ASSOCIATION FOR FINANCIAL PROFESSIONALS

# BEC Scams: Treasury's Number One Fraud Threat

## Treasury in Practice Series

Issue 9

ASSOCIATION FOR FINANCIAL PROFESSIONALS

# BEC Scams: Treasury's Number One Fraud Threat

## Treasury in Practice Series

### Introduction

Business email compromise (BEC) scams are among the top fraud threats to corporate treasury and finance, as both the frequency of attempts and the total dollar amounts stolen have increased dramatically in recent months. Whenever financial professionals gather to network, conversation quickly turns to BEC scams. Many practitioners have firsthand knowledge; they know the trends, and they know when to flag a scam attempt. So why are so many companies still being victimized?

In AFP's latest Treasury in Practice Guide, we delve into the different types of BEC scams and how you can make sure your staff doesn't fall for them. We've compiled insights from security experts, law enforcement officials, bank representatives and corporate treasury and finance professionals. This guide will give you the tools you need to recognize a BEC scam immediately—saving your organization a lot of money.

"You personally are the targets of these email scams," Cyrus Vance, Jr., District Attorney for New York County, told attendees of the CTC Executive Institute at the 2015 AFP Annual Conference. He stressed that treasury and finance professionals will need to be better prepared to recognize these scams and stop them before they start. "That might mean requiring two-step verification for important emails between managers and businesses. It might mean requiring two executives to sign off simultaneously on wire transfers, kind of like launching a missile from a submarine with two keys. It could mean requiring, perish the thought, phone calls."

### What is a BEC scam?

BEC scams target companies that make routine wire transfers to foreign suppliers and businesses. In a typical BEC scam, a company will receive a transfer request via email from what appears to be a high-level executive or a supplier. However, the request is actually coming from a hacked email account, or an account that has been "spoofed" to appear legitimate.

In most cases, BEC scams begin with a criminal sending a phishing email to a company employee and gaining access to his or her email account. For an extended period of time—sometimes several months—the fraudster will monitor that employee's email and determine who initiates wires and who requests them. From there, they'll either spoof an email or create a domain that's close to the company that they are targeting. "The domain will look really close to the domain of that particular company and they'll send an email from the CEO," said Stu Sjouwerman, founder and CEO of IT security firm KnowBe4. "It looks like it's totally real."

Sjouwerman noted that the criminals typically wait until the CEO or other executive is on an overseas business trip, at which time they'll send an email impersonating them. He added, "They'll say, 'Hey, we're acquiring a company over here; we need your support. It's not something the SEC should know about just yet. I'm counting on your cooperation. I need you to transfer $120,000 to this bank in this country.' It's a well-oiled machine these days, and people do fall for it."

It can be tough to spot false web domains, said a representative from a major bank. "They'll set up their own mail domain and change one letter," he said. "For example, if you have an 'm' in your company name, they'll change it to 'rn'. If you have a 'w', they'll change it to two 'v's. It looks identical. Companies miss this all the time."

"The CFO thought this was a weird request, so he decided to wait until the next day and ask the CEO when he was in. But the next day, he wasn't in, and the CFO got another email saying, 'Where's that wire? I really need it now.' They knew he was going to be out for two days."

The bank representative stressed that these scammers are skilled at learning employees' schedules, and even personal relationships in the office. He explained that the CEO and CFO of one of his corporate clients are best friends who have worked together for years. When the CEO was out of the office, hackers sent an email to the CFO, asking him to send a wire. "The CFO thought this was a weird request, so he decided to wait until the next day and ask the CEO when he was in," he said. "But the next day, he wasn't in, and the CFO got another email saying, 'Where's that wire? I really need it now.' They knew he was going to be out for two days."

Ultimately, the CFO sent the money. He transferred $100,000 to China, which is 14 hours ahead of the company. Once the company figured it out on a Friday, the banks were closed. "By the time we contacted the Chinese bank on Sunday night, the money was long gone, with no chance to get it back," he said.

The banker added that it is absolutely critical to train your employees so that when they come across emails with this type of urgent phrasing, it sets off a red flag. "They're in your email system," he said. "They are reading every one of your emails. It's uncanny how they know who is going to be in your office."

