Trending Fraud Schemes Targeting Businesses

Live Webinar | Oct. 19 | 9:00 a.m.

Presented by:
David Schecter, CFE, CAMS
VP and Corporate Security Officer,
Univest Financial Corporation

This presentation is designed to provide general information and a summary of the topic presented for informational purposes only. In addition, this presentation does not address any federal, state, local or foreign laws, rules or regulations that may apply in any given situation. The materials included in this presentation are obtained and drawn from a variety of sources believed to be reliable. These materials were prepared by the presenter(s) who is/are solely responsible for the correctness and appropriateness of the content. Every effort has been made to assure the accuracy of the material; however, the accuracy of this information is not guaranteed. Information is current as of the date of this presentation.

The opinions or viewpoints expressed by the presenter(s) are the sole opinion of the speakers and subject to change without notice, and do not necessarily reflect those of Univest Financial Corporation or any of its affiliates. Although this presentation is prepared by professionals, the content and information provided should not be used as a substitute for professional services (either legal, tax, financial, insurance, or otherwise), and such content and information does not constitute legal or other professional advice. If legal or other professional advice is required, the services of a professional should be sought. Neither Univest Financial Corporation nor any of its affiliates is in any way responsible or liable for any advice or information provided by the presenter(s).

Receipt of this information constitutes your acceptance of these terms and conditions. Reproduction and distribution of these materials are not permitted without the express written consent of Univest Financial Corporation.

Objectives

- Create awareness of current fraud trends affecting business customers at Univest and other banks across the country.
- Share best practices to prevent becoming a fraud victim.
- Recommend steps to take if you are victimized.
- Review resources that are available to you.

Trending Schemes

- Business Email Compromise (BEC)
- ACH/Wire Transfer Fraud
- Data Breach
- Counterfeit Checks/Alterations (Mail Theft)

Risks To Your Business

- Loss of money
- Loss of time
- Loss of reputation

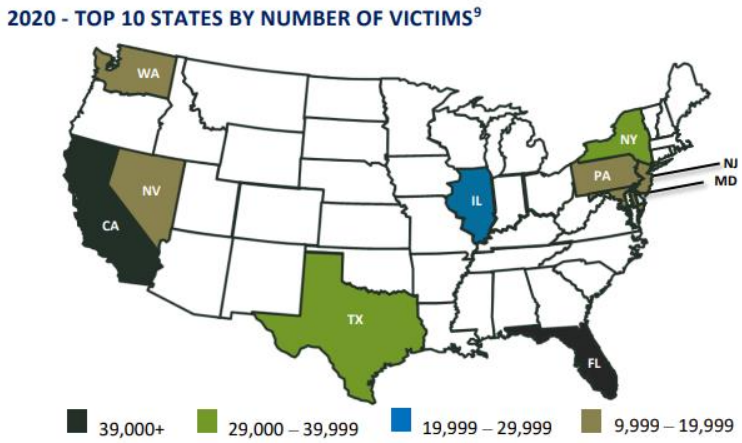
Business Email Compromise (BEC)

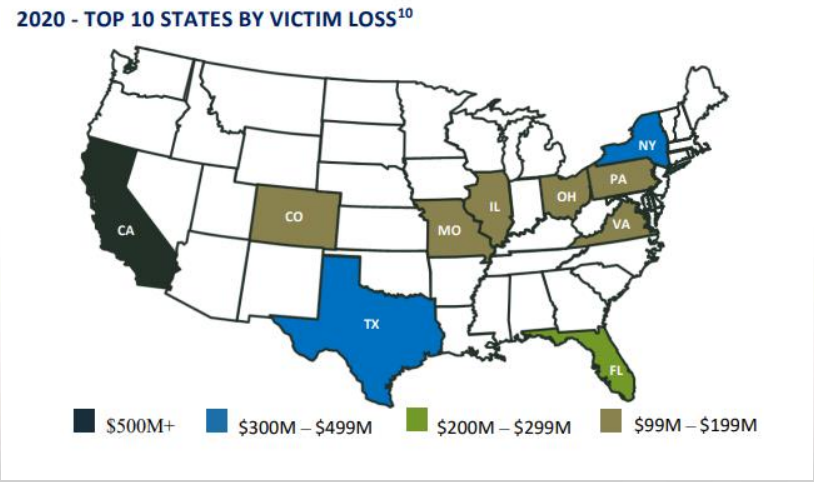
- **Business Email Compromise:** BEC is a scam targeting businesses (not individuals) working with suppliers and/or businesses regularly performing wire transfer or Automated Clearinghouse (ACH) payments. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds. These emails are coming from the actual mailbox of the sender and as a result very difficult to detect.

- These compromised emails could be from an outside sender, vendor or an internal source (company President, CFO or someone at a level to authorize electronic payments to an outside source). Your best defense is paying attention to word choice, semantics, cadence, etc., be on the lookout for anything OUT OF CHARACTER for the sender.

