ABA Litigation Section, Insurance Coverage Litigation Committee
Fake President Fraud — What Is It, and Is It Covered?
Tucson, Arizona — March 4, 2017

"Fake President" Fraud – What is It?

Lucy L. Thomson, Esq. CISSP*

What Are the Risks? Social Engineering Fraud Schemes

Cyber risks have evolved beyond traditional hacking to include sophisticated social engineering scams that rely on unwitting insiders to effectuate the scheme. In the past three years, major companies around the world have been the victims of multi-million dollar fraud schemes that were successfully perpetrated online using social engineering.

"Fake President" fraud, recognized by the FBI as a type of business e-mail compromise (BEC), is a particularly pernicious scheme that utilizes fraudulent e-mail to impersonate the company president or C-suite executive and entice unwitting officials to wire or otherwise transfer funds to bank accounts belonging to criminals.[1] FBI officials have warned of a dramatic increase of 1,300 percent since January 2015 in BEC schemes used to defraud businesses of all types and sizes, from large corporations and technology companies to small businesses and non-profit organizations.[2]

The FBI considers BEC a "sophisticated scam" that targets businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The Financial Services Information Sharing and Analysis Center (FS-ISAC) and federal law enforcement agencies released a joint alert, warning companies of this sophisticated BEC wire payment scam.[3] Criminals carry out the fraud by compromising legitimate business e-mail accounts

---

* Lucy Thomson is principal of Livingston PLLC, a Washington, D.C. law firm that advises government and private sector clients on legal and technology issues related to cybersecurity, global data privacy, and compliance and risk management. She served as 2012-13 Chair of the ABA Section of Science & Technology Law and is a member of the Cybersecurity Legal Task Force. She is the editor of the ABA *Data Breach and Encryption Handbook* and a contributing author to the *ABA Cybersecurity Handbook*. A career federal criminal prosecutor at the U.S. Department of Justice and a former senior engineer at CSC, a global technology company, she was appointed Consumer Privacy Ombudsman in 21 federal bankruptcy cases and has overseen the disposition of 250 million electronic records. She received a Master's degree from Rensselaer Polytechnic Institute (RPI) in 2001, earned the CISSP and CIPP/US/G certifications, and holds a J.D. degree from the Georgetown University Law Center.

[1] Fraud warning: increase in "Fake President" frauds, *available at* https://www2.deloitte.com/lu/en/pages/aboutdeloitte/articles/fake-presidents.html; ALERT: Fake President Fraud, March Belgium, *available at* http://belgium.marsh.com/Actualit%C3%A9setperspectives/Parolesdexperts/Articles/ID/42122/ALERT-Fake-President-Fraud.aspx.

[2] FBI Public Service Announcement: Business e-Mail Compromise: The 3.1 Billion Dollar Scam (Alert No. 1-061416-PSA) (June 14, 2016), *available at* https://www.ic3.gov/media/2016/160614.aspx#ref1.

[3] Federal Bureau of Investigation, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the United States Secret Service, Fraud Alert: Business E-mail Compromise Continues to Swindle and Defraud U.S. Businesses, (June 19, 2015), *available at* https://www.fsisac.com/sites/default/files/news/BEC_Joint_Product_Final.pdf. *See*, US-CERT Fraud Alert Issued on Business Email Compromise Scam, US-CERT Security Tip (ST04-014) (rev. Jan. 24, 2017), excerpts attached hereto as Appendix A.

Lucy L. Thomson © 2017 All Rights Reserved

through social engineering or computer intrusion techniques and orchestrate the unauthorized transfers of funds.[4]

The FBI has identified a number of scenarios by which the BEC scam is perpetrated, based on analysis of victims' complaints.[5] Criminals have begun using malware to infiltrate company networks, enabling them to access legitimate e-mail conversations about invoices and billing. This information is then used when requesting a fraudulent wire transfer. The criminals will use the method most commonly associated with their victim's normal business practices, in most cases victims use wire transfers, but others use checks as a common method of payment.[6]

One striking aspect of recent BEC schemes generally is that unlike the e-mail phishing[7] attacks of past years that were designed to trick the recipient into clicking on a malicious link or opening an attachment that would download malware onto the victim's computer, many BEC attacks did not require the use of malware to be successful. More sophisticated schemes, however, have combined social engineering with the hacking and compromise of a computer, as well as phishing attacks to steal executives' credentials.[8]

These attacks have resulted in massive financial losses in 100 countries and in all 50 states, totaling as much as $3.1 billion from U.S. and international victims. The FBI has identified more than 14,000 U.S. victims.[9]

Social engineering has been a technique used by criminals for decades to defraud unsuspecting victims.[10] US-CERT[11] describes a social engineering attack this way:

---

[4] FBI Public Service Announcement: Business eMail Compromise (Alert No. 1-082715a-PSA) (August 27, 2015), *available at* https://www.ic3.gov/media/2015/150827-1.aspx.

[5] *Id*., FBI PSA No. 1-061416-PSA (June 14, 2016), *available at* https://www.ic3.gov/media/2016/160614.aspx.

