December 21, 2017

LAW360

**Portfolio Media. Inc.** | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# The Other Cyberthreat: Business Email Compromise Schemes

By **David Chaiken, Mark Ray and Brea Croteau**

David Chaiken

Mark Ray

Brea Croteau

By now, it has become clear that virtually any type of organization could be the target of a large-scale computer-based data breach incident, from multinational corporations to local school systems. Indeed, many cybersecurity professionals accept the notion that, for nearly any entity, the question is when, not if, it will experience such an incident. Further, the consequences of these incidents can be significant, often triggering internal investigations, regulatory scrutiny, class action lawsuits, congressional inquiries, reputational harm, the departures of key executives, adverse media coverage, and, in at least one recent example, a $100,000 ransom payment.[1]

Each public revelation of such a breach — most of which involve hackers accessing or acquiring large quantities of personally identifiable information (PII) — generates front-page newspaper headlines, armchair quarterbacking by cybersecurity professionals, and the inevitable comparisons to other big data breaches to assess and rank its relative size and scope.[2] And like a mini-mite soccer game, in which the players swarm to the ball like moths drawn to a light, the media, lawyers, regulators, companies and cybersecurity professionals obsess over each new incident, trying to assess how the intrusion might have been prevented.

But in our view, this obsessive focus on large-scale, PII-based data breaches does a disservice to businesses and consumers because there is an equally or even more pervasive and damaging cyberthreat: the business e-mail compromise scheme.[3] Also known as the "CEO email scam," the FBI estimates that these schemes have resulted in billions of dollars in actual and attempted losses to individuals and organizations around the world over the past four years.[4] In fact, in an incident reported in May 2016, a single company suffered an actual loss of $47 million as a result of such a scheme, leading to the dismissal of its CEO.[5] And just last week, there was news relating to two significant business email compromise schemes, one involving a $100 million scam that victimized Google and Facebook, and another involving a $25 million scam that targeted New York-area businesses.[6] In both cases, some — but not all — of the funds have been recovered.

So, what exactly are business email compromise schemes, who do they victimize, why are they increasingly common, and what can be done to guard against them and to limit the damage?

**What are business email compromise schemes and who are their victims?**

In the typical business email compromise scheme, the perpetrators send an email to an individual in the accounting or finance department of a company, often posing as the company's CEO or other senior executive, requesting a wire transfer. Having conducted basic internet research to identify the personnel within those departments who are responsible for handling wire or electronic funds transfers, the names of the CEO and other senior executives likely authorized to request and approve

such payments, and the types of email domains and signatures used by company employees, the perpetrators can carefully craft a realistic, legitimate-looking wire transfer request from a specific executive to a particular employee.[7] The unsuspecting employee then initiates a fraudulent wire transfer in the requested amount to the bank account of the perpetrators' choosing. Unlike many email scammers of the past, the perpetrators of these schemes often use near-perfect language, grammar and spelling, making the fraud harder to detect.

There are several methods that email scammers use to commit this crime, including:

- Email Spoofing: There are many free and easily downloadable software programs that allow scammers to design and send an email that appears to come from the entity's legitimate email domain address, but actually originates from somewhere else.

- Email Compromise: Through malware, key loggers or other exploits, an employee's email credentials and account can be compromised and used by perpetrators to send the email from a web-based email portal, or directly from the employee's computer.

- Look-Alike Domain Addresses: Perpetrators of these schemes often register internet domain addresses that are nearly identical to the victim entity's true domain address, but use one or two different characters that make the difference almost imperceptible. In a recent case, for example, the accounting department of Luminant Corporation, a Texas electric utility company, received a fraudulent email purporting to be from a senior corporate executive at the email domain, "@luminiant.com," and did not notice the discrepancy with the true domain, "@luminant.com," before sending hundreds of thousands of dollars to the scammers' bank accounts in London and Hong Kong.[8]