Internet Crime Report 2020

Reported Crime: Top Ten States





- **Pennsylvania and New Jersey are in the top states by number of victims.**
- **Pennsylvania is in the top ten in dollar losses by victims.**

Source: Internet Crime Report 2020

2020 Crime Types *Continued*

By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Source: Internet Crime Report 2020

ACH/Wire Fraud

- Through BEC alternate payment instructions are sent. Typically to the company finance group.
- ACH and Wires are a favorite target of fraudsters due to the quick transfer of funds and in most cases immediate availability. Majority of the funds go through domestic "money mules" and eventually end up overseas with organized crime rings.
- Recovery of any transferred funds is extremely rare.
- According to the FBI, reported losses in 2020 were $1.8 billion

Example Scenarios

- **Company A:** **Accounting receives an email from a known vendor that submits regular invoices paid through ACH. The email stated that the vendor needed to change banks and proceeds to supply the new bank routing and account information. The email includes an attachment with a legitimate invoice that has not been paid. Accounting processes the ACH and the money is sent. Two days later, the Accounting department receives a call from the vendor to advise that the ACH was not received.**

Example Scenarios

- **Company B:** It is Friday afternoon, and an authorized signer of the company receives an email from the CEO asking that an urgent wire be sent on the company's behalf. The CEO says he is on the way to airport and provides a dollar amount and wiring instructions in the email. The wire is sent to the bank and processed that day. Monday morning the employee that requested the wire stopped in the CEO's office to let them know the wire was completed only to learn the CEO knew nothing about it.

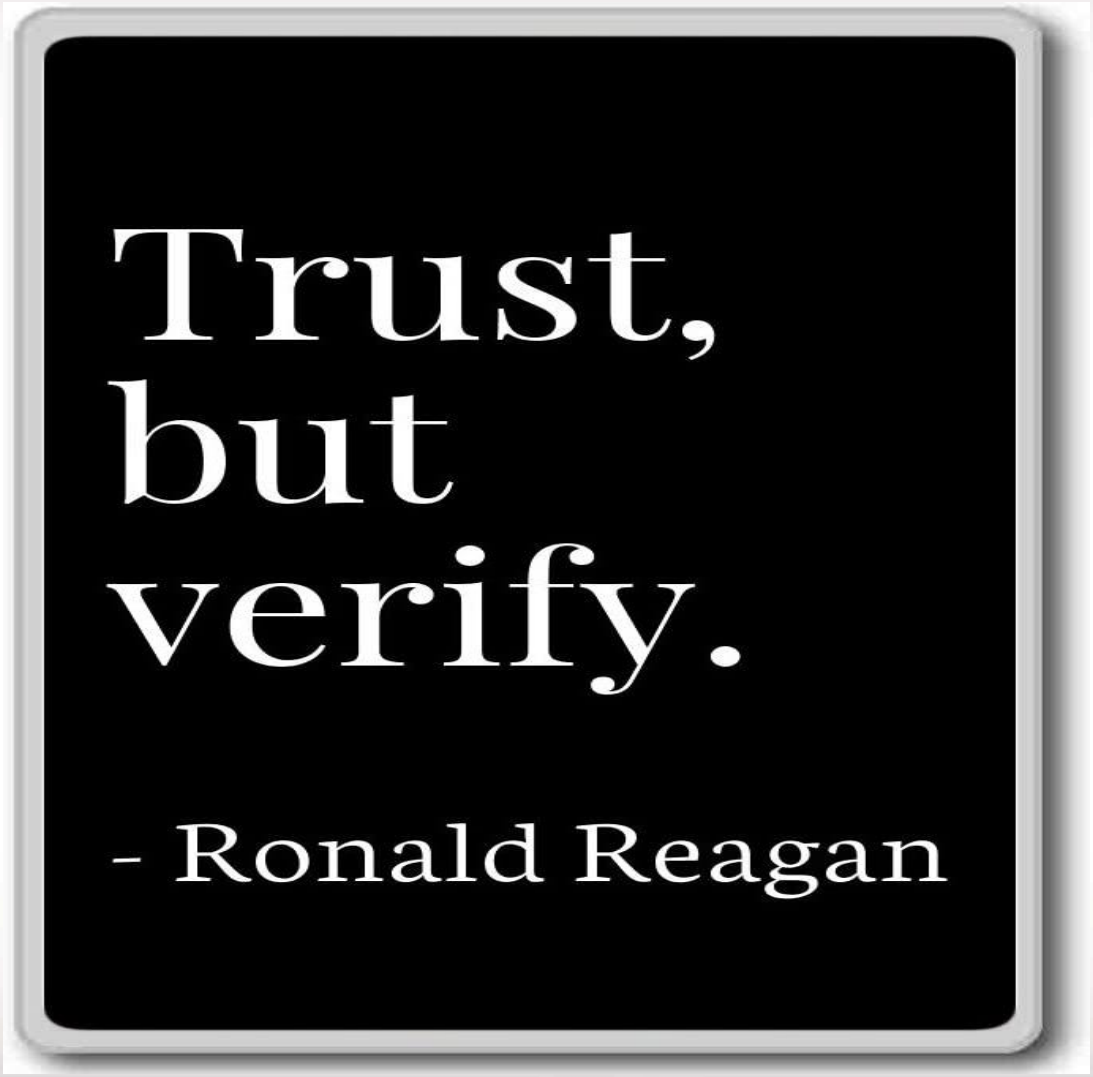
Identifying Suspicious Emails

- Unsolicited; legitimate logos can be spoofed
- May contain attachments you were not expecting
- Typos
- Subtle changes to email address of the sender:

  acmewidgets.com vs. acmewidgits.com
- Poor grammar/style of wording
- Sense of urgency/"confidentiality"
- Timing – end of day, holiday weekends, etc.
- Change of payment instructions, contacts, etc.