Michelle Young, senior vice president at Wells Fargo treasury management, refers to BEC scams as "social engineering on steroids," due to the lengths these criminals will go to acquire information about their targets.

Richard Boscovich, assistant general counsel of Microsoft's Digital Crimes Unit, provided AFP with a personal example. Several months ago, he traveled to Brazil to meet with several banks about security. The only people that were aware he was traveling there were Microsoft colleagues, staff of the company's Brazilian subsidiary, and the banks themselves. Within 48 hours of arriving in Brazil, he began receiving targeted phishing attacks in Portuguese saying that his Bank of Brazil accounts needed to be updated. "I don't have bank accounts in Brazil," he said. "But look how quickly they knew. It shows you the level of sophistication."

Of course, BEC scams don't always consist of a fraudster impersonating a CEO or CFO. Fraudsters will also impersonate companies' suppliers, sending them new payment instructions so that a routine transfer will be sent to a new account.

Danfoss Group, a Danish developer of heating, ventilation and air conditioning systems, is one such supplier. Fraudsters copied the Danfoss logo and sent a message to one of the company's customers. "They said, 'We have a new bank account; please pay to this one in the future,'" Palle Dedenroth, assistant treasurer for Danfoss, told AFP.

Dedenroth noted that this particular type of BEC scam is easy to fall for because if the request looks legitimate, the victim company might not realize anything is wrong. "You might have had a supplier the week before who got angry because you didn't pay fast enough," he said. "What you can do really depends on the circumstance and when it happens. So those of us who are handling payments, when we see something, we have to think, 'Is this right or not?' And if not, we shouldn't make the payment."

"There has been a 270 percent increase in identified victims and exposed loss since January 2015."

Sjouwerman acknowledged that there is a less awareness of supplier fraud than CEO fraud, and that is a major concern. "It's a quick hit to do the CEO scam," he said. "It takes a little more work to send a fraudulent invoice. It's a little more sophisticated, and it's a little more below-the-radar. It's not being given enough attention."

"I learned from our insurance group that this isn't covered as a fraudulent wire because we intentionally sent it."

## A $1.2 billion threat

In August 2015, the FBI reported just how much companies have lost due to BEC scams, and the numbers were shocking. Criminals reportedly stole nearly $750 million from more than 7,000 U.S. businesses between October 2013 and August 2015. Combined with international victims, the FBI estimates that more than $1.2 billion has been lost due to BEC scams.

"There has been a 270 percent increase in identified victims and exposed loss since January 2015," the FBI warned in its alert. "The scam has been reported in all 50 states and in 79 countries. Fraudulent transfers have been reported going to 72 countries; however, the majority of the transfers are going to Asian banks located within China and Hong Kong."

Some companies have been duped into sending massive amounts of money to these criminals. Ubiquiti Networks, a San Jose-based networking technology firm, revealed in an August SEC filing that it had been defrauded out of nearly $47 million.

The incident, which occurred in June, involved a fraudster impersonating an Ubiquiti employee and arranging $46.7 million wire transfer to Hong Kong. The company reached out to its Hong Kong subsidiary's bank and managed to recover $8.1 million. Ubiquiti said at the time that it expected to recover an additional $6.8 million.

In its filing, Ubiquiti explained that it "may not be successful in obtaining insurance coverage for this loss." This point is incredibly important for corporate treasurers, whose companies are making major investments in cyber insurance. BEC scams typically fall outside this type of coverage. "I learned from our insurance group that this isn't covered as a fraudulent wire because we intentionally sent it," explained a treasurer for a global development organization.

Fortunately, there is coverage available for BEC scam losses—treasurers just have to know which policy it falls under. Tom Reagan, national cyber practice leader for Marsh, explained that currently, BEC scam coverage is available as part of many traditional insurance policies, but not cyber insurance.

"Typically the broad cyber market deals with nonfinancial asset issues; it deals with data, information, things like that," said Reagan. "But on the crime side and the fidelity side, there are a variety of products that cover business email compromise. So yes, you can buy insurance for that. The market's not as deep as we would like it to be, but we expect that market to get much deeper in the coming weeks and months."

