M&T Bank
Understanding what's important®

FOCUS ON FRAUD: EXECUTIVE IMPERSONATION

M&T BANK COMMERCIAL BANKING

2/7/2018

BETHANY ARNOLD, VICE PRESIDENT

TREASURY MANAGEMENT CONSULTANT

LEGAL DISCLAIMER

This presentation is for informational purposes only and nothing herein should be considered or relied upon as legal advice. You should familiarize yourselves with your financial institution's account and service agreements and understand your liability for fraudulent ACH and wire transactions. Please consult your own legal counsel for any legal advice relating to such liability and/or other matters in this presentation.

2017 AFP® Payments Fraud and Control Survey

75% of companies were targets of payments fraud last year

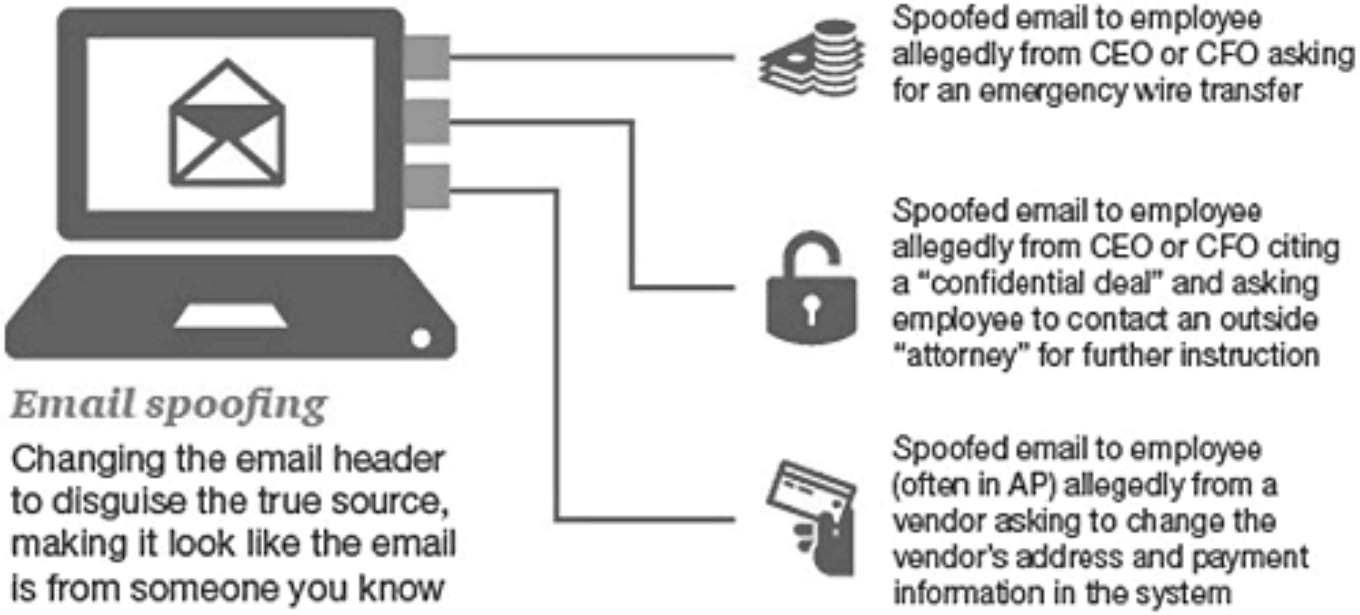
- Paper checks continue to lead as the payment type most susceptible to fraudulent attacks even as their overall use continues to decline (**75%** of organizations subject to payments fraud in 2016 were victims of check fraud)
- Credit and debit cards experienced a slight decrease in fraudulent activity, down from 39% in 2015 to **32% in 2016**
- ACH debit fraud was cited by **30%** of survey respondents
- Wire fraud incidents nearly doubled from two years ago, from 27% in 2014 to **46% in 2016** and nearly **tripled** from 14% in 2013.

"Wire fraud is second only to check fraud. Wires are attractive targets because of the speed of transaction and also the difficulty in retracting a transaction... The dramatic increase in wire fraud coincided directly with the rise in business email compromise (BEC) scams. The fact that wire fraud is still being reported around a similarly elevated level (46%) indicates that BEC scams— unfortunately—continue to be prevalent and effective."

Source: 2017 AFP Payments Fraud and Control Survey

EXECUTIVE IMPERSONATION – WHAT IS IT?

