CYBERSECURITY

The CAN-SPAM Act and Its Applicability Today

by Kyle St. James, Associate, Rutan & Tucker LLP

I. What is CAN-SPAM and why should I care?
The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 sets out requirements for sending commercial/advertising electronic messages and is enforced by the Federal Trade Commission (FTC). The purpose of the Act is to restrict the number of unsolicited and unwanted emails consumers receive from companies that are advertising products or services. Even a single violation of the CAN-SPAM Act may result in hefty financial penalties.

What messages are covered?
The CAN-SPAM Act regulates "commercial electronic mail messages," defined as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." The Act applies to electronic mail and other electronic messages, including social media. Although CAN-SPAM does not regulate the *content* of emails whose primary purpose is to facilitate an already agreed-upon transaction or to update a customer about an ongoing transaction (otherwise known as "transactional" emails), the Act requires that transactional emails recite truthful routing information (e.g., sender identification). Without violating the Act, transactional emails may also include content pertaining to warranties or recalls, account balances, memberships or subscriptions, or provide employment relationship information.

To determine whether an email is covered by the Act, look to the content of the email – does the email include advertising content, transactional content or a combination? The Act distinguishes between the following situations:

(1) if the email contains only advertising content, it is covered by the Act;

(2) if the email includes both advertising and transactional content, the email has a commercial primary purpose if: (i) the subject line would be interpreted as an email that includes advertising content, or (ii) a substantial part of the transactional content does not appear at the beginning of the email;

(3) if the email includes both advertising content and content that is not transactional in nature, the email has a commercial primary purpose if: (i) a recipient reasonably interpreting the subject line of the email would likely conclude that the email contains an advertisement, or (ii) a recipient reasonably interpreting the body of the email would likely conclude that the primary purpose of the message is advertising; and

(4) an email that contains only transactional content is not a commercial email and is not regulated by the Act beyond requiring truthful routing information.

Because the line that distinguishes between commercial emails and transactional emails is often unclear, we recommend ensuring every email you send complies with the Act.

Why should I care about the requirements of CAN-SPAM?
The CAN-SPAM Act affects nearly every business. If you – as an individual, business entity or non-profit association – send commercial emails, you must abide by the Act's requirements. A single violation of the Act may result in a monetary penalty of up to $16,000. Recognizing that advertising emails are typically sent to a large mailing list, violations can get very expensive because each email that does not meet the Act's requirements is considered a violation.

II. General Overview of CAN-SPAM Requirements
The CAN-SPAM Act can be broken down into a list of do's and don'ts. Abiding by the following list will help you avoid violating the Act.

Do's
1. Do identify the email as an advertisement or a solicitation. The law gives you a lot of leeway on how to do this, but you must disclose clearly and conspicuously that your email is an advertisement.

2. Do include your physical address in the email. Your email must include your valid physical postal address. This can be your current street address, a post office box you've registered with the U.S. Postal Service, or a private mailbox you've registered with a commercial mail receiving agency established under Postal Service regulations.

3. Do include an opt-out mechanism in the email. Your email must include a clear and conspicuous explanation of how the recipient can opt-out of getting email from you in the future. Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand. Creative use of type size, color, and location can improve clarity. Give a return email address or another easy internet-based way to allow people to communicate their choice to you. You may create a menu to allow a recipient to opt-out of certain types of emails, but you must include the option to stop all commercial emails from you. Make sure your spam filter doesn't block these opt-out requests.

4. Do honor opt-out requests within 10 days. Any opt-out mechanism you offer must enable processing of opt-out requests for at least 30 days after you send your email. You must honor a recipient's opt-out request within 10 business days. You cannot charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an internet website as a condition for honoring an opt-out request. Once a customer has told you no more emails are wanted from you, you cannot sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you've hired to help you comply with the Act. To comply with the opt-out requirements of the Act, we recommend establishing email accounts with various email providers to test your opt-out mechanism. Specifically, testing of the opt-out mechanism should be performed periodically to ensure that opt-out requests are honored within 10 days, the opt-out mechanism is enabled for at least 30 days after the email is sent and the email from which the opt-out request was received is not repopulated onto your mailing list.

