *originated from a completely unknown source*.

Despite increased awareness and spend, corporations have proven themselves largely unprepared for a more organized, strategic and persistent threat.

Craig Jeffery, Founder
*Strategic Treasurer*

Source: 2018 Treasury Fraud & Controls Survey

# The Rise of Cybercrime-As-A-Service

Data, files, e-mails can all be found on Dark Web

"Cybercrime-as-a-service — along with malware-as-a-service or fraud-as-a-service — has opened a wide digital door to anyone looking to score a quick, illicit buck on the internet."

-- Charles Cooper, Cybersecurity Insights

# Cybercrime Threats Are Pervasive

Crooks can search underground online sites for data

**The cost of cybercrime is cheap**

- Want to send phishing e-mails?
  - Cost = $1,000 for 3 million from a Russian hacker service
- Need a ransomware kit?
  - Cost = $1,000 for a one month rental
- Access to a valuable e-mail address?
  - Cost = $150 to $500 for access to a corporate finance department


***CEOs, board members and owners must manage cybersecurity risks through proactive engagement.***



HANCOCK WHITNEY

# Many Cyber Attacks Start By Phishing

Employees create financial risk unintentionally


"Phishing is really an easy way to perpetrate an attack. Creating a way to break through a complex security system takes time and money.

So, why bother when you can simply trick a victim into giving up information or clicking a link?"

-- Satti Charles, IBM Trusteer



HANCOCK WHITNEY

# Example: Fake Email Phishing for a Target

**From:** Delivery Notification <do-not-reply@en.expressparcel.com.au>
**Sent:** Thursday, November 30, 2017 1:56 PM
**To:**
**Subject:** Package Undeliverable

**Importance:** High

The Bad Guy is trying to get you to download his malware....

## Delivery Notification

**Order:** SGH-9226-99950127

**Dear J**

Your parcel has arrived at the post office. Our courier attempted but was unable to deliver the parcel to you.

To receive your parcel, please go to the nearest office and show this receipt.

**GET AND PRINT RECEIPT**

Don't Click Here!

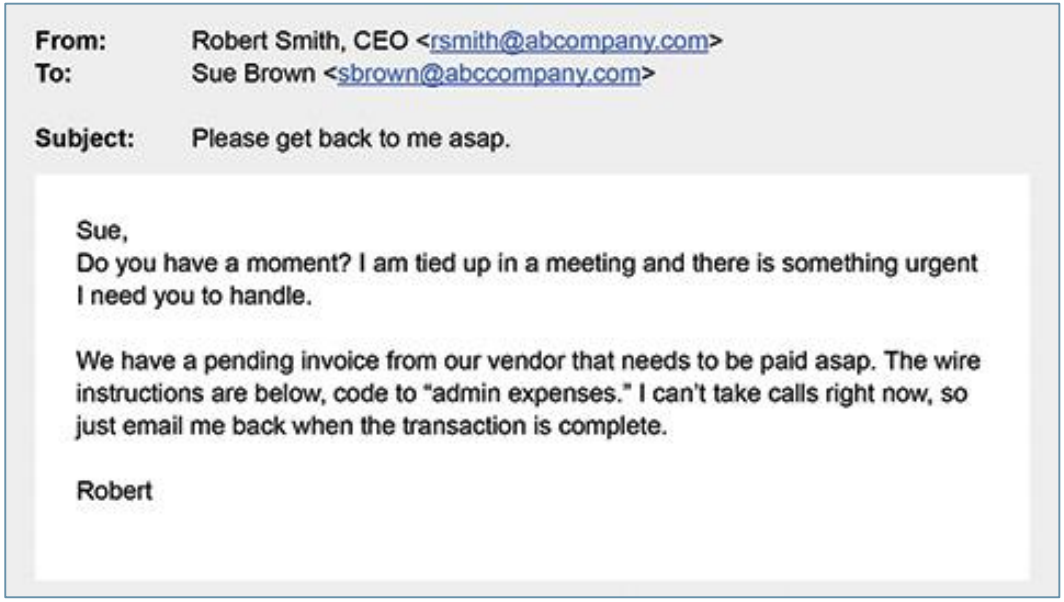


HANCOCK WHITNEY

# What Is Phishing?

It attacks your organization in multiple ways

- Phishing schemes are cybercrimes in which scammers send a message to confuse or trick someone into sending money, data or something of value to the crook.
- 83% of Infosec Pros said their organization had phishing attacks in 2018



**From:** Robert Smith, CEO <rsmith@abcompany.com>
**To:** Sue Brown <sbrown@abccompany.com>

**Subject:** Please get back to me asap.

Sue,
Do you have a moment? I am tied up in a meeting and there is something urgent I need you to handle.