[6] *Id.*

[7] Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. US-CERT Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks (rev. Jan. 24, 2017), *available at* https://www.us-cert.gov/ncas/tips/ST04-014.

[8] See, e.g., *BitPay, Inc. v. Massachusetts Bay Ins. Co.*, No. 1:15-CV-03238, 2015 WL 5446711 (N.D. Ga. filed Sept. 15, 2015). The Anti-Phishing Working Group has focused on the social engineering and technical subterfuge aspects of phishing seen in the BitPay fraud: "Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. *Social engineering schemes* use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as usernames and passwords. *Technical subterfuge schemes* plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords – and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes)." (emphasis added). APWG Phishing Activity Trends Report Q1 2016, *available at* http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf.

[9] *Id*., FBI PSA (Alert No. 1-061416-PSA), page 1.

[10] The Social Engineering Framework is a searchable resource with information on the psychological, physical and historical aspects of social engineering, *available at* http://www.social-engineer.org/framework/general-discussion/.

[11] US-CERT, the U.S. Computer Emergency Readiness Team in the Department of Homeland Security is responsible for providing a safer, stronger Internet by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world. *See* https://www.us-cert.gov/about-us.

> In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility. [12]

In its *Guide to Preventing Social Engineering Fraud*, Chubb identified a number of social engineering tactics[13] used by attackers, particularly to target businesses online:

- *Impersonation/pretexting*: This common form of deception may involve an attacker using a believable reason to impersonate a person in authority, a fellow employee, an IT representative, or vendor in order to gather confidential or other sensitive information.
- *Phishing/ spamming/ spear-phishing*: Phishing can take the form of a phone call or e-mail from someone claiming to be in a position of authority who asks for confidential information, such as a password. Phishing can also include sending e-mails to organizational contacts that contain malware designed to compromise computer systems or capture personal or private credentials.
- *IVR/Phone phishing* (a/k/a vishing): This telephone scam uses a technical tactic, an interactive voice response (IVR) system, to replicate a legitimate sounding message that appears to come from a bank or other financial institution and directs the recipient to respond in order to "verify" confidential information. These messages may claim to come from other seemingly "trusted" organizations such as a government agency or the police and may reference personal details obtained from social media or other sources.

The 2016 Verizon Data Breach Investigations Report has documented an increase in phishing attacks and reported that phishing has been a factor in more than two-thirds of cyber-espionage incidents for the past three years. The use of pretexting in financially motivated breaches increased in 2015.[14]

A. Types of social engineering scams

The FBI has identified a number of scenarios by which the BEC scam is perpetrated, based on analysis of victims' complaints.[15] The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds, usually by wire transfer, or sometimes using a bank check. The criminals will use the method most commonly associated with their victim's normal business practices.[16]

---

[12] *Id.* US-CERT Security Tip (ST04-014).
[13] Chubb *Guide to Preventing Social Engineering Fraud, available at* http://www.chubb.com/businesses/csi/chubb19441.pdf.
[14] Verizon 2016 Data Breach Investigations Report (Verizon DBIR), pages 17-19, 73, *available at* http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.
[15] *Id*., FBI PSA No. 1-061416-PSA (June 14, 2016), *available at* https://www.ic3.gov/media/2016/160614.aspx.
[16] *Id.*

The FBI stated that fraudulent transfers to 100 countries have been reported, with the majority going to Asian banks located within China and Hong Kong.

1. *Fake President Fraud – Business Executive Receiving or Initiating a Wire Transfer Request; also referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," "Financial Industry Wire Fraud," or "Whaling Scam" (scams target the organization's top executives or 'big fish')*

   The e-mail accounts of high-level business executives (CFO, CTO, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing these requests. In some instances a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y."[17]

2. *Business Executive and Attorney Impersonation; Confidential and Time-Sensitive Requests*

   Victims are contacted by fraudsters, who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week or be timed to coincide with the close of business of international financial institutions.[18]

3. *Business Working with a Foreign Supplier; referred to as "Bogus Invoice Scheme," "Supplier Swindle," and "Invoice Modification Scheme"*

   A business, which often has a long-standing relationship with a supplier, is asked to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Likewise, if a facsimile or telephone call is received, it will closely mimic a legitimate request.[19]

4. *Business Contacts Receiving Fraudulent Correspondence; Fake Invoices to Vendors*

   An employee of a business has his/her personal e-mail hacked. This personal e-mail may be used for both personal and business communications. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal e-mail to multiple vendors identified from this employee's contact list. The business may not become aware of the fraudulent requests until they are contacted by their vendors to follow up on the status of their invoice payment.[20]

5. *"Attorney Check Scam"*

   Attorneys are targeted to represent supposed (BEC) litigants in a payment dispute. Retainers in the form of checks are sent by (BEC) litigants to the attorney. The scam is revealed when

[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*

either the checks are found to be fraudulent or the (BEC) litigants are contacted. While the payment disputes are real, the (BEC) litigants neither contacted nor retained that attorney for legal assistance.[21]

6. *Data Theft*

   Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entities in the business organization responsible for W-2s or maintaining personally identifiable information (PII), such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipient of the fraudulent request. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. This data theft scenario first appeared just prior to the 2016 tax season.[22]

According to a new "urgent alert" issued by the U.S. Internal Revenue Service, criminals are now combining CEO fraud and W-2 phishing schemes to target a far broader range of organizations than ever before.[23] IRS Commissioner John Koskinen characterized the fraud as "one of the most dangerous email phishing scams we've seen in a long time."