5. Do review emails sent on your behalf. The law makes clear that even if you hire another company to handle your email marketing, you cannot contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the email and the company that actually sends the email may be held legally responsible.

Don'ts
1. Don't use false or misleading header information. Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the email.

2. Don't use deceptive subject lines. The subject line must accurately reflect the content of the email.

In addition to reviewing emails sent on your behalf, be careful with emails you send that request the recipient to forward to a friend. You, as the initial sender, are liable for CAN-SPAM compliance for the forwarded email if you offered the initial recipient a reward or benefit for forwarding to a friend. For this reason, many emails that include "forward to a friend" language raise a violation under the CAN-SPAM Act; we recommend you seek guidance from counsel before utilizing such language.

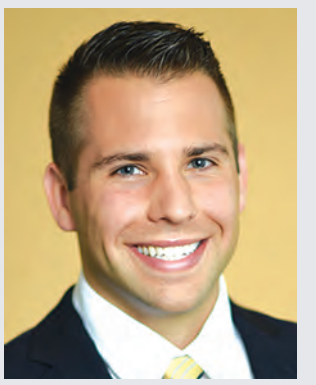
III. Opt-out mechanisms are required, what about opt-in?
a. Commercial electronic mail messages under the CAN-SPAM Act
As discussed above, the Act covers "commercial electronic mail messages," and requires that commercial emails provide an opt-out mechanism. The Act is silent, however, on requiring a recipient to give consent (e.g., opt-in) prior to receiving commercial emails. Thus, the Act does not require that recipients opt-in.

In that emails are often and easily transmitted across national borders, you should be aware of requirements in other jurisdictions, such as the European Union (EU) and Canada. In contrast to the US, the EU Opt-In Directive explicitly requires that consumers receiving electronic communications give consent prior to receiving direct marketing emails. In the EU, the exchange of contact information in a business relationship qualifies as consent. Similarly, Canada's Anti-Spam Legislation (CASL) requires that consumers receiving emails have previously given consent. Canada has extremely hefty financial penalties with each violation of CASL potentially costing between one million and ten million dollars. Like the US, the EU and Canada also require that all commercial emails sent to consumers include an opt-out mechanism.

IV. Based on the CAN-SPAM Act's lack of an opt-in requirement, is it safe to buy lists of email addresses?
Although not as commonplace today, buying lists of email addresses still occurs. Purchasing a list of email addresses presents the following question – will sending a commercial email to any of the email addresses included in the purchased list result in a violation of the CAN-SPAM Act?

As discussed above, if the owner of an email address opts-out of receiving your commercial emails, you cannot send a commercial email to the email address within 30 days. Blindly sending commercial emails to a purchased list may result in sending a commercial email to someone that has opted out of your emails within the past 30 days resulting in a CAN-SPAM violation. Therefore, it is not wise to purchase a list of email addresses and blindly send commercial emails to that list.

Kyle St. James
Kyle St. James is an associate in the firm's Intellectual Property and Cybersecurity groups. His practice includes advising clients on patent strategy including patent portfolio development and patent prosecution strategies. He focuses his practice on computer hardware and software, internet technologies, cybersecurity, 3D printers, wireless network technologies and medical devices. Kyle has handled numerous matters related to access point and network controller design and infrastructure, especially antenna design. Kyle can be reached at 714.338.1805 or kstjames@rutan.com.



Your Business Is Unique. Are Your Financial Solutions Built to Match?

We're dedicated to fostering growth in Orange County's communities. Let's start with your business. You can count on our full range of best-in-class products and services to position your business for long-term success, and seamless access to our firmwide network of experts means you'll receive customized financial solutions—along with the latest industry insights—to help meet your growing needs.

To learn more about how we can help you gain a competitive edge, please contact:

Rick Nogueira
Orange County and Inland Empire Region Manager
Chase Commercial Banking
(949) 833-4888
rick.l.nogueira@chase.com

CHASE

Keeping Yourself Safe Online

Beware of the danger of malware
From baby pictures to vital documents, we store everything on our computers and mobile devices. What would you do if you suddenly lost access? Although technology has made our lives convenient, it has also allowed a new form of crime to take root: cyber threats.