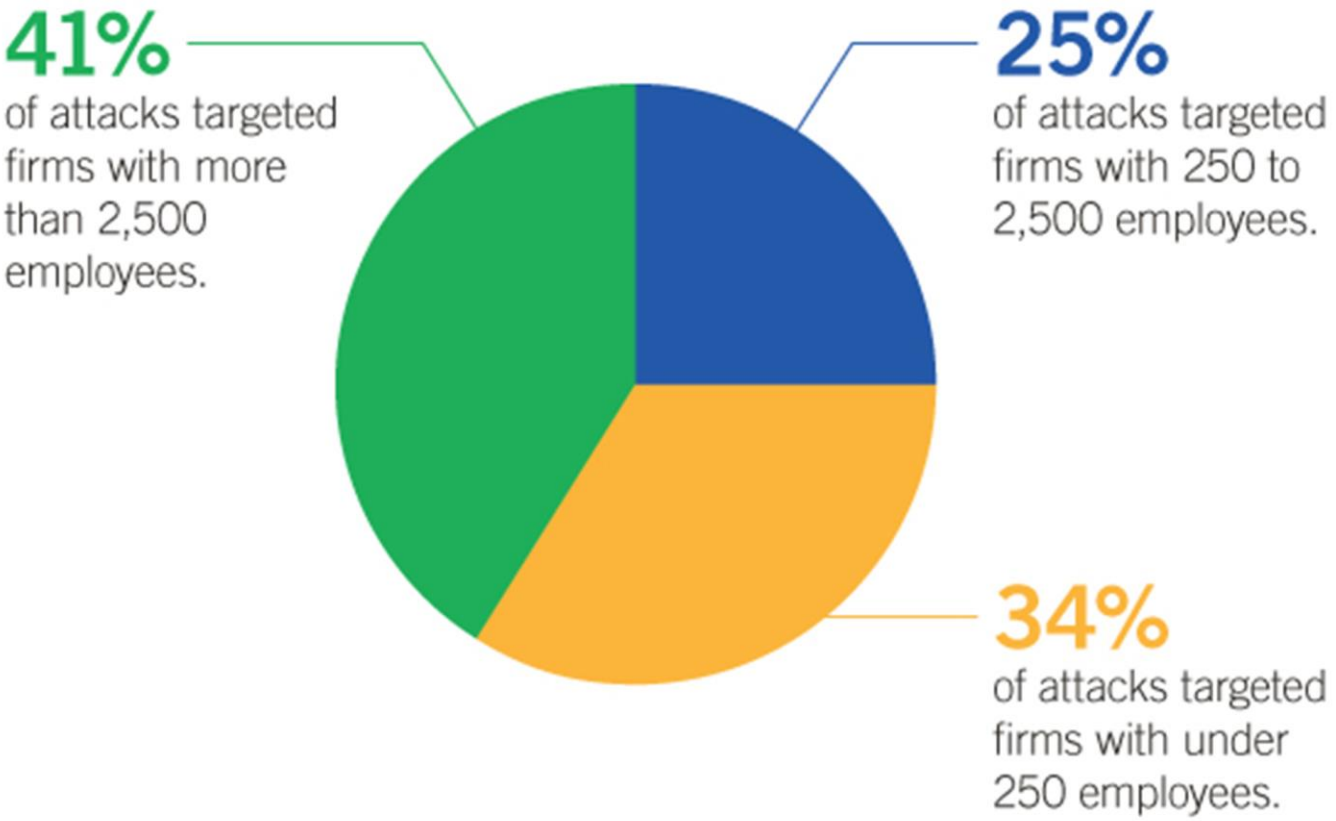
We have a pending invoice from our vendor that needs to be paid asap. The wire instructions are below, code to "admin expenses." I can't take calls right now, so just email me back when the transaction is complete.

Robert

2019 State of the Phish Report, proofpoint.com

# Myth: Only Large Firms Are At Risk

60% of spear-phishing attacks target smaller businesses




Source: Symantec: Internet Security Threat Report



HANCOCK WHITNEY

# Most Small Business Lacks Awareness

Only 13% said they experienced cyber-crime

**Small business are unaware of the varied types of cybercrime**

Once they understood the different types of cyber-attacks and the wide scope of cyber-crime, the percentage of firms that said they had fallen victim to a cyber-crime tactics increased.

