

# Wire Fraud & Remote Operations – What Every Company Needs To Know and Do NOW

Webinar



# Presenters



## **MICHAEL BRICE FOUNDER OF BW CYBER SERVICES**

28 years of experience providing technology, security, and related cybersecurity consulting solutions for multiple industries, including deep commercial and military experience in the financial services industry as well as classified government operations. Received specialized training by the National Security Agency in Signals Intelligence. Former Marine Officer – served in the 1<sup>st</sup> Gulf War.



## **BETH CRONENWETH CONSULTANT TRISTATE CAPITAL BANK**

A consultant at TriState Capital Bank, Beth has 38 years of experience in commercial banking/ treasury management risk, product management and sales. She is a frequent speaker at national and regional conferences on topics such as Risk Management, Treasury Management, and Strategic Management.



## **ANTHONY D. MASCIA MANAGING PARTNER EFSI**

Co-founder and partner of Essential Fund Services International, LLC (“EFSI”) and oversees EFSI’s business development and marketing. Anthony began his professional career as a trader and member of the New York Board of Trade in 1999. As a member of the New York Board of Trade (NYBOT) & Intercontinental Exchange (ICE).

# Purpose Of Today's Call

*Educate companies and organizations on increased risk as a result of the rush to remote operations*

- Payments Fraud
  - Business Email Compromise (BEC)
  - Unauthorized access to online banking
  - Vendor Business Email Compromise (VBEC)
  - Customer procedural weaknesses
  - Internal procedural weaknesses
  - Direct Deposit Fraud
- Reliance on “Trusted” 3<sup>rd</sup> Parties
- Ransomware



# Back To The Basics

*What we've learned doing Incident Response and Forensics in the financial services industry – Breaches and Fraud*

- **PARETO** (80/20) - Vast majority are due to simple control lapses
  - Easy fixes
  - Not costly
  - Trust but verify
  - Education is important
  - Voice confirmation is CRITICAL
    - Account changes
    - Wire callbacks
  - Authentication of authorized individuals

# Back To The Basics - Continued

*What we've learned doing Incident Response and Forensics in the financial services industry*

- **Payment Fraud** – E-mail and Network breaches are the “secret sauce” for successful frauds!
- **VERIFY** - Require your “Trusted” 3rd parties to prove they exercise “Good Security Hygiene”

# A Brief Explanation Of The Most Current Threats





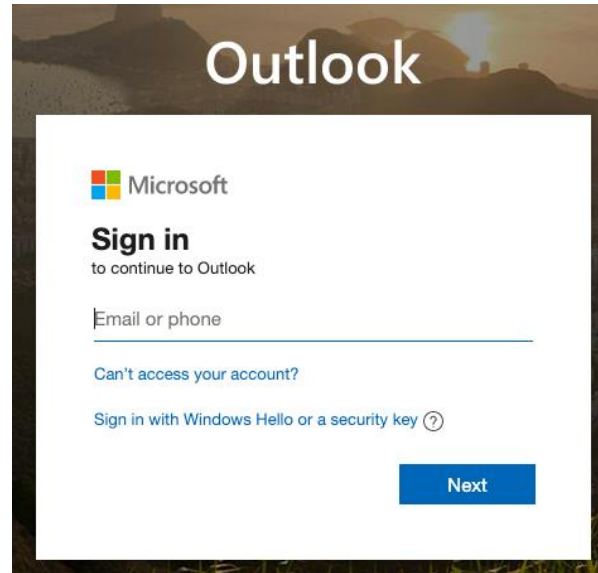
# Payments Fraud: Phishing Explained

## The Attack



A clever phishing e-mail that an employee or family member clicks

## The Prize



Redirection to a Credential Harvesting website (e.g., masquerading as Microsoft) to steal login credentials

## Financial Fraud



By secretly changing valid wire instructions to a Fraudulent Instruction (from a valid e-mail account) – the criminal redirects the funds to their bank account

# Payments Fraud: Valid E-mail Compromise or TypoSquat\* Impersonation E-mail

## The Attack

---

Fake Executive Wire Request

## The Prize

---

Employee, think request is coming from a company executive, initiates a wire transfer to the provided account

## Financial Fraud

---

Money goes to the account of the perpetrator and is irrevocable

*\*TypoSquatting is the creation of a fake domain almost identical to the real one to fool you with an impersonation e-mail*



# A New Twist to Wire Fraud – BEC & TypoSquat Combined

## The Event

---

PE holding working with a credit facility used by PE, receives information from the credit facility related to a valid payment (e.g., early payoff terms)

## The Deception

---

Holding company confirms terms and agrees to payment; HOWEVER, the valid e-mail is maliciously manipulated and actual e-mail to credit facility states decision is made NOT to proceed with early payment

## The Twist

---

Holding company then receives fake e-mail from credit facility with wiring instructions that direct funds to criminal account in US (2 bounces before going overseas); Neither PE nor holding company realize the \$1m loss for 60 days

# Ransomware: An Alternative to Wire Fraud That is Just as Profitable

## What is Ransomware?

It is a virus software that blackmails you by encrypting your hard drives or locking you out of your computer. In many instances, the victim's data is also stolen and used for additional monetization (e.g., sale of PII on Dark Web, further extortion per confidential information, etc.).