What are cyber threats?
Cyber threats are attempts to infiltrate a computer or mobile device. These threats may originate from a variety of sources and anyone can be a potential target. Cyber criminals may accomplish this goal by using malware to track your internet activities, capture your sensitive information, or block access to your computer until you pay a ransom.

Spotlight on malware
Malware is a broad term that includes computer viruses, spyware, and other types of programs that can inflict damage on hardware and compromise sensitive information. Using malware, cyber criminals swiftly gain access to your computer to locate your information and leave before you detect any unusual activity. For example, a cyber-criminal could monitor and record your keystrokes, collecting information such as username and password for financial websites.

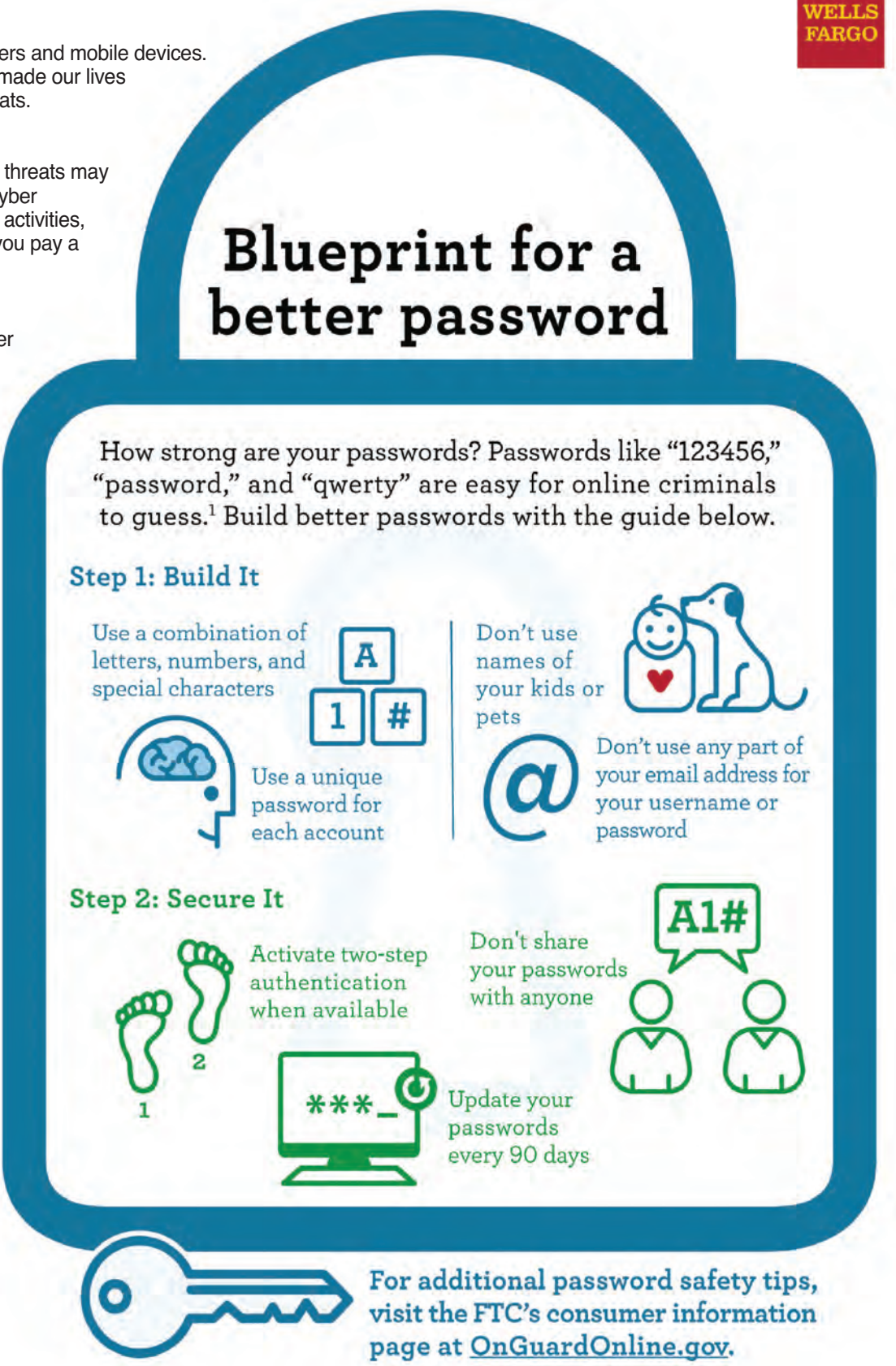
Malware can be spread by visiting contaminated websites, clicking on malicious links in emails or websites, downloading infected files such as mp3s, documents, email attachments, or videos, or inserting infected USB storage devices into your computer or device.