**58% found out they were victims**

Source: PYMNTS website, October 12, 2017 “When Small Businesses Don’t Realize They’re Cyber-Attack Victims"

# Common Types Of Cybercrime

## Phishing

Phishing sends a malicious email to individual(s) or mass users of any business by impersonating a known individual or a business partner or a service provider.

## Vishing

Vishing refers to phishing done over phone calls.

## Smishing

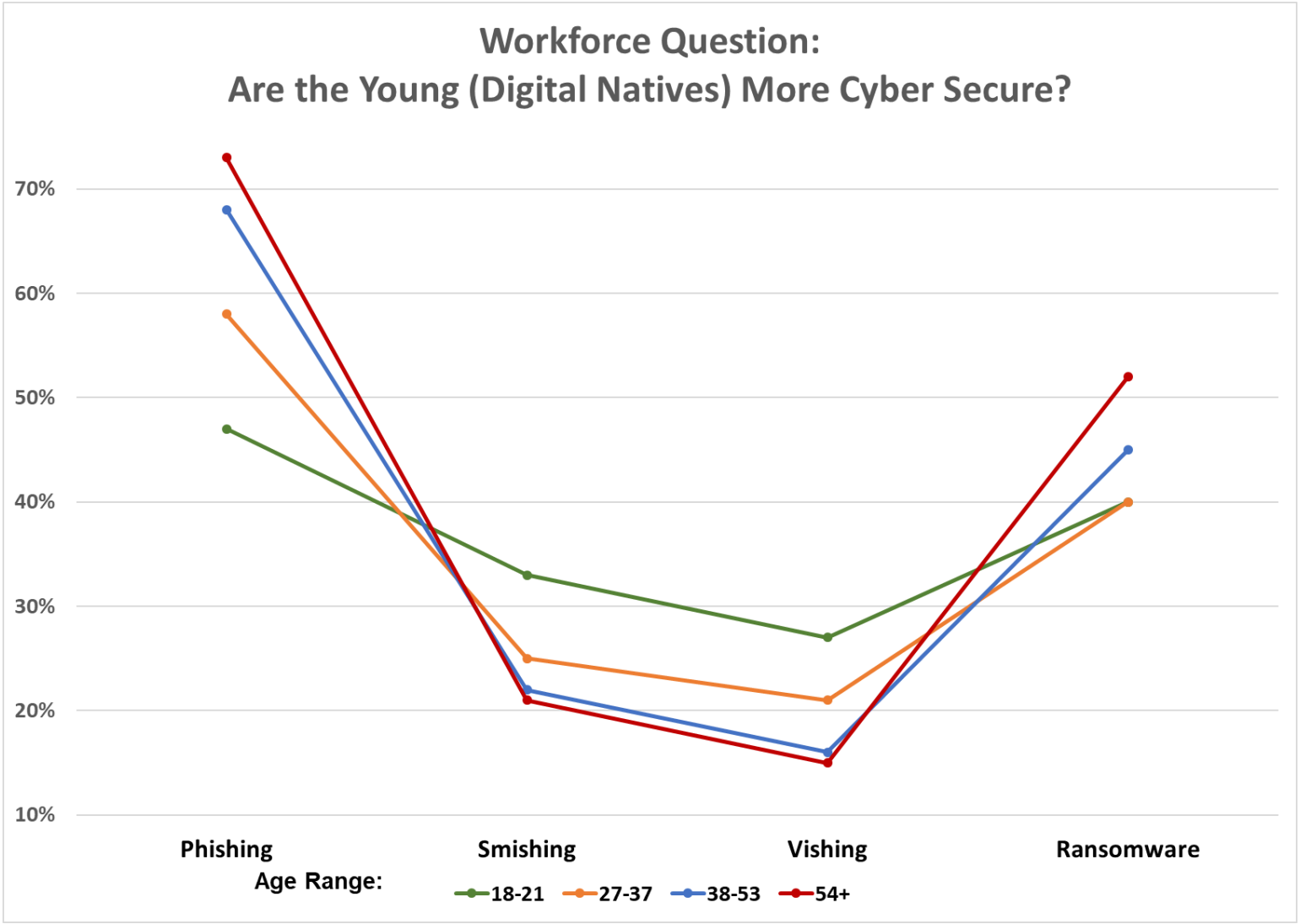
Smishing uses social engineering techniques to acquire personal information such as passwords and details by masquerading as a trustworthy entity

## Ransomware

Ransomware is a form of malware, or malicious software that takes over your computer, threatens you with harm, usually by denying access to the system or data.