Other business email compromise schemes offer variations of the same theme. For example, whereas in some cases the perpetrators use look-alike domain addresses, in other cases hackers will compromise a third-party vendor, customer or service provider's genuine email account, so that the fraudulent emails arrive from a legitimate external address and the victim entity has no reason to suspect wrongdoing. In another variation, the scammers merely pose as a third-party vendor, customer or service provider, which can be nearly as effective. In April 2017, for example, an Oregon university wired $1.9 million to pay a construction company for the construction of a new campus pavilion and student recreation center.[9] But instead of sending the money to the correct account, the school wired the funds to email scammers, who are believed to have gathered enough details about the project from public sources to convincingly pose as construction company officials requesting payment.

Virtually any organization that participates in wire or other electronic funds transfers is a potential target of a business email compromise scheme, as evidenced by the recent $100 million scam that victimized Google and Facebook.[10] That said, private, family owned businesses; small- and medium-sized businesses (especially those that engage in overseas transactions or work with foreign suppliers); wealth management firms; school systems; and other organizations with less sophisticated internal controls over the wiring and disbursement of money are more likely to be victimized by such schemes.

**Why are business email compromise schemes increasingly common?**

The FBI estimates that actual and intended losses from business email compromise schemes have increased by over 2,000 percent since the FBI began tracking them in late 2013, and that victims suffered actual and attempted loses of over $1.5 billion in the U.S. and $5 billion globally between October 2013 and December 2016.[11] We believe that there is a simple explanation for this explosive growth.

For those who might be inclined to commit cybercrimes, a business email compromise scheme is a direct hit, akin to reaching directly into a victim's pocket and removing a handful of cash. In contrast, although large-scale data breaches allow hackers to collect PII, bank account information, email addresses or other information of large numbers of people, the hackers cannot immediately or easily monetize the purloined information. They can only profit by selling it to others, or by using the

information to commit other crimes, such as by fraudulently applying for credit or filing fraudulent income tax returns, known as stolen identity refund fraud.[12] In this way, the fraud is far more attenuated, risky and each step increases the hacker's risk of detection by law enforcement. Financial institutions and the cybersecurity community have also greatly improved fraud detection and monitoring in recent years, including employing nearly real-time transaction monitoring that quickly renders stolen account numbers and PII useless to cyber thieves.

Similarly, many of the big PII-based data breaches result in the collection of nonmonetizable information, such as customer records, email addresses, social media login credentials, or the collection of financial transaction card numbers (i.e., credit and debit card numbers) that can be fairly easily disabled by the card issuers, and cannot actually be used to open fraudulent bank or credit accounts. Although hackers could use this information to engage in social engineering efforts to victimize the breach victim or other organizations or individuals, additional steps are needed to monetize the fraud.

More than anything, this probably explains the alarming increase in these schemes. There is no extra step needed to monetize the theft, no need to prepare and file a fraudulent loan application or tax return, and no need to sell stolen PII or social media login credentials over the so-called "dark web."[13]

**What can be done to guard against these schemes and to limit the damage?**

Here are a few basic steps that can be taken to protect yourself and your organization:

**Require Multifactor Authentication:** Organizations can significantly reduce risk by employing multifactor authentication. This involves requiring multiple pieces of evidence to verify identity and authenticate an interaction, such as codes, pins, passwords and different mediums, such as email, secondary email and text messages. It has become nearly ubiquitous for accessing sensitive databases and systems, and it should be standard for significant funds transfers as well. Additionally, multifactor authentication should not be viewed solely as a technological fix, but also as a procedural safeguard. For example, organizations should implement processes that prohibit acting on a large wire transfer request by email alone (regardless of the seniority of the officer or employee), instead requiring employees to pick up the phone and speak directly with the executive, customer or vendor referenced in the request to ensure that it is legitimate. Organizations should also include their financial institutions in this process and obtain assurances that such institutions also have appropriate technological and process controls in place.