Noted security researcher Brian Krebs provided some of the reasons why BEC fraud has been so successful:

> On the surface, business e-mail compromise scams may seem unsophisticated relative to moneymaking schemes that involve complex malicious software, such as Dyre and ZeuS. But in many ways, the BEC attack is more versatile and adept at sidestepping basic security strategies used by banks and their customers to minimize risks associated with account takeovers. In traditional phishing scams, the attackers interact with the victim's bank directly, but in the BEC scam the crooks trick the victim into doing that for them.[24]

Planning and Carrying Out Online BEC Fraud Schemes – Hacker Strategies

The 2016 Verizon DBIR reported seeing breaches caused by financial pretexting, which they refer to as 'CEO Fraud.' The authors characterize the criminal operations (with some wry humor) this way:[25]

> This involves old-fashioned social engineering of employees with the authorization to move money. E-mails purportedly from the CEO or other top executive provide instruction to transfer funds to an entity, with a seemingly valid reason provided. These may also be blended with other forms of communication. "Twas not the CEO behind that email and somebody who believed they were following legitimate instructions is not having a very good day."

BEC e-mails typically use the same format and approach. The fraud is conducted using one or more of the following methods.

---

[21] *Id.*
[22] *Id.*
[23] Krebs on Security, IRS: Scam Blends CEO Fraud, W-2 Phishing, *available at* https://krebsonsecurity.com/2017/02/irs-scam-blends-ceo-fraud-w-2-phishing/
[24] Krebs on Security, FBI: $2.3 Billion Lost to CEP Email Scams (April 18, 2016), *available at* http://krebsonsecurity.com/tag/ceo-fraud/.
[25] *Id*., Verizon DBIR, page 61.

- *Reconnaissance – Targeting Employees*

  The perpetrators study and monitor their selected victims using social engineering prior to initiating a BEC scam. Victims may first receive "phishing" e-mails requesting details regarding the business or individual being targeted (name, travel dates, etc.). Common recipients of BEC scams include accountants, real estate agents, title companies, attorneys involved in real estate transactions, bookkeepers and other financial officers.

  Thus, criminals are able to accurately identify the individuals and protocols necessary to perform wire transfers within the specific business environment of the organization.

- *Typo-squatting* – The criminal creates a "look-alike" domain name that resembles the actual domain of the targeted company (one or two letters off, *e.g.* "myydomain.com" versus "mydomain.com"; or substituting the letter "L" for the numeral 1), *e.g.* "examp1e.com" or "example.co"). These domains are often registered on the same day that the e-mail is sent, often within a matter of hours.

- *Crafting the e-mail* – Hackers spoof company e-mail or use social engineering to assume the identity of senior officials such as the CEO, a company attorney, or trusted vendor.

  Criminals will forge the sender's e-mail address displayed to the recipient, so that the e-mail will include the address of the company's domain. However, the "reply-to" address is the spoofed external domain, often a free e-mail service, ensuring that any replies are sent to the hacker. The victims often do not realize they are being duped.

- *Content of e-mails tailored to the company*

  Using the same techniques, "phishing" text messages can be sent purporting to be from the recipient's bank. Hackers use software that alters the sender ID so it appears with the name of the bank, potentially within an existing thread of genuine messages, so the user believes the e-mail is trustworthy and is likely to respond.

  After researching employees who manage money, hackers use language specific to the company they are targeting. They request by e-mail a wire transfer using dollar amounts that would be usual and expected in the company to lend legitimacy.

- *Urgency* – The request always contains a sense of urgency or secrecy and it is followed up with a pattern of increasing urgency so the hacker can know the funds were sent.

- *Avoiding suspicion* – Criminals may plan to initiate the fraudulent e-mail wire transfer request while the executive being impersonated is away from the office.

  The e-mails may state that the CEO is traveling or is in a meeting and cannot accept phone calls. Many of the e-mails have "sent from my iPad" appended, to suggest the sender is on the road or to excuse typos in the message. They are often sent on a Friday to give the criminals more time to avoid detection.

Types of Attacks – Illustrative examples of social engineering scams and the resulting losses

News reports, Securities and Exchange Commission (SEC) filings, and cases in litigation provide an inside look at some of the specific techniques used to defraud high-level executives and key figures in global companies. Many of these BEC frauds have contributed to the greatest reported losses since 2015.

The methodology and details of how these schemes are architected and carried out are often important in determining whether a particular fraud incident is covered under an insurance policy.