One type of malware, called ransomware, is becoming increasingly popular with cyber criminals due to its lucrative nature and the difficulty with tracking the perpetrators. In a ransomware attack, cyber criminals essentially hold your computer hostage, blocking access to your operating system by locking your screen or encrypting important files until you pay a sum of money. This type of attack primarily occurs on computers. From January 2015 to December 2015, ransomware incidents doubled from three million to six million.

Signs your computer or mobile device may be infected by malware:
▶ Runs slower than normal.
▶ Stops responding or locks up often.
▶ Crashes and restarts on its own.
▶ Does not operate correctly when restarted.
▶ Your computer or mobile device displays:
- Emails you do not recognize in your sent folder.
- Unusual error messages, distorted menus, strange dialogue boxes, or unwanted pop-up ads.
- Threatening messages claiming to be from law enforcement or an anonymous blackmailer and may demand payment, indicating ransomware.

How to protect yourself from malware
▶ Do keep security patches and anti-virus software up to date for your computer and mobile devices.
▶ Do back up your data on a daily basis. Sync your files to a secure external drive or cloud-based software.
▶ Don't auto-download any attachments – be sure to turn off this setting on your mobile device.
▶ Don't click on links, open attachments, or provide sensitive information through a suspicious email or text message.

Passwords also play an important part in protecting yourself and your data. Check out the following infographic "Blueprint for a Better Password" for tips and advice.



[1] "The 25 Worst Passwords You Should Never Use." Time.com. 2017.

Ben Alvarado
Ben Alvarado is executive vice president and president of Wells Fargo's Southern California Community Bank. He oversees approximately 3,800 financial professionals at 233 branches and manages more than $37.7 billion in deposits and $9.5 billion in loans.

Alvarado, a 25-year banking veteran, assumed his current role in December of 2014. Prior to being named president for the Southern California Region, he ran the Orange County-Inland Community Bank. He also has served in various positions at the company, including retail bank district manager for the Pasadena and South Bay markets; commercial loan officer; sales development coach; branch manager; personal banking officer, and bank teller. As one of the top ranking executives in the bank, he also sits on the Management Committee, which provides oversight on operations, practices and to lines of business.

Alvarado earned his bachelor's degree at California State University, Long Beach, and an MBA from Pepperdine University. He is active in the community and serves on the board of directors for Orange County United Way; the advisory board for Miller Children's & Women's Hospital in Long Beach; the board of directors for Bundles of Books in Los Alamitos; Game Changer Charity and is the current president of Wells Fargo's Latin Connection team member networking group.

Alvarado resides in Rossmoor with his wife and two children.

McDermott Will & Emery

Facing the Challenges of Complex, Global Data Breaches

by Michael G. Morgan and Vincent Schroder, Partners, McDermott Will & Emery LLP

Responding to data breaches has become increasingly complex in the age of global commerce, Big Data and the rapidly expanding Internet of Things. They result from more sophisticated cyber-attacks, involve larger numbers of data records, and contain more sensitive and highly regulated information.

To keep pace with this development, businesses need to implement state-of-the-art cybersecurity and breach-management protocols. The traditional checklists for breach preparation include incident response plans, data breach exercises, the identification of key decision-makers, analysis of legal obligations arising from an organization's data, and retention of knowledgeable external resources in important areas such as forensics, PR and legal services. Additional precautions often include the establishment of data breach teams capable of handling multiple work streams, the creation of communications systems and protocols segregated from general business communication channels, and enterprise-wide vulnerability assessments.

