The Scope of the Problem

Financial Fraud is prevalent and growing

- 15.4 million consumers affected in 2016, up 16% from 2015 and the highest number ever recorded.
- 47% of large companies experienced fraud or cybercrime in past 12 months; total losses of $1.45 trillion
- Underreporting: 41% of known instances of private-sector financial crime are not reported internally or externally

Costs include:

- $2.67 in costs to businesses for every $1 of fraud
- That cost is passed on to you the consumer

Sources: www.cnbc.com/2017/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year
Thomson Reuters, "Revealing the True Cost of Financial Crime", May 2018
http://Risk.lexisnexis.com/about-us/press-room/press-release/20180301-true-cost-of-fraud-financial

Financial Fraud

Affects the entire economy:

- Businesses
- Nonprofits
- Education
- Public Entities
- Consumers

Types of Fraud

Many ways to separate people and businesses from their funds:

- Fraudulent emails
- Wire Fraud
- Fraudulent ACH transactions
- Check Fraud
- Card Fraud
  - Account Takeover Fraud
  - Card Not Present Fraud
- Theft/ embezzlement

As banks we have seen it all and have tools to help you.

Fraudulent emails

Targeted phishing and "whaling" emails hit many firms

- "Phishing": Bogus emails appearing to be from a trusted party
- Contain a URL or attachment that they want you to click
- Gets you to hand over confidential info or download malware
- High-profile examples:
  - Hillary Clinton campaign chair John Podesta tricked by a phishing email to give up his Gmail password in 2016
  - University of Kansas employees responding to a phishing email gave fraudsters their paycheck deposit information, and lost their pay as a result

Example phishing email

From: **IT Service** <clarkbakerfunding@gmail.com>
Date: Mon, Jul 25, 2016 at 7:52 AM
Subject:
To:

Attn: Lehigh University web-mail User,

We noticed that your mailbox has exceeded the allocated storage limit as set by our administrator, you will not be able to send or received email until you upgrade your allocated quota for effective use.

To upgrade your quota now, you need to Copy/click below link to fill the upgrade form.:

http://admincentre.byethost13.com/form.php

Failure to do this will have your account inactive.

Lehigh University Support Team.
27 Memorial Drive West, Bethlehem, PA 18015 USA · Phone: (610) 758-3000

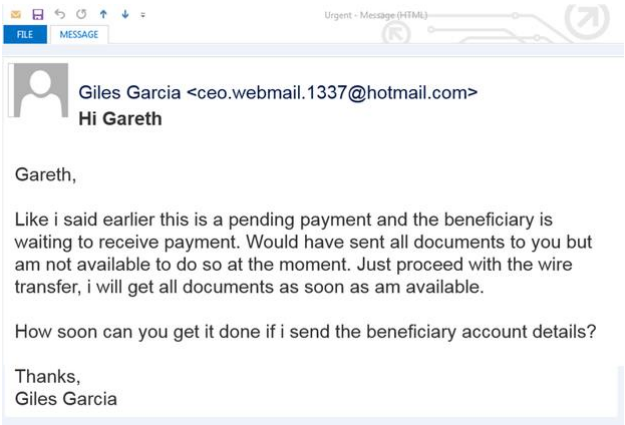
Source: https://lts.lehigh.edu/phishing/examples

Wire Fraud

Targeted phishing and "whaling" emails hit many firms

- "Whaling": Scammer impersonates a senior executive such as CFO
- Asks a low-level employee to wire money
- Can also involve asking for W2's, other confidential data
- Phrasing and jargon designed to sound like typical correspondence from staff
- Written by a human, with no links or attachments; and spammers change domains frequently- much harder for a spam filter to detect

Wire Fraud



Wire Fraud

Phishing and Whaling

- IT security vendors have/ are developing products to fight these scams BUT:
- Best defense: Train employees to be vigilant and ask questions!
  - VALIDATE new payment instructions received via email- even internal email
  - PICK up the phone whenever possible and speak directly to the individual allegedly requesting a funds transfer
  - CONTACT outside vendors or clients directly to confirm any requests for payment method changes
  - REVIEW all payments before they are sent
  - ENSURE all correspondence is validated and documented in a unified way across your business.
- "AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE"

Sources: Clinton Boulton, CIO Magazine, "Whaling emerges as major cybersecurity threat," April 21, 2016
www.jpmorgan.com/global/cb/wire-transfer-fraud

Wire Fraud

Voice Phishing

- Scammers still use phone-based fraud as well
- Callers impersonate legitimate companies to get your personal info
- Don't give out personal information in response to unsolicited phone calls
- Call back vendors at known numbers or the main customer support numbers on their websites