2019 State of the Phish Report, proofpoint.com

# What % Understand the Meaning Of The Threat?




2019 State of the Phish Report, proofpoint.com



HANCOCK WHITNEY

# Big Question

How can you recognize an attack if you don't know how it's coming?

**% who answered 'incorrectly' or 'I don't know" when identifying these schemes**

- Phishing = 35%
- Smishing = 83%
- Vishing = 80%
- Ransomware = 44%

2019 State of the Phish Report, proofpoint.com

# Cyber-thieves Use Clever Tricks

The designs have a sense of urgency & familiarity

## In e-mail fraud or BEC Attacks

- The 3 *most common lines* include:
  - Request (22%)
  - Urgent (21%)
  - Payment (15%)
- The response rate to phishing increases using personalized data:
  - First & last name
  - E-mail address

## Attacks with high 'fooled you' rates

- The *trickiest subject lines* include:
  - Toll Violation Notification
  - Your Unclaimed Property
  - Updated Building Evacuation Plan
  - Invoice Payment Required
  - Updated Org Chart
  - Urgent Attention (a notification requesting an email password change)

"Phishing Email Subject Lines That Reel Them In"; web-article by Aaron Jentzen, February 14, 2019 on proofpoint.com

# Top Cybercrime Is Spear-Phishing

Targets a weak security link: C-suite executives

**Business Email Compromise (BEC) or CEO Fraud**

***Attacks target people - the CEO & accounting staff***

- The attacker tricks your staff into thinking they've received an email from a boss or vendor or submitting a fake invoice for payment.
- The impostor requests a payment via wire transfer, ACH or check.
- Some cyber-thieves may request a copy of files with sensitive company data.

***Spear Phishing – The #1 Attack Method Targeting Businesses***

***Your employee unsuspectingly accommodates the request because it came from an executive or trusted source.***

# How Business Email Compromise Works

The Bad Guy researches the firm to spear-phish the attack

Using the CEO's email address, the Bad Guy sends an email to a targeted finance or corporate employee

Your employee receives an email from the 'CEO' instructing them to wire funds to pay for a business–related expense

Money is then wired or sent by ACH to an account controlled by the crooks

# Why does CEO Fraud Succeed?

- New Attacks Succeed Through Trickery

- **Simplicity - the payment request seems normal**
  - The crook asks victims to perform tasks that fall under their normal duties
  - The request looks authentic; contains wire details & amount
- **Leverages today's corporate culture**
  - Employees are available 24/7
  - They respond quickly when asked to solve a problem
  - Because of the requestor's position, the crook's instructions are followed with NO questions asked
- **Lack of Awareness – employees don't recognize the threat**
  - Companies that have trained on BEC and established new payment processing procedures tend to catch the scheme before it can succeed
  - These emails typically slip by traditional security solutions designed to detect attacks that exploit technology

# Multiple types of fraud attacks

Basic attack and variation off the scheme

- **CEO Fraud or BEC:** Attackers compromise a high-level business executive's email account and use it to impersonate the executive and send money-transfer requests to internal victims.
- **Bogus Invoice Scheme:** Attackers call or email a business that has a longstanding relationship with a supplier, pretending to be the supplier, and tries to trick you into wiring funds for invoices to the crook's account or they request invoice payments be sent to them or to a new address. You won't see the fraud until contacted by your vendor to request payment.
- **Payroll Diversion:** The bad actors snare login credentials from employees, and change direct deposit information.
- **Data Theft:** Attackers target personally identifiable information - including Social Security numbers - or employees' tax statements, in what's known as W-2 attacks. Such data is used for filing fake tax returns and identity theft.

# Does Anyone REALLY Fall For That Stuff?

Unfortunately, yes, they do

**Trend Micro's 'Cost of Compromise Study' estimates over 70% of CEOs, Directors and other C-Suite executives fell for the BEC scheme**

**The BEC losses are real –**

- Restaurant sent two wires overseas for: $223,000 – Funds lost
- Engineering firm sent a wire overseas: $85,000 – Funds lost
- Trucking firm sent wires: $145,000 – Funds lost
- Real Estate firm sent a wire: $49,000 – Funds lost

***Following your internal procedures can defeat the 'BEC' scam.***
***[We've had clients tell us their security procedures avoided a loss!]***