Michael G. Morgan

Where a data breach occurs on a global scale or concerns multiple jurisdictions, the complexity of a response is further increased by the variety of applicable legal requirements, many of which substantially deviate from those in the United States and change with regularity. Especially in the European Union, any security incident affecting the availability, integrity, or confidentiality of information pertaining to a natural person can result in breach notification obligations. Short notification deadlines triggered by the detection of the breach may require a prompt reaction to the incident, fast decision making, and a thoughtful, coordinated communication strategy, which can be especially difficult where the attack resulted in loss of business systems or in case sophisticated attack techniques were applied that complicate recovery and forensic investigation. In addition, detailed information about the breach might need to be provided not only to the competent government authorities but also affected individuals. Potential consequences of non-compliance frequently include government investigations, cease-and-desist orders, and drastic fines in the multi-million dollar range.

Vincent Schroder

McDermott's Global Privacy and Cybersecurity team has game-changing experience in handling complex cybersecurity incidents on behalf of its clients across different jurisdictions including the Unites States, the European Union, Asia, and around the globe. Please contact us for detailed information on how we can assist you.

For more information, please visit www.mwe.com or call 949.851.0633.

Get the business credit card with more rewards horsepower

WELLS FARGO

The Business Platinum Credit Card is packed with the rewards you deserve — choose how you want to be rewarded for everyday purchases.

- The *Wells Fargo Business Card Rewards*® program comes with no annual fee[1]
- Choose the cash back option and earn 1.5% with no cap
- Select the rewards points option and earn 1 point for every $1 in net purchases, plus receive 1,000 bonus points every month net spend reaches $1,000 or more

You can also take advantage of a 0% introductory rate for nine months on purchases and balance transfers.[2]

To apply, stop by to speak with a local banker, or visit **wellsfargo.com/appointments** to make an appointment.

Together we'll go far

Offers valid 01/02/2017 through 06/30/2017. Offers subject to change. All financing decisions subject to credit approval.

[1] New Business Platinum Credit Card accounts only. Enroll in the optional *Wells Fargo Business Card Rewards* program when you open a new Business Platinum Credit Card account and you will not be charged an annual rewards program fee. A $24 redemption fee will be assessed for each airline ticket redemption.

[2] **Business Card Rewards program — 1.5% cash back for life of the account.** New Business Platinum Credit Card accounts only. You must enroll in the optional *Wells Fargo Business Card Rewards* program and select the cash back option at the time of account opening. 3% introductory rate for nine months. New Business Platinum Credit Card accounts only. Apply for a new Business Platinum Credit Card and, upon approval, receive a promotional rate of 0% on purchases and balance transfer convenience checks for the first nine months after account opening. Valid as long as a default does not occur under the Business Platinum Credit Card Customer Agreement. You will be assigned an interest rate at account opening that will be Prime + 7.99% to Prime + 17.99% and will become effective after the expiration of the nine-month period unless a default occurs under the Customer Agreement and we elect to increase the rate, or we exercise our right to change the terms of the account. Each balance transfer transaction will be assessed a 4% fee ($10 minimum). Payments will be applied to advances with promotional rates before application to other advances. Balance transfers from Wells Fargo accounts are not permitted. Prime refers to Bank's announced Prime Rate which is 3.75% as of 01/15/2017.

CHASE

What to Know About Detecting Compromised Emails

Criminals continue to refine their methods and targets for cyberfraud attacks like business email compromise, but there are steps you can take to help protect your organization.

As criminals expand targets for cyberfraud attacks by posing as executives of companies or vendors, JPMorgan Chase & Co. developed a process to help clients protect themselves from business email compromise (BEC) attacks.

Technology Solutions
These cyber attacks increasingly include the use of domains and associated email addresses, often referred to as "lookalike domains," that are very similar to those of victim companies. By leveraging technology solutions in unique ways, the firm's cybersecurity team created a proprietary process—currently pending before the US Patent Office—that can potentially detect the use of client lookalike domains. For example, criminals might use "wi***b***getcompany.com" to target the legitimate domain wi***d***getcompany.com.