Wire Fraud

Fax Phishing

- Some scammers still use fax machines
- As email filtering got better, other lines of communication became attractive
- No, the IRS won't ask you to fax them your EIN and e-file PIN
- Also, some phishing emails claim to have a fax-to-email message for the user

ACH Fraud

Social-engineering scams target public entities and others

- 2017 NACHA report: municipalities and colleges prime targets
- Request appears to be from a valid vendor, asks to update their payment information
  - New routing #
  - Change from ACH to wire
- Those who complied sent money to fraudsters
- Why public entities? Their contracting information is typically a matter of public record

Source: https://www.nacha.org/news/ach-operations-bulletin-1-2017-social-engineering-fraud-against-public-sector-and-other

Check Fraud

Still persistent in the Digital Age

- Even as legitimate use of paper checks declines, check fraud continues
- Total forged, counterfeit, and stolen checks in USA to top $7 billion in 2018
- Digital payments clear quickly, checks can take days- and time is the scammer's friend
- Per the Association of Financial Professionals, checks are the preferred means of payments fraud. 74% of finance professionals say that their organizations' payments have been exposed to check fraud*

**Source: 2018 AFP Payments Fraud and Control Survey Report*

Card Fraud

Card-Not-Present Fraud

- Transactions made online or by phone with no physical card presented
- EMV (chip card) technology has e-commerce increasingly attractive to criminals
- Fraudulent e-commerce sales were estimated at 3.85% of all sales in 2Q17
- Publicly available estimates of e-commerce fraud losses range from $25 to $40 billion

Card Fraud

Card-Not-Present Fraud

- Massive breaches and information compromises at retailers flooded the Dark Web with info needed to perpetrate these frauds
- Fraudsters can also use publicly available databases, social media, etc. to learn about their targets- and guess answers to security questions

Sources: https://financeandriskblog.accenture.com/cyber-risk/finance-and-risk/the-scope-of-the-card-not-present-cnp-fraud-problem

Card Fraud

Credit Card Skimming

- Fraudster obtains a legitimate card's details, copies onto a bogus card or uses them online, and charges away; or sells the information on the web
- Skimmers can be placed over legitimate card readers
  - Gas stations, ATMs, frequent targets
  - Retail and restaurant workers are commonly recruited: wait staff can swipe your card in a skimming device when they step awy from your table
- Red flags:
  - Credit card reader that sticks out far past the panel
  - Parts of the creidt card reader are loose
  - Gas pump security seal has been voided
  - Thicker than normal pin pad: keystroke logging device can be put on to capture your PIN

Physical Security

- Physical security is just as important as electronic security.
- Physical and electronic systems are only as strong as their weakest link.
- A locked-down network and servers will not help you if an employee leaves his or her laptop unlocked and open
- Intrusion Testing: where are the weak points?

Physical Security

PHYSICAL SECURITY

Do you have robust policies and procedures for accessing:
- Restricted areas?
- Restricted material?
- Company vehicles?

Do you have cameras and alarm systems and are they operational?
Who manages access and entrance points? Are they properly trained?

Physical Security

- Social Engineering- manipulating others to give you access or information
- Physical infiltration can be an end in itself, or a step to breaching technical infrastructure
- Employees: an organization's greatest asset- but their practices can undermine a security regimen
  - The "broken paper shredder"

Laptop Security

Planes, Trains, and Automobiles

Laptops, phones, and other employer devices at risk when traveling

- Car break-in- stow laptops in trunk or under the seat
  - Take inside when you arrive at hotel/ office/ home
- Gas pumps- do you lock your car while pumping gas?
- Tokens- do not store in the same bag as your laptop

Who Are the Criminals?

It's not always who you'd think

- Foreign actors often blamed for card hacks, ACH/ wire fraud
  - Some nations do play outsized roles: former Soviet bloc, China, etc.
- Much fraud is actually perpetrated domestically
- KPMG: People who commit fraud are typically experienced employees in a position to collude with others inside and outside an organization
  - Usually hold managerial or senior positions
  - No prior history of criminal activity
  - Only 35% face criminal or civil litigation; only 7% do jail time
  - 93% of frauds perpetrated in multiple transactions; 72% over a 1-5 year period

Source: KPMG "Profiles of a Fraudster":

Bank Products to Help

Securing against different types of fraud with Treasury Management solutions

Positive Pay- protects against check fraud

- Checks presented are verified against a file uploaded by user
- Electronic and/or text notification- approve or deny?
- If no decision by cutoff time, default to deny the check

