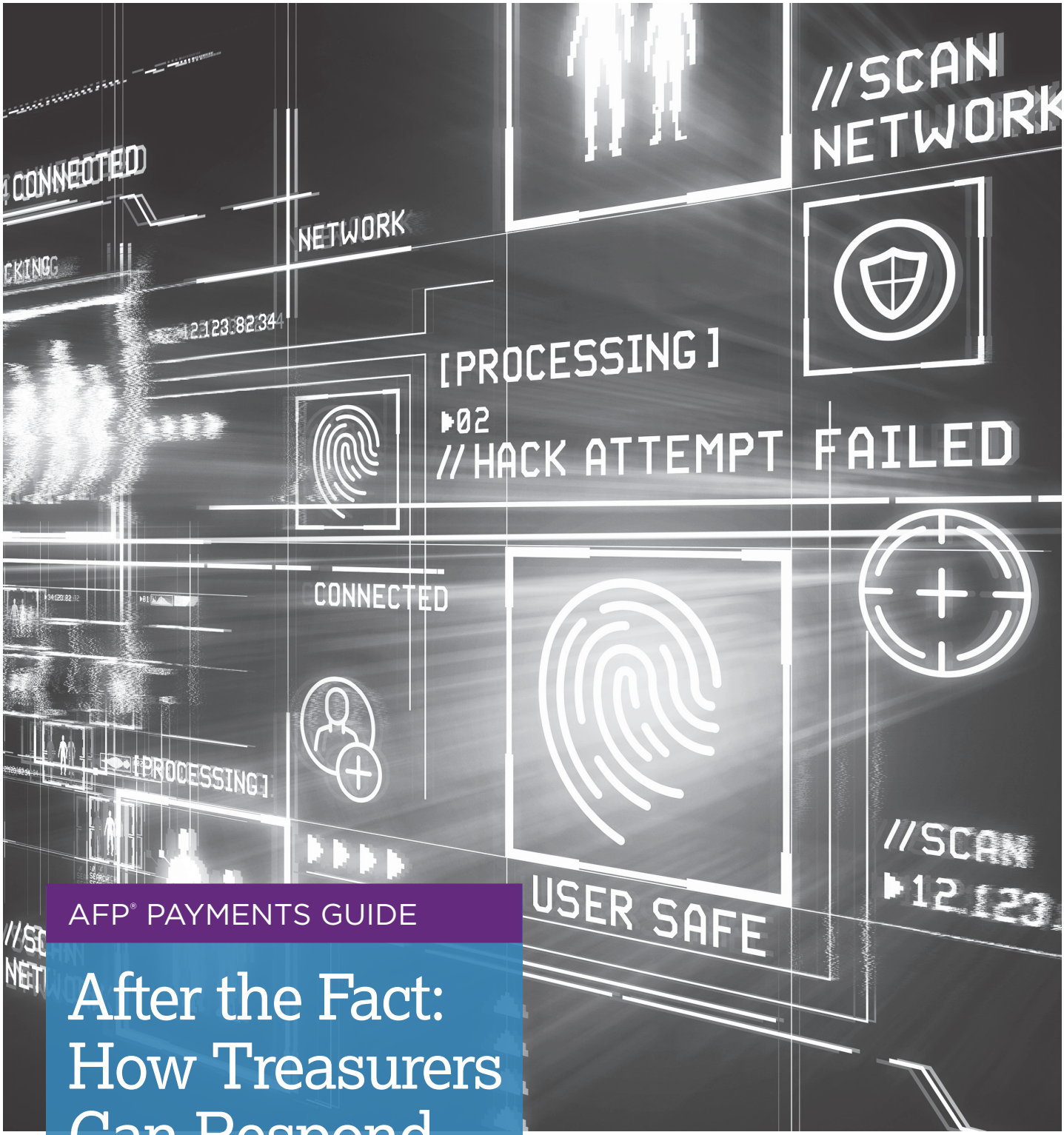
ASSOCIATION FOR FINANCIAL PROFESSIONALS



AFP® PAYMENTS GUIDE

After the Fact: How Treasurers Can Respond to Fraud

Underwritten by:

MUFG

UnionBank

AFP® PAYMENTS GUIDE

After the Fact: How Treasurers Can Respond to Fraud

CONTENTS

AFP® PAYMENTS GUIDE

AFTER THE FACT: HOW TREASURERS CAN RESPOND TO FRAUD

Cybersecurity and payments fraud are top of mind for CFOs and Corporate Treasurers across industries and company size. To provide actionable information to financial professionals, MUFG Union Bank, N.A. is sponsoring our eighth AFP Payments Guide, titled *After the Fact: How Treasurers Can Respond to Fraud*. This guide aligns with our organization's investment in fraud prevention education programs and offerings.