Cyber criminals impersonating senior level company executives via email in an attempt to trick a member of that company into sending money by wire or ACH



EXECUTIVE IMPERSONATION WIRE FRAUD: A REAL LIFE SCENARIO

Hundreds of millions of dollars are stolen each year by wire fraud, with executive impersonation attempts continuing to rise. What better way to drive home the importance of organizations consistently demonstrating the right behaviors than to view a real-life example of an executive impersonation wire fraud that was successful.

The Scene

The Controller of XYZ Company is forwarded an email exchange between her CEO and CFO, in which the CFO instructs her to originate a wire transfer out of their business account. The Controller complies with the request and receives a wire call back from M&T Bank to confirm the instructions.

Cast

Tim Smith……XYZ Company CEO
David Jones……XYZ Company's CFO
Gina Green……XYZ Company's Controller

Note: All names and client information have been changed to protect the parties.

-------- Original Message --------

Subject: Wire Payment
Date: 2015-05-29 10:44
From: Tim Smith <Tim. Smith@XYZCompany.com>
To: David Jones <David.Jones@ XYZCompany.com>

David,

Per our conversation, attached is the wiring instructions. As you already know, the support for this will come in handy later. Let me know once this is processed.

Tim

Notice of Confidentiality
This transmission contains information that may be confidential. It has been prepared for the sole and exclusive use of the intended recipient and on the basis agreed with that person. If you are not the intended recipient of the message (or authorized to receive it for the intended recipient), you should notify us immediately; you should delete it from your system and may not disclose its contents to anyone else.

From: David Jones [mailto:david.Jones@XYZCompany.com]
Sent: Friday, May 29, 2015 1:55 PM
To: Green, Gina (Anywhere)
Subject: Fwd: Wire Payment

Gina,

Are you able to process an international wire before the cutoff time?

David

On 2015-05-29 19:22, Green, Gina wrote:

For how much?

Gina Green
Gina.Green@XYZCompany.com
555-828-8366 (Office)
888-555-1059 (Fax)
199 Blank Street, Suite 800
Anywhere, NY 12345
www.XYZCompany.com

From: David Jones [mailto:david.Jones@XYZCompany.com]
Sent: Friday, May 29, 2015 3:27 PM
To: Green, Gina
Subject: RE: Wire Payment

$314,701.65.

On 2015-05-29 19:28, Green, Gina (Anywhere) wrote:

Ok. Is this supposed to be out of our M&T lockbox account? Do you have a free moment to call my cell 555.913.8568?

Gina Green
Gina.Green@XYZCompany.com
555-828-8366 (Office)
888-555-1059 (Fax)
199 Blank Street, Suite 800
Anywhere, NY 12345
www.XYZCompany.com

From: David Jones [mailto:david.Jones@XYZCompany.com]
Sent: Friday, May 29, 2015 3:39 PM
To: Green, Gina (Anywhere)
Subject: RE: Wire Payment

Can it wait? What's the issue?

From: Green, Gina
Sent: Friday, May 29, 2015 3:51 PM
To: 'David Jones'
Subject: RE: Wire Payment

You answered my question. I just need to understand this a bit better because in order to be paid out of the lockbox it needs to be paid into that account in the first place. I have approved the wire, so it is submitted.

Gina Green
XYZCompany
Gina.Green@XYZCompany.com
555-828-8366 (Office)
888-555-1059 (Fax)
199 Blank Street, Suite 800
Anywhere, NY 12345
www.XYZCompany.com

From: Green, Gina [mailto:Gina.Green@XYZCompany.com]
Sent: Monday, June 01, 2015 3:10 PM
To: M&T Bank Relationship Manager; TM Consultant; Relationship Liaison
Subject: FW: Wire Payment
Importance: High

The wire that was sent on Friday was completely bogus. I need it pulled back immediately. Please call me ASAP.