## Keys to BEC's effectiveness

One reason why BEC scams are more of a threat than traditional cyberattacks is the approach that criminals take, noted Brad Deflin, president and co-founder of Total Digital Security. "The perpetrators of these attacks are highly skilled social engineers, versus cyber-technicians that are hacking the technology, and the ingenuity and methodology of these attacks are evolving faster than our idle imaginations can grasp," he said.

The crux of the problem, Deflin explained, is the human element. People need to become more aware of the telltale signs of these attacks, rather than simply hoping IT will catch any and all questionable emails. He advises treasurers to not only be vigilant while they are in the office, but also to have their guard up in their personal lives.

For example, when you receive an email from one of your contacts, do you just accept that you are talking to that person? Do you know for sure that the person you're communicating with is who they say they are? Even if you're familiar with your contact's writing style, remember—someone else could be familiar with that too and could be copying them. This is the way treasury and finance professionals need to be thinking in the current threat environment.

"I think about my own style in my email; I never end it with 'Sincerely,' and I never start it with 'Dear'. If you really paid attention, you could pick up on the way I speak in email and simply copy that."

"We're seeing very sophisticated social mimicking, down to the way in which your cadence is," Wells Fargo's Young said. "I think about my own style in my email; I never end it with 'Sincerely,' and

I never start it with 'Dear'. If you really paid attention, you could pick up on the way I speak in email and simply copy that. And folks would think, 'That's Michelle' on the other end of that email."

Indeed, the more the fraudsters know about you, the easier it will be for them to scam someone at your company. That's why Microsoft's Boscovich warns treasury and finance professionals against putting too much personal information out there on social media sites. "If you have any employee who puts where they work on Facebook or even LinkedIn, you have to be careful," he said. "If I post on LinkedIn that I'm going to be somewhere, I just assume that the bad guys are going to know where I am. But most people are not very attuned to that. And that's the kind of information that they take, they'll social engineer, and they'll send you an email. Social media is one of the ways where you can find out just enough about a person—where they went to high school, where they went to college—and then create a phishing email and someone will fall for it."

KnowBe4's Sjouwerman noted that business size is also playing a role in the pervasiveness of these incidents. While large corporates appear to be picking up on the threat and taking steps to mitigate it, smaller firms are a different story. "The massive amount of attempts on small and medium businesses [SMBs] is where the big change is—a change for the worse in this particular case," he said. "Large corporates usually have a procedure in place that requires at least two people to sign off on these types of wire transfers, but SMBs often do not have these safeguards in place. So when a CEO email arrives, people tend to think, 'This is the boss; I had better do what he says.'"

Sjouwerman added, "Anybody who is in finance is essentially a target these days," he said. "About 30 percent of employees of SMBs who get these types of requests actually transfer the money."

## Even legitimate sources can't be trusted

Treasurers know that they must be more vigilant. But what if the request comes from a legitimate source?

Treasurers should be wary of those too, said Richard Turner, president EMEA for security firm FireEye, following his session on cyberthreats at the EuroFinance International Cash & Treasury Management conference in September.

Turner told AFP that criminals are becoming so crafty in their social engineering techniques that some fraud rings are actually hiring legitimate organizations to call or email companies to inquire about information. Therefore, financial professionals need to be careful about giving information out—to anyone. "Everyone needs to adopt a state of continuous vigilance," Turner said.

"People fall for quite simple attacks. They're launched by sophisticated organizations, but often the attack itself is pretty straightforward."

Financial professionals need to have protocols in place to make sure the requests they receive are legitimate. "If I don't have a process to really validate that it really is a CEO asking me to make a transfer, then you have to get people to be inquisitive," Turner said. "People fall for quite simple attacks. They're launched by sophisticated organizations, but often the attack itself is pretty straightforward."

For example, an employee in human resources might receive an email that appears to be from a prospective employee. The email has a CV attached to it. "You're probably going to open it," Turner said. "And why not? You're in the HR department; someone sends a CV, you're going to open it. So you've got to make people think, 'Who is this person? Is this coming from a place I recognize?' And they need to be skeptical if that's not the case."

## FBI tips

In a recent alert, the FBI provided some best practices that businesses can apply to recognize these scams before any money is transferred.