1) **Fake President Fraud – CEO Fraud**

- **Xoom** (NASDAQ:XOOM) California, an international money transfer company (online wire-transfer provider) acquired by PayPal in mid-2015 – $30.8 million loss

Xoom reported an incident involving employee impersonation and fraudulent requests targeting the company's finance department. As a result, $30.8 million in corporate cash was transferred to overseas accounts.[26]

Impact of the Fraud – $30.8 million loss in Q4 2015. The CFO resigned. The Company's audit committee authorized an independent investigation by outside advisors. The company has implemented additional internal procedures, and federal law enforcement authorities are actively pursuing a multi-agency criminal investigation. Stock for the low-cost payments company, which competes with Western Union, dipped 14%, or $31 million, after the loss was announced, but later recovered.

- **Scoular Co**., an Omaha-based commodities trader, one of Omaha, Nebraska's oldest companies (and one of the top privately held companies in the U.S.) – $17.2 million loss

The company reported an incident involving a spear-phishing wire fraud scam. According to Omaha.com, a company executive wired the money in installments last summer to a bank in China after receiving e-mails ordering him to do so.

- **Ubiquiti Networks**, a San Jose-based wireless networking technology company – $46.7 million

In a 2015 SEC filing,[27] Ubiquiti Networks reported an incident involving employee impersonation and fraudulent requests from an outside entity targeting the company's finance department. This fraud resulted in wire transfers of funds aggregating $46.7 million held by a company subsidiary incorporated in Hong Kong to other overseas bank accounts held by third parties, believed to be the attackers.

Impact of the Fraud – As soon as the company became aware of the fraudulent activity, it initiated contact with its Hong Kong subsidiary's bank and promptly initiated legal proceedings in various foreign jurisdictions. As a result of these efforts, the company has recovered $8.1 million of the amounts transferred. Furthermore, an additional $6.8 million are currently subject to legal injunction and reasonably expected to be recovered by the company in due course. The company is continuing to pursue the recovery of the remaining $31.8 million and is cooperating with U.S. federal and numerous overseas law enforcement authorities who are actively pursuing a multi-agency criminal investigation.

In its SEC filing, Ubiquiti said that this is an isolated event and does not believe its technology systems have been compromised. A 2015 investigation by outside advisors uncovered no evidence that company systems were penetrated or that any corporate information, including

[26] Xoom SEC Form 8-K, Item 8.01 Other Events (December 30, 2014), *available at* https://www.sec.gov/Archives/edgar/data/1315657/000110465915000360/a15-1144_18k.htm.

[27] Ubiquiti Networks, Inc. Form 8-K, Item 8.01 Business Fraud (August 4, 2015); *available at* https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm.

financial and account information, was accessed. The investigation found no evidence of employee criminal involvement in the fraud. The company, its Audit Committee and advisors have concluded that the company's internal control over financial reporting is ineffective due to one or more material weaknesses. The company has implemented enhanced internal controls over financial reporting.

- **FACC** (Austria),[28] an Austrian aerospace manufacturer that designs and supplies parts to Airbus and Boeing – $54 million loss

In January 2016 FACC AG announced that it had became a victim of fraudulent activities involving communication and information technologies. Based on the current state of the forensic and criminal investigations, the financial accounting department of FACC Operations GmbH was the target of cyber fraud.

Impact of the Fraud – FACC's IT infrastructure, data security, and IP rights, as well as the operational business of the group, were not affected by the criminal activities. The damage is an outflow of approximately EUR 50 million of liquid funds. The management board has taken immediate structural measures and is evaluating damages and insurance claims.

- **Crelan Bank** (Belgium), Belgian Bank Crelan, Crédit Agricole's Belgian subsidiary – €70 million ($75.8 million) loss

Crelan Bank reported that it was the victim of CEO fraud, a targeted spear-phishing wire fraud campaign.[29] The fraud was discovered during an internal audit.

Impact of the Fraud – To date, this is the largest reported loss from a targeted spear-phishing wire fraud attack.

- **Mattel**, U.S. toymaker, Barbie dolls and other toys – $3 million loss/recovered

The fraud was the result of a well-researched phishing e-mail directed to an unnamed finance executive who was on the approved sign-off list for large cash transfers. The e-mail appeared to be written by the new CEO Christopher Sinclair, one of two executives also required to sign off on cash transfers. Attackers had harvested open source information on Mattel staff, enabling them to understand its corporate hierarchy and payment patterns. Company officials wired $3 million to an account of Chinese hackers at the Bank of Wenzhou, China.[30]

Impact of the Fraud – The recovery was mostly due to luck: the cash was wired on a Chinese bank holiday so the funds were held up and later returned by fast-acting authorities. Mattel contacted the FBI and local and foreign banks; after a visit to the Bank of Wenzhou headquarters by an anti-fraud investigator with an FBI letter in hand, the funds were returned. The bank is located in a region infamous for tunneling cash stolen from CEO phishing scams.

The Barbie-company has since tracked a dozen more chief executive officer scams that have arrived since the attack.