**Increase Employee Training:** Training is an extremely effective and inexpensive defense against all types of cyber-based attacks and fraud. This is particularly applicable to business email compromise schemes, which exploit trust and human error rather than sophisticated malware or technological vulnerabilities. If your organization has not already implemented a security education training and awareness (SETA) program, it should do so immediately and consider making it mandatory, especially for executives and employees involved in requesting and approving wire and other funds transfers. Training should include emphasis on prohibiting C-suite or C-level executives from overriding your organization's procedural safeguards discussed above, and from inadvertently disseminating information that could be used to increase your organization's vulnerability to a business email compromise scheme (such as by revealing a key executive's vacation or travel schedule over social media).

**Install Anti-Spoofing and Email Filtering Technology:** There are many simple, affordable technologies that can identify and block potential email scams, including software that attempts to identify cloaked or spoofed email display names (which conceal the sender's true email address) and look-alike domain names. They also include software capable of filtering or quarantining certain emails based on keywords defined by your organization's information technology staff.

**Update Your Organization's Insurance Coverages:** Review your organization's insurance policies to identify gaps in coverage. There is some uncertainty in the courts over whether losses from business email compromise schemes will be covered under the computer fraud provisions of cyber liability and crime policies, given that such schemes do not involve an actual computer intrusion or network security breach, but only a duped employee sending funds on his or her own accord.[14] As a result, experts advise organizations to negotiate for broader policy language or special

endorsements to specifically insure against these schemes. Additionally, coverage amounts should be commensurate with the value of the transactions or funds transfers in which your organization engages.

**Report Incidents to Law Enforcement:** It is virtually impossible for authorities to stop these schemes if victims do not come forward. Merely reporting an incident through the FBI's Internet Crime Complaint Center may not be enough. There is no substitute for preserving and collecting the evidence in a form that could be presented in court and presenting it to your local U.S. attorney's office for investigation. Victims may be reluctant to contact prosecutors based on the assumption that the perpetrators may be overseas and beyond the reach of U.S. law enforcement. But that assumption is mistaken. The U.S. Department of Justice has dramatically increased its global cybercrime fighting efforts in recent years — establishing Computer Hacking & Intellectual Property (CHIP) units in U.S. attorney's offices throughout the country and a stand-alone cybercrime section at main justice in Washington, D.C., — and successfully charged and extradited hackers from all over the world, including the Czech Republic, Estonia, Lithuania, Malaysia, Nigeria, Russia, Ukraine, and West Africa.[15] Moreover, the FBI's Legal Attaché program, through which FBI special agents are stationed in 64 offices around the globe, has been working closely with international law enforcement partners to combat this problem. Depending upon the country in which the beneficiary bank account is located, the FBI has shown it can assist victims in freezing and even reversing transfers if notified within 24 hours of the compromise, and it has successfully done so in many cases.

## Key Takeaways

The staggering losses caused by business email compromise schemes should be a wake-up call for organizations that have not yet taken steps to protect themselves from this rapidly growing threat. A new year is always a good time to reassess your organization's internal controls, training, fraud-detection procedures, software, and insurance to update and improve your defenses and decrease your vulnerabilities. Don't let the obsessive focus on large-scale PII-based data breach incidents blind you to business email compromise schemes that are fleecing businesses and other organizations with alarming frequency.

---

*David M. Chaiken is a partner in the Atlanta office of Troutman Sanders LLP and a former assistant U.S. attorney in the Economic Crimes Section of the U.S. attorney's office for the Northern District of Georgia, where he also served as the CHIP Coordinator for several years.*

*Mark C. Ray is the managing director and head of the digital investigations and cybersecurity practice of Nardello & Co in Atlanta. He is a former special agent with the FBI's Cyber Division in Atlanta.*

*Brea M. Croteau is an associate in the government investigations, compliance and enforcement practice in Troutman Sanders' Atlanta office.*



[1] Selena Larson, "Uber's massive hack: What we know," CNN.com (Nov. 23, 2017) (reporting on company's payment of $100,000 to hackers following ransomware attack), http://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html.