# Think Ahead for Cyber-Security

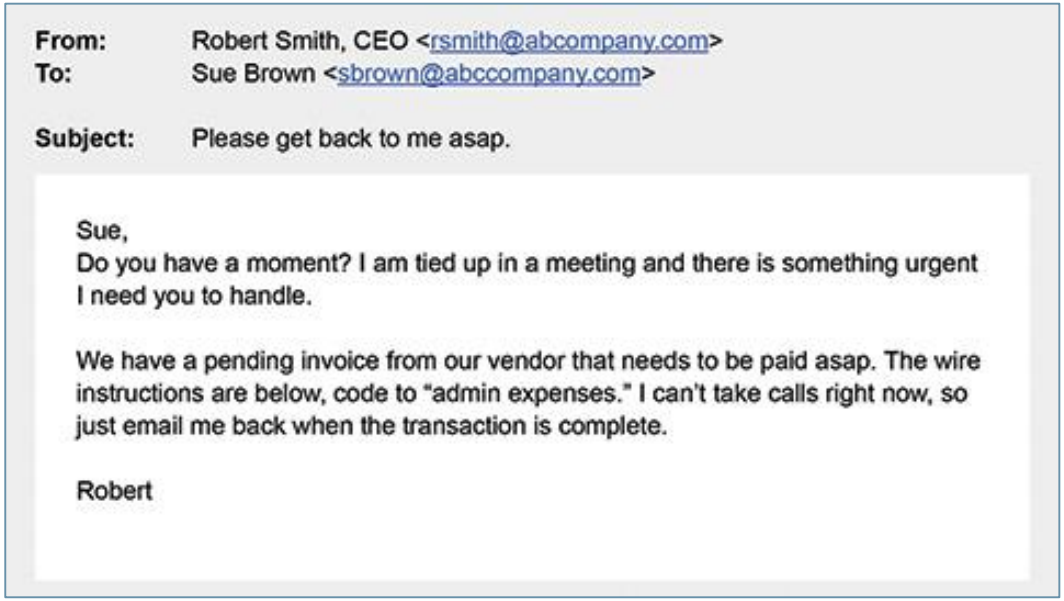
Stop Low-Tech Attacks with Low-Tech Defenses

| ✓ Verify | ✓ Review | ✓ Coach |
|---|---|---|
| ➢ Check for requests with secrecy or urgency | ➢ Confirm changes using a secure communications channel | ➢ Coach your employees to understand the threats |
| ➢ Check for consistency with previous wire or ACH payments | ➢ Confirm all out-of-office payment requests before processing | ➢ Coach your executives & staff to follow all internal procedures |
| ➢ Check all address change requests from vendors | ➢ Confirm payments over $X amount are OK; use dual approvals | ➢ Coach on the dangers of social media & internet |
| ***Establish and follow internal procedures for payment processing*** | | |

# Don’t Fall For The Fake Message

**Can Your Employees Spot A Fraudulent Email From Your CEO?**

After all, it doesn’t say “I’rn a fake”



**From:** Robert Smith, CEO <rsmith@abcompany.com>
**To:** Sue Brown <sbrown@abccompany.com>

**Subject:** Please get back to me asap.

Sue,
Do you have a moment? I am tied up in a meeting and there is something urgent I need you to handle.

We have a pending invoice from our vendor that needs to be paid asap. The wire instructions are below, code to “admin expenses.” I can’t take calls right now, so just email me back when the transaction is complete.

Robert

# Pop Quiz!

**Did you just read that phrase as “I’m a fake”?**

Really?
Because that’s NOT what it says.

[Let’s look again]

**You read the ‘rn’ as an ‘m’, but that represents a different email address and that’s how problems start**

# Old Scams Are Still Effective

The ‘Man-in-the-Middle’ Attack

**The crook tries to take over your account by hijacking your online banking session to initiate fraudulent payments.**

It happens everyday after you fall for the trickery by –

- **Being Curious:** Don’t click on a link and invite the crook in
- **Opening a Fake E-mail:** Carefully read the address behind the signature
- **Open an Attachment:** If you don’t know the source, don’t ‘click’

Malware allows the bad guy to see everything you do (and everything you type). When you enter a financial website, he harvests your User ID and Password so he can sign on as you!

# The ‘Man-in-the-Middle’ Attack

## Malware allows the cyber-crook to see what you are doing

The cyber-thief is after your login credentials so he can login as you.