Thank you,
Gina

Gina Green
XYZCompany
Gina.Green@XYZCompany.com
555-828-8366 (Office)
888-555-1059 (Fax)
199 Blank Street, Suite 800
Anywhere, NY 12345
www.XYZCompany.com

Click here to listen to recording of the M&T wire room call back conversation

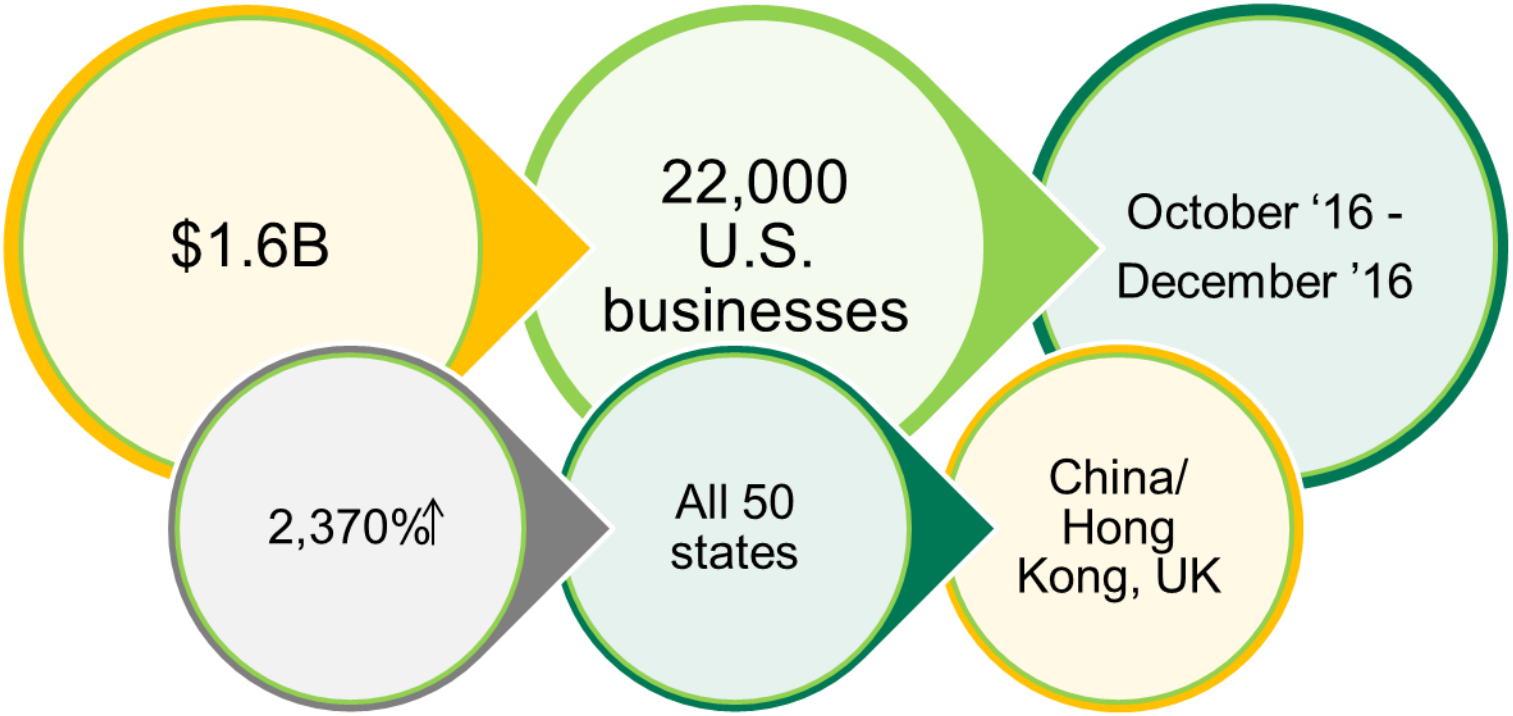
EXECUTIVE IMPERSONATION – HOW DOES IT HAPPEN?

- An increase in **malware** is being used in connection with Impersonation scams
- Email accounts are **hacked** or email addresses are made to appear very similar
- Instructions are often purported to be **urgent** or confidential
- Spoofed emails very closely **mimic** a legitimate email account or recent request
- Email recipients are usually **authorized** to initiate payments, such as web based banking application user or an authorized signor on an account
- Many times, the transactions are sent to **international** banks in China or Hong Kong
- Fraudsters may pose as lawyers who claim to be handling **confidential or time-sensitive** information.

EXECUTIVE IMPERSONATION – WHY DOES IT WORK?

- Traditional cyber attacks work against a company's technology
- Criminals can easily obtain business information online
- Executive impersonation works to manipulate human beings
- Criminals prey on people's natural tendency to respond to authority, and their need for urgency
- Executive verification of legitimacy is difficult because they are often unavailable
- Wire transfer requests are commonly business specific and similar to normal business transaction amounts

EXECUTIVE IMPERSONATION – THE CONSEQUENCES



Source: FBI News Stories, May 2017

CUSTOMER CONTROLLED FRAUD BEST PRACTICES