**It can infect an entire organization.**

## *Cryptolocker Screenshot of Infected Computer*



# Your “Trusted” 3<sup>rd</sup> Party – A Recent Example

*“Attorney Allen Grubman — the most prominent entertainment attorney in the world, whose firm represents stars including Lady Gaga, Madonna, Mariah Carey, U2, Bruce Springsteen, Priyanka Chopra and Bette Midler — is being shaken down by hackers who attacked his New York law firm for \$42 million.”*

 The American Lawyer

## Lady Gaga's Law Firm Got Hacked. Now What? | The ...

Lady Gaga's Law Firm Got Hacked. Now What? Allen Grubman's New York firm says its celebrity clients have shown "overwhelming support" ...

3 days ago



 Page Six

## NYC attorney to likes of Lady Gaga, Elton John hacked, files held for \$21M ransom

Hackers have attacked the website of top showbiz attorney Allen Grubman, demanding \$21 million while threatening to reveal personal details ...

5 days ago



# “Trusted” 3<sup>rd</sup> Parties Should Not Be Trusted

- Attorneys
- Accountants
- Outsource IT Staff or IT Managed Service Provider
- Other vendors with access to your data



# What Do You Do?



# Trust But Verify Your Trusted 3rd Party Vendors

- Always check credentials
- Callbacks to authorized individuals
- Anomaly Detection
- Require IT Risk Assessments and PenTesting

# Work With Your Financial Institution

- Wire callbacks
- Anomaly detection
- Positive Pay
  - Check Positive Pay
    - Payee Positive Pay
    - Reverse Positive Pay
  - ACH Positive Pay
  - Debit Block
- Dual/Triple control on payment initiation
- Secure browser
- Multi-factor authentication
- Token authentication



# Pay Special Attention To 7 Key Internal IT Security Controls

- These are 7 very simple questions that EVERY Executive should be asking of their IT Staff

## 7 AREAS

to Address with Your IT Staff or Outsourced Vendor to Ensure Your Remote Workforce is Appropriately Protected

- 1 Local Administrative Privileges** - Have you disabled Local Admin Privileges on all user's remote PCs? (Also strongly recommend not allowing business use of non-company issued PCs.)
- 2 Patching & Anti-Virus** - Are remote user's PCs still being patched, and are A/V definitions being updated and PCs scanned per policy?
- 3 Outlook Web Access (OWA)** - For MicroSoft users, is OWA enabled? If so, can you confirm that multifactor authentication (MFA) is configured as "Mandatory" (not just "Enabled")? Same with G-Suite & other cloud providers.
- 4 Malicious Rules** - Can you perform a "rules" search on users' mailboxes to see if there are any auto forward, auto delete, or other anomalous rules (unknown to the user) that would be indicative of an ongoing breach? Do you get and review alerts when a user creates a new rule?
- 5 Remote Access** - Do you have MFA in place for all other means of remote access (e.g. VPN, RDP, LogMeIn, TeamViewer, etc.)?
- 6 MS Application Permissions** - For MicroSoft users, can you confirm the applications that our users have granted permission to are valid?
- 7 Phishing Training** - Have you provided phishing training to our users recently? If so, was it custom tailored for the types of attacks that are being directed toward the asset management industry?

Unfortunately, in today's world – it's often not a case of "if" but "when" you might be breached. Consequently, we strongly recommend that you verbally confirm all wire information (especially when there are changes to the wiring instructions). Equally as important, we recommend you ensure your investors know to also verbally confirm all wires with you as well.



Contact Us Today to Schedule Your FREE Consultation: (646) 779-8976  
Or visit [bwcyberservices.com](http://bwcyberservices.com) for more information



# 7 Areas to Address

- 1) **Local Administrative Privileges** - Have you disabled Local Admin Privileges on all user's remote PCs? (Also strongly recommend not allowing business use of non-company issued PCs.)
- 2) **Patching & Anti-Virus** - Are remote user's PCs still being patched, and are A/V definitions being updated and PCs scanned per policy?
- 3) **Outlook Web Access (OWA)** - For Microsoft users, is OWA enabled? If so, can you confirm that multifactor authentication (MFA) is configured as "Mandatory" (not just "Enabled")? Same with G-Suite & other cloud providers.
- 4) **Malicious Rules** - Can you perform a "rules" search on users' mailboxes to see if there are any auto forward, auto delete, or other anomalous rules (unknown to the user) that would be indicative of an ongoing breach? Do you get and review alerts when a user creates a new rule?
- 5) **Remote Access** - Do you have MFA in place for all other means of remote access (e.g. VPN, RDP, LogMeIn, TeamViewer, etc.)?
- 6) **MS Application Permissions** - For Microsoft users, can you confirm the applications that our users have granted permission to are valid?
- 7) **Phishing Training** - Have you provided phishing training to users recently? Was it tailored for the types of attacks that are being directed toward the financial services industry?

# The Bottom Line

- Unfortunately, often - it's not a matter of “If” but “When”...
- Verbal confirmation on all wires is critical
  - Dollar thresholds may apply
- Data backup (multiple copies) must be kept off-site and access to the data tested annually
- Check internal controls on a regular basis
  - Revise as necessary
- Continuous education and training (every quarter) is essential
- Trust but Verify...



# QUESTIONS?

# THANK YOU



(646) 779-8976  
[www.bwcyberservices.com](http://www.bwcyberservices.com)



(412) 304-0304  
[www.tristatecapitalbank.com](http://www.tristatecapitalbank.com)



(646) 0948-6500  
[www.essentialfsi.com](http://www.essentialfsi.com)