Fraudsters Want Your Business 2

Fraud Trends Preview

June 15, 2023

NEACH

CELEBRATING

Facilitator

Rayleen M. Pirnie, *BCJ, AAP, CERP*

NEACH Director, Risk & Fraud

NPG Advisor

rpirnie@neach.org

781-345-7642

- 26 years fraud investigations, payments compliance and
- ACFE Advisory Council
- Federal Reserve Scams Workgroup member
- Is it love or an encounter you will regret?

NEACH, as a Direct Member of Nacha, is a specially recognized a
provider of ACH education, publications and support. Payments A
are directly engaged in the Nacha rulemaking process and the Ac
Professional (AAP) and Accredited Payments Risk Professional (A
programs.

This material is not intended to provide any warranties or legal ad
intended for educational purposes only. Nacha owns the copyrigh
Nacha Operating Rules & Guidelines. Any unauthorized use or acc
expressly prohibited.

Images: iStock & Articulate unless otherwise cited

NEACH
Your Trusted Resource in Payments

join our
VIBRANT PAYMENTS COMMUNITY

Did you know that companies and business users of the payment systems can join NEACH as Corpo

MEMBERSHIP GETS YOU:

An unbiased partner for information on what's happening in the payments industry.

Help managing fraud and other risks inherent to sending and receiving payments.

Education and Training on your contractual obligation under payments system rules and agreements.

Discounts on all NEACH publications and education.

Connect today > neach.org/membership

Welcome!

- Schedule for 3-part Fraud Series:
  - ✓ March 16
  - ✓ June 15
  - ▹ November 8
- 2-Part ACH Education Series:
  - ▹ April 25 – ACH Rules
  - ▹ September 19 – B2B Payments
- Contact your Financial Institution to register

NEACH CELEBRATING 50 YEARS

Large Business Losses

Business Email Compromise Update

Business Email Compromise (BEC)

- Criminals send an email message that appears to com
  known source making a legitimate request
  - Vendor's compromised email – Request for future payments to different
  - Spoofed email that appears to come from Company CEO requesting emp
  - Email that appears to come from Company Executive with urgent Wire Tr
- Business sends the payment per request ultimately lea
  scam

Step 1:
Identifying a Target

Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer

Upon transfers, the funds are steered to a bank account control by the organized crime group.*

*Note: Perpetrators may continue to groom the victims into transferring more funds.

Business Email Compromise Timeline

An outline of how the business email compromise is executed by some organized crime groups

BEC – Communication Hijacking

1. Invoice from legit source such as PayPal or Quickbooks
   - Vendor ID theft

2. Deep fake used to mimic voice of known person requesting transfer
   - Use of technology to mimic the voice of a person known to t targeted employee
   - Variety of open-source tools are available to allow anyone to deepfakes, both video and audio

BEC Resources

Cybersecurity Intelligence Deep Fakes Making BEC Worse

Dark Reading Deepfake Scores $35m in Corporate Heist

FBI *How Business Email Compromise Works*

FBI PSA Business Email Compromise: Virtual Meeting Platf

Security Magazine When Seeing is No Longer Believing

BEC – Sound Business Practices

- Out-of-Band Authentication for email requests
  - Call Vendor or person who allegedly sent email using phone you already know / have on file, not what is in email
  - Do not respond to the email request
- Monitor accounts for ACH and Wire Transfer activity DA
- Dual-Control / Internal control protocols
- Ongoing staff education
- Notify FI immediately if identify suspect transfer
  - FI will attempt to recall Transfer
  - Business liability; payment is authorized

BEC – Sound Business Practices

- Have procedure for cases when someone calls you clai be an executive, even if you recognize the voice
- Corporate Risk Management Strategy and Vulnerability Framework
  - Perform Threat / Risk Analysis
  - Identify digital assets and data to protect
  - Limit or restrict employee information sharing
  - Limit or restrict employee access to personal email and soc
  - Encryption
  - Threat intel and detection capabilities
  - Identity Access Management

Check Fraud


MAIL &
CHECK
FRAUD IS
ON THE
RISE
WHAT YOU CAN
DO TO STAY
PROTECTED

Check Fraud is Soaring

- Mail theft
  - Blue collection boxes – Mailbox "Phishing"
  - Delivery vehicles stolen
  - Carriers held up at gunpoint for master keys
  - Stolen from unattended offices / desks