Bank Products to Help

ACH Block and ACH Filter

- ACH Block for accounts that should NOT have ACH activity
- All attempted ACH debits will be returned to the originating bank

- ACH Filter allows you to define who may debit ACH's from your account and for what amounts
  - For example a payroll processor or utility provider
- ACH debits not on approved list will be "suspect" items, you decide to pay/return

Bank Products to Help

Trusteer Rapport

- Additional layer of security to anti-virus software
- IBM product, free to download
- Protects against malware and phishing attacks
- Verifies the website you're connecting to is genuine not a fake
- Once verified, Trusteer locks down communication between you and the site so your credentials can't be stolen

Bank Products to Help

Out of Band authentication

- Two-factor authentication requires a second verification method (e.g. not just a password)
- Out-of-band authentication is when the second method is through a separate communication channel (e.g., code to your phone plus ID and password from laptop)
- Even if a fraudster gains access to your laptop, they cannot complete a transaction without also accessing your phone
- Ensures only legitimate users initiate wires, ACH transactions, and internal transfers.

Bank Products to Help

Regular Relationship Reviews with your Banker

- Do you know who your banker(s) is (are)? You should- and they should know you and your needs.
- Review of online banking users and authorized signers
- Review of limits and authorizations

Use online banking to monitor your accounts daily

Some Resources

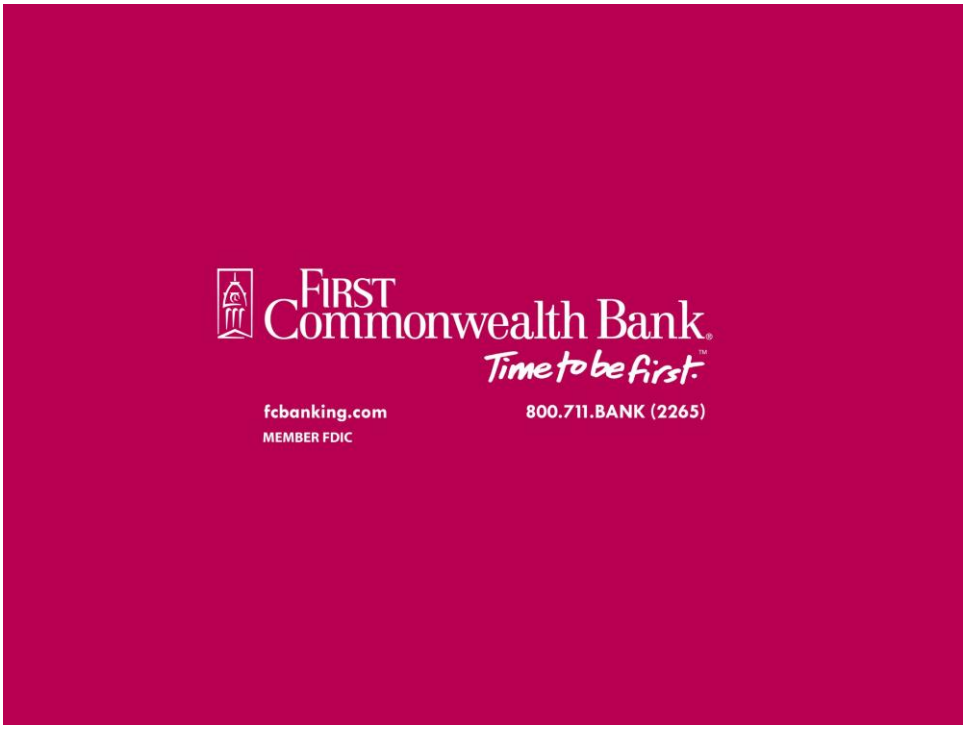
- Krebs on Security: www.krebsonsecurity.com
- Accenture Finance and Risk Blog: www.financeandriskblog.accenture.com
- Ohio Protects: www.ohioprotects.org/learn-about-fraud
- 2018 AFP Payments Fraud and Control Survey: www.afponline.org
- FBI: https://www.fbi.gov/scams-and-safety
- NACHA Current Fraud Threats Resource Center: https://www.nacha.org/content/current-fraud-threats-resource-center

THANK YOU!

Thank you to OAPT!

Travis Kelley
VP/ Government Banking
Address: 100 Central Plaza S
Canton, OH 44702
Email: Tkelley@fcbanking.com
Phone: (330) 280-5212

FIRST COMMONWEALTH BANK
www.fcbanking.com
Twitter: @financebetter


FIRST Commonwealth Bank
Time to be first.
fcbanking.com
MEMBER FDIC
800.711.BANK (2265)