[28] FACC AG Interim Report, Q3 2015/16, page 20, *available at* http://www.facc.com/en/Investor-Relations/Reports.
[29] http://www.crelan.be/sites/default/files/COMM/presse/pb_01-2016_nl.pdf (in Dutch).
[30] Darren Pauli, Chinese Bank Holiday Foils Near Perfect 3 Million Mattel Fleecing, The Register (April 2016), *available at* www.theregister.co.uk/2016/04/06/chinese_bank_holiday_foils_nearperfect_3_million_mattel_fleecing/

- **Medidata Solutions Inc.** (NASDAQ: MDSO), New York, N.Y., provides applications, analytics and benchmarks to facilitate medical research and run clinical trials – $4.8 million loss

Insurance Litigation: Medidata Solutions, Inc. v. Federal Ins. Co., No. 15-cv-00907, Dkt. No. 64 (S.D.N.Y. Mar. 9, 2016)

Nature of the Fraud: In 2014 Medidata Solutions discovered that it had been the subject of an international wire transfer fraud.[31] e-mails that purported to come from company executives, including the CEO and an attorney, instructed mid-level employees in the Finance Department to wire money to a Chinese bank. The impostor's e-mail included the executive's picture and the CEO's forged signature, and the "From" line was altered to appear as if it had been sent from the executive's company e-mail address. The employees were instructed to contact another individual, who posed as an attorney. Through a series of e-mails and phone calls, the impostor and fake attorney convinced the employees to transfer nearly $4.8 million to a bank account in China. The company caught on – and the impostor disappeared – when the impostor requested an additional $4.8 million. The money that had already been transferred was never recovered.

The SEC filing stated: "While the Company believes that it has appropriate internal controls, its audit committee and advisors are reviewing these controls and processes as part of the investigation. The Company has contacted federal law enforcement authorities and has implemented additional internal procedures to prevent future incidents."

- **BitPay**, Atlanta, Georgia, Global bitcoin[32] payment processor – $1.85 million in digital currency loss

Insurance Litigation: *BitPay, Inc. v. Massachusetts Bay Ins. Co.*, No. 1:15-CV-03238, 2015 WL 5446711 (N.D. Ga. filed Sept. 15, 2015); case settled, parties jointly requested dismissal with prejudice on June 1, 2016

Multi-Pronged Nature of the Fraud: This complex fraud was launched through the use of a spear-phishing attack and successfully carried out with social engineering.[33] The perpetrator, who had previously compromised the computer and taken over the e-mail account of BTC Media CEO David Bailey, initiated the attack by sending a phony e-mail (purportedly from Bailey) to BitPay CFO Bryan Krohn, requesting a comment for an article by journalist Bailey for the publication yBitcoin. The e-mail directed Kohn to click on the link to a Google document. Bryan Krohn responded to the e-mail and clicked on the link which directed him to a website controlled by the hacker; there Krohn entered the authentication credentials for his BitPay corporate e-mail account.

After capturing Krohn's BitPay credentials, the hacker used that information to prompt CEO Stephen Pair and executive chairman Tony Gallippi to authorize three payments totaling 5,000 BTC, including one transaction from a wallet on the bitcoin exchange Bitstamp.

---

[31] *Medidata Solutions, Inc.*, SEC Form 8-K, Item 8.01 Other Events (September 25, 2014), *available at* https://www.sec.gov/Archives/edgar/data/1453814/000119312514353189/d795328d8k.htm.

[32] Bitcoin is a digital currency transferred electronically via the Internet and can be used to pay for products and services.

[33] Massachusetts Bay initial denial letter, Case 1:15-cv-03238-SCJ Document 1-1 Filed 09/15/15 Pages 34-36 of 48.

This fraud was successful because after capturing Krohn's BitPay corporate e-mail, a key detail in the e-mails was now accessible to the fraudster: the fact that BitPay did not require SecondMarket to advance pay for bitcoins it received from the company.

Using this information, the individual crafted an e-mail chain showing a conversation between Krohn and SecondMarket VP Preston Blankenship regarding a purchase of 1,000 BTC. The e-mail requested that 1,000 bitcoins be transferred to SecondMarket at a specific wallet address provided. At 3:33 PM the bitcoins were sent from BitPay's hot wallet.

Less than an hour later, the criminal controlling Krohn's e-mail requested an additional 1,000 BTC be sent to the same bitcoin address. This amount was then transferred from an account held on Bitstamp by Gallippi after Pair indicated by e-mail that there were insufficient funds in BitPay's "warm" wallet following the second request.

The next day, Krohn's e-mail was used to request that Pair send an additional 3,000 BTC to another address said to be controlled by SecondMarket. Pair responded "to confirm that this request, which exceeded the usual 1000-2000 daily bitcoin amount between the companies, was valid." The assailant responded by copying an e-mail address purportedly from SecondMarket and confirming that the request was valid.

After processing the transaction, Pair confirmed the move by e-mail and copied SecondMarket employee Gina Guarnaccia. Guarnaccia wrote back that she "did not send the prior e-mail noting the 3,000 bitcoins and address for them to be sent, and that SecondMarket did not purchase the bitcoins."

- **Long Beach Escrow Corporation,** California real estate agency **–** $250,000 loss

Insurance Litigation: *Maxum Indemnity Co. v. Long Beach Escrow Corp.*, No. 2:16-CV-05907, 2016 WL 4199087 (C.D. Cal. filed Aug. 8, 2016). Case settled; complaint voluntarily dismissed in September 2016

Impact of the Fraud: Real estate firm Keely Partners sued Long Beach Escrow Corporation (LBEC) in April for negligence and breach of fiduciary duty after the escrow company was duped into wiring more than $250,000 to hackers who had taken control of a Keely partner's e-mail account.