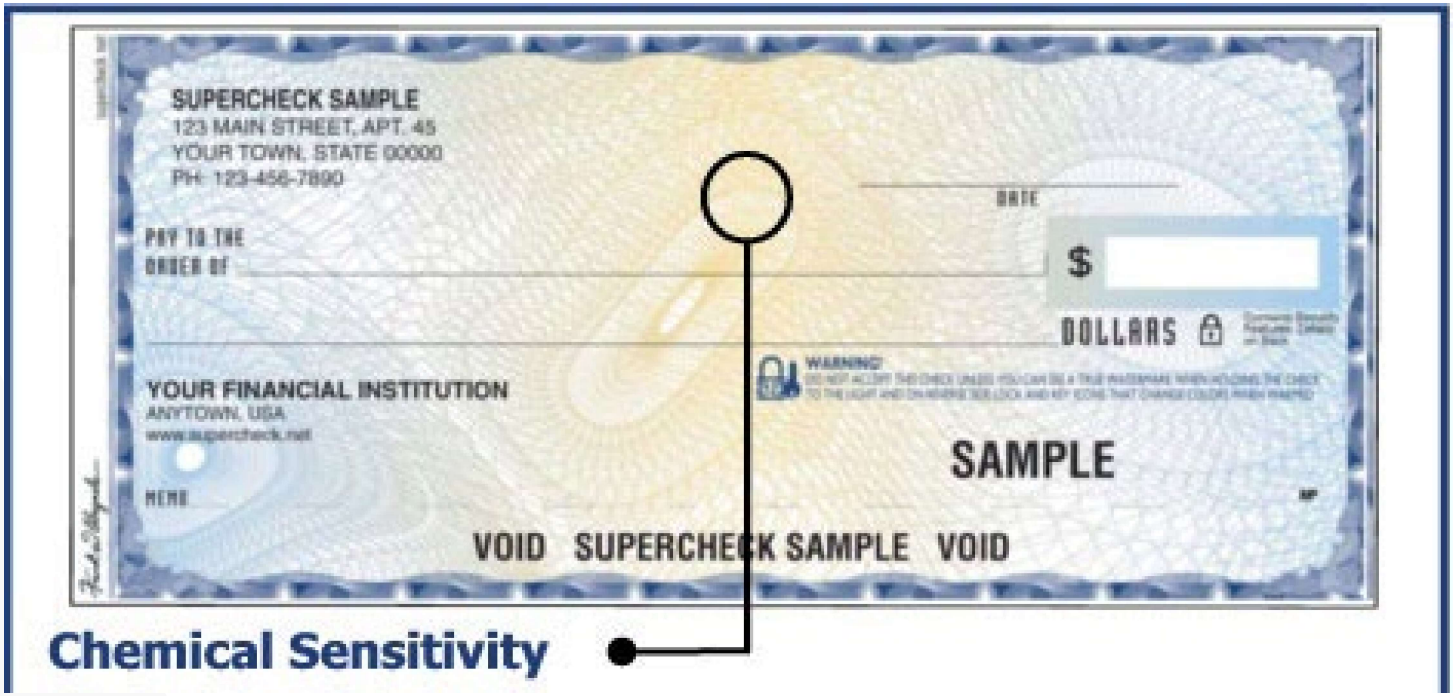
Image source:

Check Washing / Altered Check

- Use of chemicals to alter payee and/or dollar amount o legitimate check
- Handwritten checks easier to wash than printer ink
  - Printed checks – presence of white out or scratch thrus likel to alter payee
- Some stolen checks are also counterfeited

- https://www.uspis.gov/news/scam-article/check-wash


Acetone
EYE FOR THE OBVIOUS
N. M. BARTO, R. W. BELL
7631 MARIPOSA AVE
CITRUS HEIGHTS, CA 95610
916-225-3058
3529
Test test
Pay to the Order of
Test Test Test
$ 500.00
Five hundred Exacting
Dollars
WELLS FARGO
For Test Test Tes
Test Test Test
⑆121042882⑈2000[redacted]⑈03529



Source: Supercheck

Check Fraud Mitigation Strategies

- Lock up check stock
- Do not leave incoming or outgoing mail in unattended l
- Take mail directly to post office vs. blue collection box
- If must use blue collection box, do not rubber band all c mail together – easier to Phish
- Use check stock that is apparent when washed
- Log into account(s) daily
  - Report suspicious items to institution immediately – limited time to do so
- Positive Pay or Reverse Positive Pay

Closing

Wrap-Up

- Threat Assessments
- Strengthen security posture with detailed policies and procedures
- Escalation strategies: Staff protocols if staff encounter suspicious activity
- Use financial institution suggested (or required) accour
- Meet with insurance agent and account officer at least assess additional security needs.


time for