- **Implement a detection system that flags e-mails with extensions that are similar to the company e-mail.** For example, if your legitimate company is e-mail is @company.com, the e-mail @company.com would be flagged. Don't just rely on spam filters to catch these emails. According to security blogger Brian Krebs, spoofed emails used in BEC scams are unlikely to set off spam traps because the targets are not mass emailed.
- **Register all company domains that are similar to the actual company domain.**
- **Verify changes in vendor payment locations** by adding additional two-factor authentication, such as having a secondary sign-off by company personnel.
- **Confirm requests for funds transfers.** When using phone verification, use previously known numbers and not the numbers provided in an e-mail request.

- **Know the habits of your customers** when it comes to payment tendencies and amounts. Flag anything out of the ordinary.
- **Carefully scrutinize all e-mail requests for funds transfers** to determine if the requests are legitimate.
- **Speak to your banking partners** and see if they will hold their requests for international wire transfers for an additional period of time, to verify that the requests are legitimate. Some banks are already doing this on their own.

The FBI also provided actions that companies can take should they realize they have been victimized:

- **Immediately contact your bank** and request that they contact the corresponding financial institution where the transfer was sent.
- **Contact your FBI office if the transfer was recent.** The FBI, working with the Financial Crimes Enforcement Network (FinCEN), might be able to help return or freeze the funds.
- **File a detailed complaint with www.IC3.gov.** Be sure to identify the incident as a BEC scam.

"Hover over the link in the email before you click. Let's say it's supposed to be coming from IBM but when you hover over the link it says IBM.com but then there's a huge string after it… you know it's not coming from IBM."

## Additional tips for treasurers

**Watch for urgent or "secret" requests—particularly when they come from an executive who is absent.** Timing and phrasing can help companies recognize these types of scams. The fraudster making the request typically says that the transfer is for administrative purposes or an acquisition, and will stress that the payment needs to be made immediately. The request usually comes on a Thursday or Friday, or right before a holiday weekend when the company is short-staffed, and the person who is supposedly sending the request is usually not in the office.

Additionally, if the request is secretive, that's a big red flag, noted Wells Fargo's Young. "We're seeing a lot of that; emails that are like, 'We need to make this important payment right now and it's confidential; don't tell anybody,'" she explained.

**Carefully read your emails.** Microsoft's Boscovich advises treasury and finance professionals to train themselves to pick up on anything that looks suspicious in an email. "Hover over the link in the email before you click. Let's say it's supposed to be coming from IBM but when you hover over the link it says IBM.com but then there's a huge string after it… you know it's not coming from IBM," he said.

However, given that financial professionals receive a multitude of emails every day, it can be incredibly difficult to go over every questionable email you receive. Spotting a fake email address can be nearly impossible when only one letter is changed, which is why it can benefit you to employ a third-party service like Barracuda Networks or Symantec for help. "There are some third-party services that can help with monitoring of emails," Young said. "It's hard to spot a wrong domain address."

"When your vendors email you and say, 'I have a new bank account, send it here instead of there,' tell your AP to call them back. Verify it. That's something people aren't doing."

**Verify before you send.** Be wary of any emailed request instructing a routine wire payment to be sent to a new account. One treasurer stressed that sometimes just a simple phone call can keep thousands or even millions of dollars from walking out the door. "When your vendors email you and say, 'I have a new bank account, send it here instead of there,' tell your AP to call them back," she said. "Verify it. That's something people aren't doing."

Young agreed that most BEC scams can be stopped by simple verification and other precautionary steps. "If you confirm a request, monitor your accounts and really be a little bit suspicious about things that look out of the ordinary, these things can quickly be stopped," she said. "Our main message is: verify. Just pick up the phone and make a simple call to that person and validate it."

**Fully support your staff to enforce policies that mitigate risk.** Treasury staff members should be encouraged to properly vet each emailed request that comes through, regardless of whether timeliness is an issue. "If an employee waits to send a wire out as part of the verification process, their supervisor should fully support them if it ends up delaying a legitimate issue—they have to be the gatekeeper in safeguarding the company's liquid assets," noted Tom Hunt, CTP, AFP's director of treasury services.