- **Te Wananga o Aotearoa** *(*New Zealand), one of New Zealand's largest learning institutions – $US79,000 ($118,000) loss

The executive director of finance at Te Wananga o Aotearoa, Bronwyn Koroheke, transferred $US79,000 ($118,000) to an offshore bank account after receiving an e-mail which appeared to be from her chief executive Jim Mather telling her to send the money.

In fact, the e-mail was from Chinese-based fraudsters running the scam. They forged Mather's e-mail address to make it look like he was sending it from a mobile device.

Impact of the Fraud: The chief financial officer left her job after falling for the e-mail scam.

- **AF Global**, privately-held Houston, Texas company that provides engineering, manufacturing and aftermarket services for the oil and gas, power generation, industrial and aerospace markets – $480,000 loss

Insurance Litigation: *Ameriforge Grp. Inc. v. Fed. Ins. Co.*, No. 4:16-CV-00377, 2016 WL 67625 (S.D. Tex. filed Jan. 4, 2016)

Nature of the Fraud: On May 21, 2014, the AF Global Director of Accounting received an e-mail purporting to be from the company's CEO. The e-mail instructed the director to cooperate with a named attorney to handle a highly confidential financial operation. The e-mail instructions received advised that this was a confidential financial operation, which should take priority over other tasks. The e-mail indicated that he would receive a call purportedly from an attorney for KPMG. The Accounting Director then received follow-up telephone and e-mail communications from the purported attorney, who explained that the Director should immediately wire $480,000 to a Chinese bank account to pay the due diligence fees related to a sensitive acquisition in China that AF Global was pursuing.

A week after the director transferred the funds, he received another e-mail requesting a second transfer in the amount of $18 million. The Director became suspicious and notified his supervisors, who determined the company had been scammed. After determining that both requests were fraudulent, AF Global attempted, without success, to recall the wire from Bank of America and reported the matter to the police.

- **Quality Sausage Co.,** Texas food producer, $1 million loss ($90,000 recovered)

Insurance Litigation: Quality Sausage Company LLC et. al. v. Twin City Fire Ins. Co., Case No. 4:17-cv-111 (S.D. Texas, filed Jan. 13, 2017)

HM International (HMI) of Oklahoma is a subsidiary of QSC. Gregory Geib and Kathryn Geib are HMI clientele who provide HMI with accounting, tax preparation, and insurance services.

Nature of the Fraud: HMI officer Tamara Rains received an e-mail purporting to be from Greg Geib directing HMI to wire transfer $1 million from a Geib bank account to a Bank of America account. After receiving a second e-mail request purportedly from Geib directing a second wire transfer, Reins called Geib who indicated that he did not send the e-mail or instruct either wire transfer. According to the complaint, upon information and belief, an unknown hacker, using a "man-in-the-middle attack," sent a fraudulent e-mail. When plaintiffs learned that a large part of the $1 million had been transferred to Singapore they initiated contact with Singapore authorities who are holding approximately $351,506 in escrow while investigating the theft.

- **Principle Solutions Group,** Georgia, technology staffing and consulting firm, $1.7 million loss

Insurance Litigation: Principle Solutions Group, LLC v. Ironshore Indemnity, Inc., No. 1:15-CV-4130, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016)

Nature of the Fraud: In July 2015 the controller of Principle Solutions Group received an e-mail purportedly from one of the firm's managing directors, instructing her to issue a wire transfer that day in coordination with an attorney named "Mark Leach" of Alston & Bird.[34] The controller then received an e-mail from "Mark Leach" with instructions to wire a payment to a bank in China.

When the controller logged into Principle's online account with its bank to initiate the transfer, the bank's fraud prevention unit called and e-mailed the controller to request verification of the transaction, including confirmation of how Mr. Leach had received the wire instructions. The

[34] *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, No. 1:15-CV-4130, 2016 WL 4618761, at *1 (N.D. Ga. Aug. 30, 2016).

controller called Mark Leach, who said that he had received the instructions from the firm's managing director who had allegedly sent the original e-mail. The controller relayed this information to the bank, which then released the funds to the Chinese bank. The next day, the controller spoke with the managing director and told him the wire transfer had been completed successfully. The managing director said he had no knowledge of the transfer, the Mr. Leach, or the previous day's e-mails. By the time the bank's fraud department tried to recover the funds, it was too late.

2) ***"Bogus Invoice Scheme," "Supplier Swindle," and "Invoice Modification Scheme"***

- **Aqua Star Corp.**, Seattle, WA Seafood distributor, importer, processor, wholesaler – $700,000 loss

Insurance Litigation: *Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co. of Am.*, 2016 WL 3655265 (W.D. Wa. July 8, 2016)

Nature of the Fraud: A hacker had monitored e-mail exchanges between an employee of Aqua Star and an employee of Zhanjiang Longwei Aquatic Products, Aqua Star's supplier of frozen shrimp.