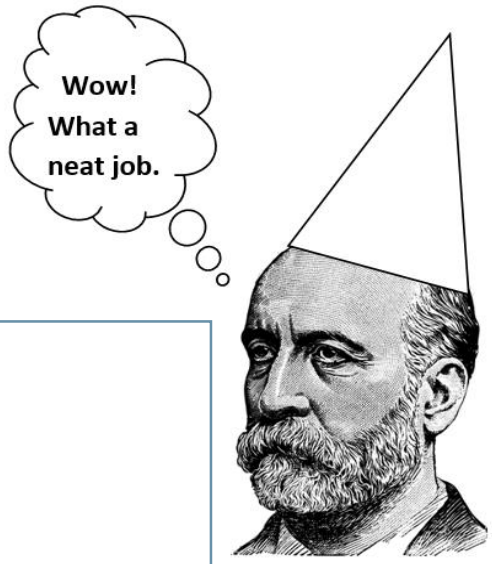
**What Does The Bad Guy Do After He Steals My Banking Credentials?**




HANCOCK WHITNEY

# The Story Starts Long Before You Were Involved

The bad guy puts a fake job posting on a search engine -




careerbuster.com

Click here for a groovy job!

Career Opportunity:

Transfer Agent for a Major Corporation

We will send Direct Deposits into your bank account.

You keep a 10% Commission

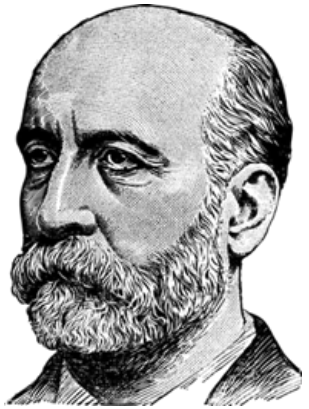
Wire Transfer the remainder to our business partner in the Ukraine.



HANCOCK WHITNEY

# Here's Where You Get Involved . . .

Using the credentials he stole from you, the Bad Guy logs into your bank . . . as YOU



He sends an ACH or wire transfer out of your account and into the account of the "Mule"

The Mule diligently wires 90% of the money to the bad guy's overseas account

# Five Red Flags of Wire Fraud

How to spot a wire fraud attempt

1. **The sender places a "rush" request:** Scammer insists the transfer take place immediately. Resist the hustle.
2. **The sender insists on communicating via e-mail only:** If you can't verify the request, wait.
3. **The requestor – the CEO or executive – is out of the office:** Always verify this request with another executive before sending any funds.
4. **The nature of the request or the amount is unusual or inconsistent with prior experience:** If it is out of the ordinary, definitely be suspicious.
5. **The email address or details in the request is wrong:** If it looks strange, don't fulfill the request without getting authorization.

# Fraud attacks compromise many payments

Cyber-thieves success rate range up to 30% of attempts

**Criminal Success Ratios By Fraud Type**

- Wire Fraud (system oriented): 29%
- T&E Card Fraud: 27%
- PCard Fraud: 24%
- Check Forgery: 19%
- BEC/Imposter Fraud: 16%
- ACH Fraud: 13%

**Most corporates take a piecemeal approach to security, only 29% have a formal fraud control framework**

2018 Treasury Fraud & Controls Survey Report

# Overview of Fraud Prevention

## Security Guidance

1. **Fraud Prevention is ongoing – not a ‘one-and-done’ effort**
2. **Recognize crooks are constantly evolving to become more sophisticated and calculated**
3. **Consider both technology and human components of your security infrastructure and don’t hesitate to update your controls when a problem is identified.**

2018 Treasury Fraud & Controls Survey Report

# Raise Employee Cyber-Security Awareness

Ask your employees to be a 'firewall'

- **Do you allow full access to the internet at the office, including social media sites (Facebook, etc.)?**
  - Recommendation – Isolate the online banking PC, block access to personal email & social media sites.
- **Ask each of your associates to be an "Employee Firewall"**
  - To be conscious of their online activities and location
  - To act as a protective barrier against unauthorized access to account numbers, user IDs, passwords and tokens.
  - To be aware of phishing attempts and how to counter them.
- **Don't Ignore A Hijacked Online Banking Session**
  - Be suspicious of dropped internet sessions immediately after entering login credentials. Call your bank!