Best Practices

- Maintain dedicated computers for business use only; all devices should have current virus and spyware protections.
- Never open links or attachments unless you were expecting the email or verified verbally with the sender.
- Educate employees about email security; dual controls for approvals/changes.
- Always pick up the phone to verify ANY changes in vendor information especially related to payments.
- Review insurance options suitable for your particular line of business


Trust,
but
verify.
- Ronald Reagan

Data Breach

- A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. A small company or large organization may suffer a data breach.
- The goal of the fraudsters may be to obtain personal, confidential non-public information. This could include customer data, trade secrets or payment information.
- The breach could occur trough social engineering or malware. Email attachments/links could lead to malicious programs being installed allowing the unauthorized access.
- In 2020 there were more than 5,500 reported data breaches.
- Ransomware/Denial of Service accounts for 10% of all data breaches.
- Significant financial and reputation risk.

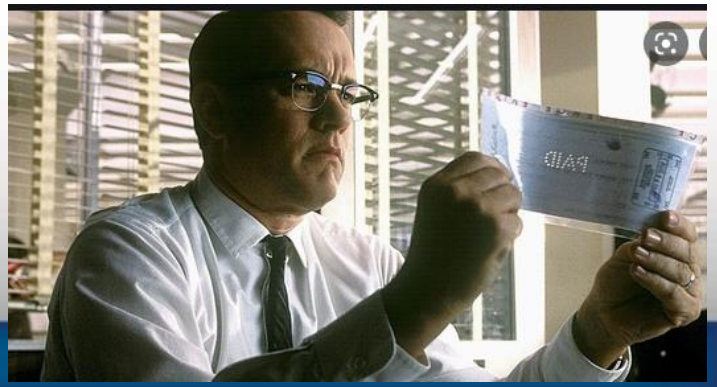
Source: Verizon

What to do if you become a victim

- Notify your Univest Relationship Manager, Univest Customer Support or local Financial Center immediately to discuss next steps.
- Change ALL email passwords immediately. Even for those accounts not known to be compromised.
- Implement multi-factor authentication.
- Run anti-virus/anti-malware scans. Repeat until "clean."
- If anything was found during the scans, it is suggested that you consult with a qualified information security professional.
- Notify your insurance company.
- File a police report. Get the incident on record.
- For internet-based crimes/attempts, report the incident to the FBI using ic3.gov.

Check Fraud

- According to a bi-annual survey released by the American Bankers Association, check fraud (attempts and losses) as of 2018 was $15.1 billion dollars. That number was more than double the prior survey in 2016.
- Check stock is widely available on the Internet. Fraudsters only need an image of your check to replicate and send to unsuspecting money mules.
- Counterfeits often go undetected until the business reconciles their checks. The timing of that reconciliation varies greatly depemding on the type and size of business. To avoid the loss, the item must be returned to the bank of deposit by the next business day.
- Stealing legitimate checks from the mail and altering them or chemically “washing” checks is on the rise. It is a very low-tech crime which makes it more appealing to fraudsters.



Mailbox Fishing

Check Washing/Alteration

Best Practices

- **Take outgoing mail directly to the post office or hand mail directly to the carrier.**
- **Keep check stock and outgoing mail in a secure locked area daily.**
- **Use checks with security features such as chemical/heat resistant check stock.**
- **Monitor account activity daily to ensure posted checks match your records.**
- **Consider enrolling in *Positive Pay.***

What to do if you detect an unauthorized check(s)

- **Notify your Univest Relationship Manager, Service Center or your local branch office immediately to discuss next steps.**
- **Univest will mostly likely recommend enrolling in *Positive Pay* or closure of the existing account and opening a new one.**
- **If you experience a loss you may want to file a police report or insurance claim depending on the loss amount.**

Resources

- **Internet Crime Center, Ic3.gov (FBI)** – report any internet-based crime or attempt. Excellent source of internet crime trends, press releases, information and various reports.
- **Federal Trade Commission, Ftc.gov** – numerous publications and resources for business and consumers on topics such as identity theft and data security.
- **Verizon 2021 Data Breach Investigations Report (DBIR),** *https://www.verizon.com/business/resources/reports/dbir/*
- **Univest Relationship Manager** – can review products and services that may be available based on specific needs.

Contact Information

David Schecter

schecterd@univest.net

(215) 721-2413