The hacker then sent a "spoofed" e-mail directing the Aqua Star employee to change the bank account information for future wire transfers to Longwei, causing some $700,000 intended for Longwei to be misdirected to the hacker.

In 2013, a hacker impersonating a vendor directed an Aqua Star employee to change the bank account information for future payments to the vendor. The employee entered the new account information into Aqua Star's computer system and initiated the transfers with the bank.

- **Taylor and Lieberman**, California, accounting firm that issues payments and transfers funds on behalf of its clients – $100,000 loss

Insurance Litigation: Taylor and Lieberman v. Fed. Ins. Co., No. 2:14-CV-03608 (C.D. Cal. June 18, 2015); appealed to the Ninth Circuit

Nature of the Fraud: An imposter fraudulently took control of the e-mail account of the accounting firm's client. Purporting to be the client, the criminal sent e-mails to the accounting firm requesting that the firm wire money from the client's account, over which the firm had power of attorney, to an account in Malaysia. The Taylor employee wired several payments before discovering the fraud. By that time, it had lost almost $100,000 of its client's money.

- **Apache Corp**., Houston, Texas, oil and gas exploration and production company – $2.4 million loss

Insurance Litigation: Apache Corp v. Great Am. Ins. Co., No. 4:14-CV-00237, 2015 WL 7709584 (S.D. Tex. Aug. 7, 2015), *rev'd*, --- F. App'x ---, 2016 WL 6090901 (5th Cir. Oct. 18, 2016)

Nature of the Fraud: An Apache employee received a call and then an e-mail attaching a letter from a person claiming to be an employee of one of Apache's vendors, requesting a change of the account information to which payment was to be sent for the vendor's services. Another Apache employee called the number on the letterhead to verify the request and, once approved by an Apache supervisor, the change was made, and $2.4 million was directed to the fraudulent account.

3) Attorney Check Scam

Owens Schine & Nicola P.C., Connecticut law firm – $200,000 loss

Insurance Litigation: *Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am.*, No. CV-09-5024601-S, 2011 WL 3200296 (Conn. Super. Ct. June 24, 2011), *vacated*, No. CV-09-5024601-S, 2012 WL 12246940 (Conn. Super Ct. Apr. 18, 2012)

Impact of the Fraud: An imposter who purported to be an attorney from North Carolina asked the law firm to help a Chinese client collect a payment in Connecticut. The potential "client" e-mailed the law firm, which accepted the representation; Owens agreed to act as an intermediary. Subsequently, the fraudster "client" e-mailed the law firm that its debtor had agreed to send the funds owed to the firm's office. When a bank check arrived, the law firm deposited it into its client IOLTA account and, pursuant to the "client's" e-mailed instructions, had its bank wire the funds, less a fee, to the "client's" account in a South Korean bank. The original check Owens received was fraudulent, and Owens's bank charged the firm for the full amount. The law firm faced nearly a $200,000 loss in its IOLTA account.

B. Meeting the Challenges of Social Engineering Fraud

Organizations must take proactive steps to establish appropriate policies and procedures to address the risks of social engineering fraud, and educate all employees about their role and responsibility to help prevent this rapidly growing problem.

The FBI has said that as devastating as this crime is, it is equally easy to thwart. Executives must develop the habit of verifying the authenticity of e-email requests to send money. The best way to do this is through in-person conversations using a known telephone number.

The important recommendations of the FBI, US-CERT, and the Chubb Group of Insurance Companies are included with this article as Attachment A.

ATTACHMENT A

FBI Public Service Announcement
June 14, 2016
Alert Number I-061416-PSA

Business E-mail Compromise: The 3.1 Billion Dollar Scam

SUGGESTIONS FOR PROTECTION AND BEST PRACTICES

Businesses with an increased awareness and understanding of the BEC scam are more likely to recognize when they have been targeted by BEC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments.

Businesses that deploy robust internal prevention techniques at all levels (especially targeting front line employees who may be the recipients of initial phishing attempts), have proven highly successful in recognizing and deflecting BEC attempts.

Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request.

The following is a compilation of self protection strategies provided in the BEC PSAs from 2015.

- Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional IT and financial security procedures, including the implementation of a 2-step verification process. For example -
    - Out of Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.
    - Digital Signatures: Both entities on each side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.
    - Delete Spam: Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.
    - Forward vs. Reply: Do not use the “Reply” option to respond to any business e-mails. Instead, use the “Forward” option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient’s correct e-mail address is used.
    - Consider implementing Two Factor Authentication (TFA) for corporate e-mail accounts. TFA mitigates the threat of a subject gaining access to an employee’s e-mail account through a compromised password by requiring two pieces of information to login: something you know (a password) and something you have (such as a dynamic PIN or code).

  Significant Changes: Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been through company e-mail, the request could be

fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of abc_company.com would flag fraudulent e-mail of abc-company.com.
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign-off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all e-mail requests for transfers of funds to determine if the requests are out of the ordinary.

Additional information is publicly available on the United States Department of Justice website www.justice.gov publication entitled “Best Practices for Victim Response and Reporting of Cyber Incidents”.