[2] See, e.g., Seth Fiegerman, "The biggest data breaches ever," CNN.com (Sept. 7, 2017), http://money.cnn.com/2017/09/07/technology/business/biggest-breaches-ever/index.html; Taylor Armerding, "The 16 biggest data breaches of the 21st century," CSOonline.com (Oct. 11, 2017), https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html.

[3] Business email compromise schemes are sometimes referred to by the initials, "BEC," and are also referred to as "CEO fraud" and "man-in-the-middle" or "man-in-the-email" scams.

[4] FBI Internet Crime Complaint Center, https://www.ic3.gov/media/2017/170504.aspx#fn3

[5] Liam Tung , "CEO fired after 'fake CEO' email scam cost firm $47m," CSO Online (May 26, 2016), https://www.cso.com.au/article/600535/ceo-fired-after-fake-ceo-email-scam-cost-firm-47m/.

[6] ; Pete Brush, "Lithuanian Named In Facebook, Google Scam Working On Plea," Law360 (Dec. 13, 2017); Cara Salvatore, "Conspirator In Fake-Business-Invoice Scam Gets 41 Months," Law360, New York (Dec. 14, 2017) (reporting over $1.4 million in actual losses).

[7] In some instances, rather than identifying a specific person, the perpetrators simply correctly guess the company's generic internal wire or disbursement request address, such as "billing@yourcompany.com."

[8] United States v. Amuegbunam, No. 3:15-CR-411 (N.D. Tex.); Michelle Casady, "Nigerian Man Gets Nearly 4 Years For $3.7M Email Scam," Law360 (Aug. 29, 2017); Kevin Krause, "Nigerian student's scam tricks U.S. companies into sending him millions," Dallasnews.com (Sept. 8, 2017), https://www.dallasnews.com/news/crime/2017/09/08/nigerian-students-scam-tricks-us-companies-sending-millions; "Nigerian Man Sentenced for Role in 'Business Email Compromise' Scheme That Caused $3.7 Million Loss to U.S. Companies," DOJ.gov (Aug. 28, 2017), https://www.justice.gov/usao-ndtx/pr/nigerian-man-sentenced-role-business-email-compromise-scheme-caused-37-million-loss-us.

[9] AJ Dellinger, "Fraudulent Email: Business Email Compromise Attack Costs Southern Oregon University $2M," Int'l Bus. Times (June 13, 2017), http://www.ibtimes.com/fradulent-email-business-email-compromise-attack-costs-southern-oregon-university-2m-2551724

[10] Cara Bayles, "Big Internet Cos. Fell For $100M Email Scam, DOJ Says," Law360 (March 21, 2017).

[11] Federal Bureau of Investigation/Internet Crime Complaint Center, Alert No. I-050417-PSA, "Business E-mail Compromise, E-mail Account Compromise, The 5 Billion Dollar Scam" (May 4, 2017) (updated Dec. 31, 2016), https://www.ic3.gov/media/2017/170504.aspx.

[12] See, e.g, Editor, "Once Stolen, What Do Hackers Do With Your Data?" Secplicity.com (May 8, 2017), https://www.secplicity.org/2017/05/18/stolen-hackers-data/.

[13] "Once Stolen, What Do Hackers Do With Your Data?" Secplicity.com (May 8, 2017).

[14] Jan Larson & Caroline Meneau, "Courts Continue To Split Over Coverage For Email Scams," Law360 (Sept. 8, 2017).

[15] See, e.g., United States v. Levitskyy, No. 1:15-CR-00373-SCJ-LTW-1 (N.D. Ga.); United States v. Panin et al., No. 1:11-CR-00557-AT-AJB-2 (N.D. Ga.); United States v. Sahurovs et al., No. 0:11-CR-00177-ADM-HB-1 (D. Minn.); United States v. Ibiwoye et al., No. 1:15-CR-00457-SCJ-JSA (N.D. Ga.); Stewart Bishop, "$122M Alleged Facebook-Google Scammer To Be Extradited," Law360 (Aug. 11, 2017).