Clients are notified of domains that closely resemble their corporate domains and receive information about tools that can help them protect their employees and accounts from BEC attacks.

"We saw an opportunity to enhance our cybersecurity program by analyzing client data in a different way," said Matt Zames, the firm's Chief Operating Officer. "This process reflects our commitment to battling cybercrime and our focus on technology to help our clients."

The Rise of Email Scams
The 2017 Association for Financial Professionals Payments Fraud and Controls Survey reports that 74 percent of finance professionals surveyed said their organizations were targets of BEC in 2016, an increase from 64 percent in 2015. Large organizations with more than 100 payment accounts continue to be more likely than other organizations to report potential financial loss in the highest dollar range.

"Business email compromise really focuses more on human nature than technology, although there is a technology component to it," said Anish Bhimani, Commercial Banking's Chief Information Officer. "Criminals are counting on the fact that people may not be paying close attention to an email, and may be reluctant to call a manager or senior executive to validate those instructions."

Lookalike Domain Process
The lookalike domain process is just one part of the firm's substantial investment in cybersecurity, which includes a "Follow the Sun" model with three Cybersecurity Operations Centers in New York, London and Singapore, as well as a dedicated team of more than 1,000 employees.

The firm's lookalike domain process uses specialized logic to continuously analyze new domains to find those that resemble clients' registered domains, and it is able to sort visually similar domains. These sorted domains are provided to Commercial Banking and Corporate & Investment Bank Operations and Service teams so clients can be alerted and apply best practices when executing payments.

"Fundamentally, it's a three-step process," said Rohan Amin, the firm's Global Chief Information Security Officer. "Criminals register a malicious lookalike domain. We apply the analysis process and, if possible, detect a lookalike registration. Then we take steps to mitigate risks internally and notify clients as appropriate."

Lookalike domains may include an array of methods with anomalies like character substitution. Often a client's employee believes he or she is receiving an email from within the organization.

"A one-letter difference in the address can be all a criminal needs to convince an unsuspecting client to transfer funds to the criminal's account," said Josh Pope, Corporate & Investment Bank Operations Executive. "If we can spot those subtle changes early, we can help our clients and protect the firm."

Clients appreciate being notified about the possibility they may be targeted, Pope said. "Recently, our team alerted a Commercial Banking client about a lookalike domain. The client later received a fake email with payment request, and they did not fall for the scheme."

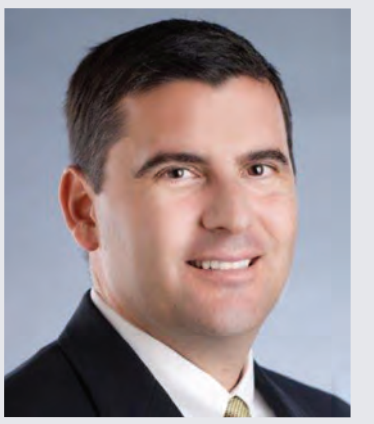
The Role of Social Media and Company Websites
Criminals have expanded BEC attacks by searching social media platforms to identify specific payment controllers through a user's job title or profile. Other methods include researching a firm's website to learn the members of the management team or impersonate the company's CEO by mimicking their written and verbal communications style. By impersonating a client vendor with an email tied to a lookalike domain registration, cyber criminals can request changes to routing or account details in an attempt to steal funds.

Practices to Help Avoid BEC
Cyber experts advise companies to implement practices to help avoid BEC-related emails by verifying instructions in person or by using a known telephone number, internally and with vendors, and if an attack does occur, to escalate right away. Clients that notify the firm within "the golden hour" after an attack have a better chance of recovering stolen funds before the transactions move between countries and people.

"Payments often are settled in a few minutes and cyberfraud can take place just as quickly. If fraud is detected days later, it can be extremely difficult to recover stolen funds," said Lester Owens, Corporate & Investment Bank Global Head of Wholesale Banking Operations. "We tell our clients that it's very important to validate and authenticate who you're communicating with when processing payments, and to waste no time reporting to your bank when you discover fraud or theft."