WHAT TO DO IF YOU ARE A VICTIM

If funds are transferred to a fraudulent account, it is important to act quickly:

- Contact your financial institution immediately upon discovering the fraudulent transfer
- Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds
- File a complaint, regardless of dollar loss, at www.IC3.gov

When contacting law enforcement or filing a complaint with the IC3, it is important to identify your incident as “BEC”, provide a brief description of the incident, and consider providing the following financial information:

- Originating[4] Name:
- Originating Location:
- Originating Bank Name:
- Originating Bank Account Number:
- Recipient[5] Name:
- Recipient Bank Name:
- Recipient Bank Account Number:
- Recipient Bank Location (if available):
- Intermediary Bank Name (if available):
- SWIFT Number:
- Date:
- Amount of Transaction:
- Additional Information (if available) - including “FFC”- For Further Credit; “FAV” – In Favor Of:

Filing a complaint with IC3

Victims should always file a complaint regardless of dollar loss or timing of incident at www.IC3.gov and, in addition to the financial information, provide the following descriptors:

- IP and/or e-mail address of fraudulent e-mail
- Date and time of incidents
- Incorrectly formatted invoices or letterheads
- Requests for secrecy or immediate action
- Unusual timing, requests, or wording of the fraudulent phone calls or e-mails
- Phone numbers of the fraudulent phone calls
- Description of any phone contact to include frequency and timing of calls
- Foreign accents of the callers
- Poorly worded or grammatically incorrect e-mails
- Reports of any previous e-mail phishing activity

https://www.ic3.gov/media/2016/160614.aspx

* * * * *

US-CERT
Security Tip (ST04-014)

Avoiding Social Engineering and Phishing Attacks

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the Internet before checking a website's security (see Protecting Your Privacy for more information).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org)
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (see Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam).
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

- Watch for other signs of identity theft. (See Preventing and Responding to Identity Theft for more information.) Consider reporting the attack to the police, and file a report with the Federal Trade Commission.

US-CERT Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks (revised January 24, 2017), *available at* https://www.us-cert.gov/ncas/tips/ST04-014

* * * * *

Chubb Guide to Preventing Social Engineering Fraud

Counter Measures For Combating Social Engineering Fraud

The best defense for combating social engineering fraud is awareness through corporate culture, education and training. It is not enough for a workforce to simply follow a policy guideline; employees must be educated on how to recognize and respond to an attacker's methods and thus become a "human firewall."

A proper counter measure training program should include the following measures:

- Conduct a **data classification assessment**, identifying which employees have access to what types and levels of sensitive company information. Know who the primary targets of a social engineering scheme are likely to be. Remember, all employees are at risk.

- **Never release confidential or sensitive information to someone you don't know** or who doesn't have a valid reason for having it – even if the person identifies himself or herself as a co-worker, superior or IT representative. If a password must be shared, it should never be given out either over the phone or by email.

- Establish procedures to **verify incoming checks and ensure clearance prior to transferring any money by wire.**

- Reduce the reliance on email for all financial transactions. If email must be used, **establish call-back procedures to clients and vendors** for all outgoing fund transfers to a previously established phone number, or implement a customer verification system with similar dual verification properties.

- Establish procedures to **verify any changes to customer or vendor details**, independent of the requester of the change.

- **Avoid using or exploring "rogue devices"** such as unauthenticated thumb/flash drives or software on a computer or network.

- **Be suspicious of unsolicited emails** and only open ones from trusted sources. Never forward, respond to or access attachments or links in such emails; delete or quarantine them.

- **Avoid responding to any offers made over the phone or via email.** If it sounds too good to be true, then it probably is. This could include unsolicited offers to help to solve a problem such as a computer issue or other technical matter.

- **Be cautious in situations where a party refuses to provide basic contact information**, attempts to rush a conversation (act now, think later), uses intimidating language or requests confidential information.

- Physical documents and other tangible material such as computer hardware and software should **always be shredded and/or destroyed prior to disposal** in any on-site receptacles, such as dumpsters.

  Proactively combat information security complacency in the workplace by implementing internal awareness and training programs that are reviewed with employees on an ongoing basis. This includes developing an incident reporting and tracking program to catalog incidents of social engineering and implementing an incident-response strategy.

- **Train customer service staff to recognize psychological methods that social engineers use:** power, authority, enticement, speed and pressure. If it is important enough to move quickly on, it's important enough to verify.

- Consider **conducting a recurring, third-party penetration test** to assess your organization's vulnerabilities, including unannounced random calls or emails to employees soliciting information that should not be shared.

- **Guard against unauthorized physical access** by maintaining strict policies on displaying security badges and other credentials and making sure all guests are escorted. Politely refuse entry to anyone "tailgating." Keep sensitive areas, such as server rooms, phone closets, mail rooms and executive offices, secured at all times.

- **Monitor use of social media outlets, open sources and online commercial information** to prevent sensitive information from being posted on the Internet.

Chubb Group of Insurance Companies, 14-01-1157 (ed. 10/14), pages 6-7, *available at* http://www.chubb.com/businesses/csi/chubb19441.pdf