**Test your staff.** Sjouwerman advises financial professionals to avoid an "old-school" approach when it comes to security awareness training. "Old-school is: You're herded into the breakroom once a year, you're given coffee and donuts and you get exposed to death by PowerPoint," he said. "Twenty minutes later you're let out, and you use your checkbox compliance for another 12 months. No pun intended—but that doesn't hack it anymore."

"You just test people, you find out how many people are click-happy or what we call phish-prone, and you train them online, in the browser. Then you regularly send them simulated phishing attacks. That works."

Instead, Sjouwerman favors a "new-school" approach to security training. "You just test people, you find out how many people are click-happy or what we call phish-prone, and you train them online, in the browser. Then you regularly send them simulated phishing attacks. That works. We've seen the phish-prone percentage go down from 16 percent to 1 percent in a 12 month period. But you need to do it and it needs to come from the top down," he said.

Total Digital Security's Deflin also favors a more in-depth approach to training that actually effects change in employee behavior. An approach that simply says, "Here's the threat, here are the tools, go use them," doesn't work. "I think it has to be an approach that says, 'Here's why this is happening, here's how it's happening, here's what you can do, here are the tools. Let's get back together in a week and talk about our experiences,'" he said. "After that, you're pretty much done, because once people get to that level, they don't want to go back. They feel more autonomous and more empowered; they're reading the headlines and they're understanding them better than they previously were."

**Change your out-of-office processes.** A good tip for treasurers and CFOs is to change their processes when they are out of the office. Sassan Parandeh, CTP, global treasurer of ChildFund International, suggested that treasurers and CFOs refrain from leaving an out-of-office message in Outlook. That way they will not be targeted by fraudsters looking for easy targets to impersonate via email. As an alternative, financial professionals can simply keep out-of-office messages internal.

"It appeared that our CFO was writing to us from his vacation. They probably knew he was out of the office because of his out-of-office message."

ChildFund should know; last summer, a criminal group based in China hit the child development organization with a BEC scam attempt. Posing as ChildFund's CFO, the criminals wrote to ChildFund's assistant controller ordering the delivery of funds. "It appeared that our CFO was writing to us from his vacation," said Parandeh. "They probably knew he was out of the office because of his out-of-office message. They emulated an almost identical e-mail to ours where instead of @ccfusa.org they used @ccfsusa.org."

Thankfully, due to ChildFund's strong internal controls, the organization caught this immediately. But instead of stopping there, ChildFund went the extra mile and wrote back to the fraudsters multiple times, luring them in. "Once we clearly identified their IP address, we informed the U.S. marshals," Parandeh said.

## Conclusion

Simply put, BEC scams are everywhere, and they're not going anywhere. These fraudsters are dedicated, and if you give them a way in, they're going to exploit it. And while large corporations might be more prepared for them than smaller ones, they are by no means immune. A simple email could be all it takes to wipe out thousands or even millions of dollars from your company's bank account, and if so, good luck getting it back.

Fortunately, with good policies and training in place, treasury and finance professionals can avoid making a fatal mistake. That way, the next time you receive an urgent, secretive wire request from an executive who is out of the office—you'll probably think twice.

## About the Author

Andrew Deichler is editor, web and publications, for the Association for Financial Professionals (AFP). He writes and edits content for a number of media outlets, including AFP Exchange, Payments, Global Treasury and Finance Insights and Treasury and Finance Week. Deichler regularly reports on a variety of complex topics, including payments fraud, emerging technologies and financial regulation.

---

AFP® ASSOCIATION FOR FINANCIAL PROFESSIONALS

## About the Association for Financial Professionals®

Headquartered outside Washington, D.C., the Association for Financial Professionals (AFP®) is the professional society that represents finance executives globally. AFP established and administers the Certified Treasury Professional® and Certified Corporate FP&A Professional™ credentials, which set standards of excellence in finance. The quarterly AFP Corporate Cash Indicators® serve as a bellwether of economic growth. The AFP Annual Conference is the largest networking event for corporate finance professionals in the world.


General Inquiries: AFP@AFPonline.org
Website: www.AFPonline.org
Phone: 301.907.2862