# Employee Firewalls

## Security Principles for Employees

- **Educate Employees – learn about cyber-security**
  1. **Secure Your Workplace –** lock computers, desks, offices from unauthorized access
  2. **Be Cyber-Smart –** raise awareness of phishing scams
  3. **Report Issues –** when you encounter a security threat, know what to do and who to engage on the topic
  4. **Ask Questions --** Encourage all staff members to ask about a suspicious payment requests before processing the payment
  5. **Establish internal procedures for payment requests** – be ready before the attack comes

# Employee Firewall - Rules for Online Safety

- **Beware of "Free"**

  Download apps & software from safe sources **only**

  - Avoid links in emails, they may hide malware
  - Practice safe email – If you don't know the source – delete it
  - Avoid the friends and family email "Hey check this out!" hyperlink

- **Maintain The Latest Version Of Your System Software**
  - Keep up with updates & patches, especially for operating systems that are targeted for malware
  - Keep seldom-used programs updated (otherwise, delete them)

- **Use Strong Passwords**
  - 8 to 10 characters long, with letters, numbers and special characters. Avoid using the same password with multiple sites. Never allow your system to save passwords.

# Change The Payments Culture in Your Firm

Instead of thinking “ASAP”, think “As Securely As Possible”

**Require Dual Authorization for all wires over a specific amount**

Standardize the process to issue a wire or ACH

1. Never authorize a wire or ACH by e-mail request alone
2. Always get 2nd executive to approve a wire request for an out-of-town executive
3. Only release payments after verifying request and obtaining proper approvals

# Future of Payments = Speed & Mobility

Will your payment risk increase?

### Corporate Treasurers

- Over half make more than half of their B2B payments electronically and cite ACH as the preferred payment

### Same Day ACH Usage Grows

- NACHA Payments Survey found 40% of corporate treasurers said same day ACH is a top tool for payments

# Be Aware Of Your ACH Transactions

Keep up with activity on your accounts

**Review your account's ACH debits every day**

- Reconcile or at least review your accounts DAILY.
- *As a business or institutional entity, you do not have Regulation E protection that allows you to take 60 days to return an unauthorized ACH item*

**If an unauthorized ACH debit posted to your account last night, you have to return it today or it's yours!**

# Does Faster Payments = Faster Fraud?

It can, if you don't protect your accounts

## ACH Fraud Prevention Tools

Reduce operational risk and protect yourself from unauthorized ACH transactions by monitoring your accounts each day

- **ACH Positive Pay** allows you to review the each ACH debit and decide to accept or reject it
- **ACH Block** prevents all ACH transactions from posting to an account

# We Are Not Quite Done…

What Form Of Payment Is Most Vulnerable?

**THE CHECK!**

**Three out of four businesses subject to fraud attempts were targeted through checks**

# Cyber-fraud Gets The Headlines

But check fraud is still king!

- Percentage of fraud dollars lost as a result of unauthorized Wire Transfers: 20%
- Percentage of fraud dollars lost as a result of unauthorized ACH transactions: 8%
- Percentage of fraud dollars lost as a result of altered/forged/counterfeit checks:

**45%**

Source: Association of Financial Professionals

# How Can My Bank Help?

- **Utilize Commercial Online Banking**
  - View current-day ACH, wire and teller transactions
  - Review prior-day information for transactions, balances and deposits
  - Manage your accounts with daily reports, alerts and electronic statements
  - Add transparency with Dual Administration – a second administrator will see and approve any changes, new users, new functionality
  - Regularly review view audit logs (by Auditors if possible)

- **Recommendations**
  - If you only have 1 Administrator, require that they maintain 2 login credentials if they are also an active user of the system
  - Use dedicated computers for banking access – no email or internet access allowed

# What Can My Bank Provide for Defense?

Four ways to add security

- Use **Positive Pay** to review checks and ACH debits
- Use **UPIC** to receive ACH or **Safewire** to receive wire payments safely (masking confidential bank R/T and account numbers)
- Use **ACH Block** to stop unauthorized incoming ACH transactions
- Download **Trusteer Rapport** to all PCs & laptops
  - Encrypts keystrokes, authenticates websites, secures data
  - Works with your anti-virus software and firewalls

# Key Takeaways

- **Fraud Attacks Continue To Increase:** AFP reports the number of organizations that experience payments fraud has risen to an all time high of 82%. Today, payments fraud attacks wires, ACH, checks and cards.
- **Today's Cyber-thief Is Tech-Savvy and Tenacious:** Today's cyber-crime schemes have become incredibly complex and technologically advanced. They target payments, your credentials and devices; plus, your staff.
- **Your Security Response Must Include Technology & People Elements:** In the current cyber-fraud era, you must adopt prudent security layers and internal controls that reveal all threats and protect your payment processing.
- **Be Proactive -- Do Not Procrastinate:** Be proactive in educating your staff, implementing internal controls and spotting your vulnerable points before a criminal identifies them.