Source: *https://commercial.jpmorganchase.com/pages/commercial-banking/executive-connect/fraud-prevention*

Rick Nogueira
For additional information, please contact Rick Nogueira at rick.l.nogueira@chase.com
Rick is the Region Manager of Chase's Middle Market Banking group serving Orange County and Inland Empire. In this capacity, he provides leadership and financial solutions to companies with revenues between $20 million and $500 million. A 25-year banking veteran in Southern California, Rick has spent more than 17 years of that time dedicated to Middle Market Banking. He joined Chase as a Senior Banker in 2009 and was promoted to the position of Region Manager in January 2012.



About Chase Commercial Banking
Chase Commercial Banking has a long history of providing comprehensive solutions, including lending and treasury services, to corporations, municipalities, financial institutions and not-for-profit entities with annual revenues generally ranging from $20 million to $2 billion, as well as real estate investors and owners. Please visit us at www.jpmorganchase.com/commercial.

Fisher Phillips

ON THE FRONT LINES OF WORKPLACE LAW™

The Benefits of Security Audits Before and After a Data Breach

By: Usama Kahf, Fisher Phillips

KAHF

State and federal laws require businesses to take reasonable steps to safeguard personal information of employees and consumers. Unfortunately, many businesses wait to upgrade their systems, implement new policies, train their staff, and take other preventive measures until after they are affected by a data security breach. It is never too late, however, to shore up security and work to achieve compliance with privacy laws. No one is truly immune from cybersecurity risk, no matter how small or large an operation. But an ounce of prevention can go a long way to mitigating potential damages.

One important step that should be taken on a regular basis, whether before or after a data breach, is to undergo an independent security vulnerability assessment or audit by a third-party security consultant.

Just as your financial books are audited by an independent outsider, so too should your IT security infrastructure. A security vulnerability assessment or audit can identify gaps in computer security and data breach preparedness and give you a roadmap or checklist of areas that need improvement. For example, you might learn that some of your staff are not following security protocols or have a tendency to click on suspicious links and attachments. You might also learn of a security weakness in your firewall or that your backups are useless because of a technical glitch. You can wait to learn this the hard way, or you can prioritize IT security as a necessary cost of doing business.

Some companies are inclined to assign the task of conducting a security audit to their internal IT department or to their outsourced IT vendor, often due to budgetary constraints. While an internal study may help identify some of the issues, such a study could lack the credibility and objectivity of an external and independent consultant whose job and service contract with the company are not on the line. Computer security consultants also tend to be more specialized and more up to speed on developments in this field than basic IT support vendors. It's like going to a cardiologist for heart issues instead of your general physician.

As far as timing, a security audit should be conducted as a routine best practice, but in the absence of an existing practice of conducting security assessments, you should consider undergoing such assessment immediately in the aftermath of a data breach. Once you undergo your first audit, an annual or bi-annual check-up is in order. Technology changes so fast that this kind of audit is best conducted on an annual or bi-annual basis.

Undergoing a computer security audit is a commitment – once you learn the levy is about to break, you have to fix it. If you are going to commission a security assessment, you should be prepared to implement the consultant's recommendations to prevent or prepare for future data breaches. This is a golden opportunity to create positive evidence of your efforts to understand what went wrong, and your commitment to take the necessary steps to protect private information.

Finally, if you fear that you are behind on security and that an audit will create bad evidence to be used against you in a court of law, fear not. The security audit and all communications and work product made in the course of such audit may be protected by the attorney-client privilege where the audit is conducted at the direction of and with the active involvement of your outside counsel. If a privileged audit report reveals positive, praiseworthy things about your current IT security infrastructure, the report can be declassified so that it can be an exhibit in your defense against claims that may arise after a data breach. Conversely, if the report reveals major weaknesses, and if the process for maintaining the attorney-client privilege is properly followed, the report may never see the light of day, but you can still proceed to implement necessary changes.

Usama Kahf is an associate in the Irvine office of the national labor and employment law firm Fisher Phillips. He may be reached at ukahf@fisherphillips.com.