# Conclusion

With regard to financial fraud there are two kinds of organizations

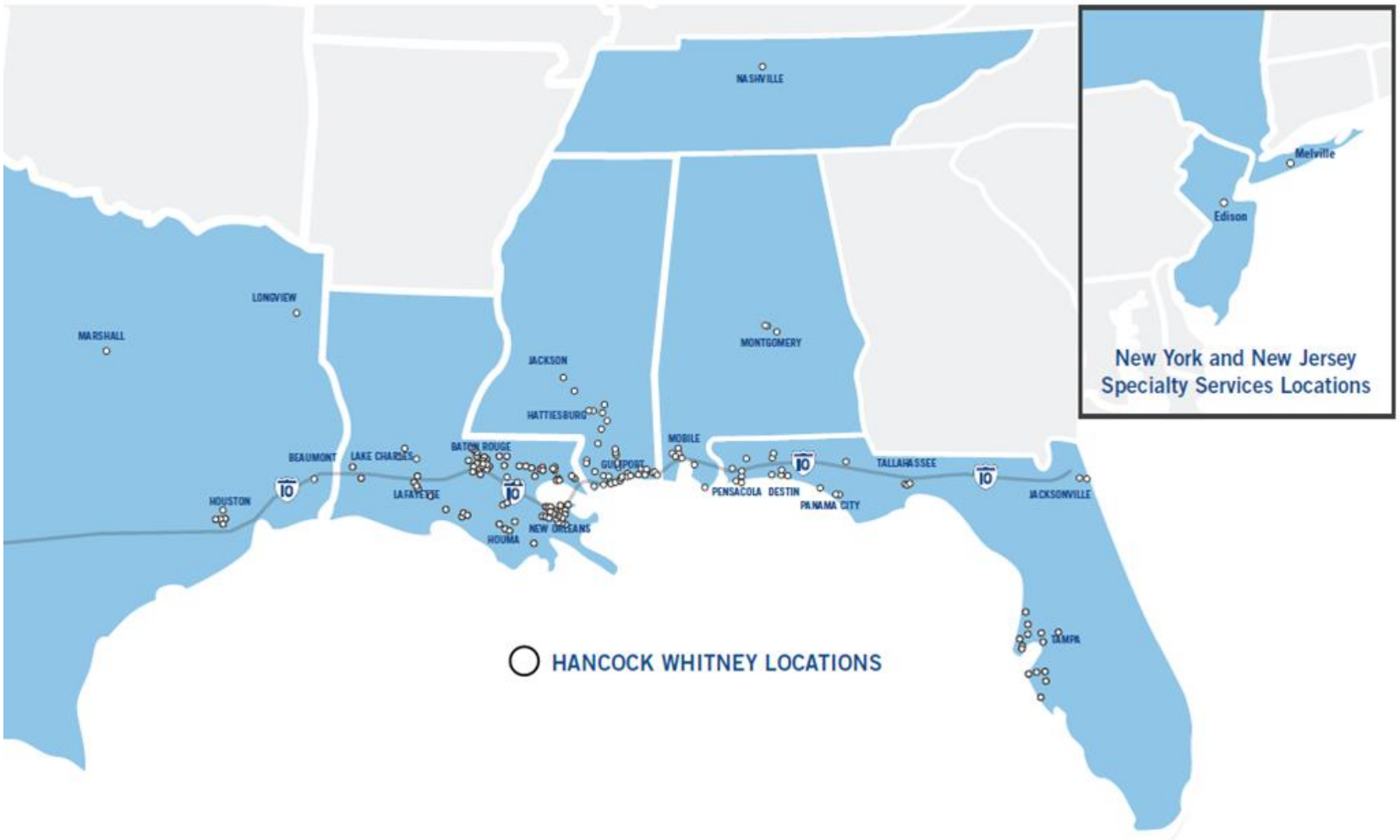
**Those who have been targeted for fraud … And those who will be**

**Most bank clients implement protective measures … right after a loss**

**Why wait for that?**

**Take Action Now!**
**Through the right combination of protective tools, your own common sense and proper internal controls, you can encourage the bad guys go pick on somebody else.**

# Hancock Whitney Bank Locations






HANCOCK WHITNEY

# Contact

Jerry Brodnax

SVP, Treasury Services

Hancock Whitney Bank

504-299-5260

jerry.brodnax@hancockwhitney.com



HANCOCK WHITNEY