Fraud — and its threat — are a reality. According to the *2019 AFP Payments Fraud and Control Survey*, 58 percent of treasury and finance professionals reported that payments fraud at their companies was a result of Business Email Compromise. Also, 80 percent of organizations experienced these scams in 2018, which is a growing trend over the past four years. This booklet takes a closer look at how fraud is evolving and how treasury teams are addressing these changes.

We commend the AFP for educating readers of this guide on what they can do in the fight against fraud and to mitigate risks. While payment breaches are not completely preventable, the services that banks provide, together with the useful information in this guide, can help reduce the number of incidents.

MUFG Union Bank is committed to supporting the AFP in developing resources such as this booklet that can be shared with employees and partners. We plan to share this with our clients and colleagues. Every day, innovation is overcoming challenges and creating new opportunities in the industry. We are also pleased to sponsor the AFP Pinnacle Awards that recognize excellence in treasury and finance.

Best regards,

Ranjana B. Clark
Head of Transaction Banking Americas and Bay Area President
MUFG Union Bank, N.A.

INTRODUCTION

Payments fraud is a problem for nearly every treasury organization. As fraudsters' schemes continue to evolve, companies' responses to these threats must also advance. Those that don't will ultimately be setting themselves up for major losses.

In this new Payments Guide, underwritten by MUFG Union Bank, we will examine some of the ways that fraud is changing and how treasury departments are responding to those changes. "We've done guides before that looked at different types of fraud, but we haven't done one on what happens afterwards," said Magnus Carlsson, AFP's manager of treasury and payments. "I've had corporate contacts come to me after fraud happened, and they just didn't know what to do. So this guide aims to really be a step-by-step process to show treasurers what to do and who they should contact when they experience fraud."

2 DISCOVERING FRAUD

So how can organizations best discover fraud? Often, by the time fraud is recognized, it's far too late to do anything about it. Are there any systems or routines that make fraud more noticeable?

Though it may sound obvious, the importance of educating your workforce can not be overstated. Treasury departments need to make sure that any employees who touch company money are aware of the latest threats and learn to recognize the telltale signs of a scam.

Furthermore, criminals adapt, and employees can't always count on fraud to be obvious. Steven D'Antuono, Financial Crimes Section Chief for the FBI, noted that fraudsters have gotten very good at circumventing email systems. If companies are on the lookout for certain keywords in emails, then criminals will try different ones. "So I think just having good filters, good internal controls and constant messaging to your people to check on new payment methods and be skeptical," he said.

D'Antuono added that everyone from Fortune 500 companies to small construction companies are being taken advantage of, particularly by Business Email Compromise (BEC) scams. "It's human nature," he said. "It's real people who push out those payments, whether it's through electronic systems or cutting a check the old fashioned way. So you have to just be skeptical and know who you're paying at the end of the day."

FBI Assistant Section Chief Aaron Seres added that companies also should assess their risk tolerance for fraud losses. "You can't control every single transaction to the degree that you would like to; you can't scrutinize every single one," he said. "So whether it's $1 million or $500,000, consider having a dual check threshold level before you send out a payment. So if your threshold is $1 million and you get a request for $1 million, you need to get someone to take a second look at it. So controls like that are what we talk about a lot, because they're used before you send out the money. Because once it's sent, that's the harder part."

> "It's real people who push out those payments, whether it's through electronic systems or cutting a check the old fashioned way. So you have to just be skeptical and know who you're paying at the end of the day."

> "When you contact your local field office, they will try to help, but they don't have the same expertise as our IC3 location. So that's the best vehicle if you want to get action."

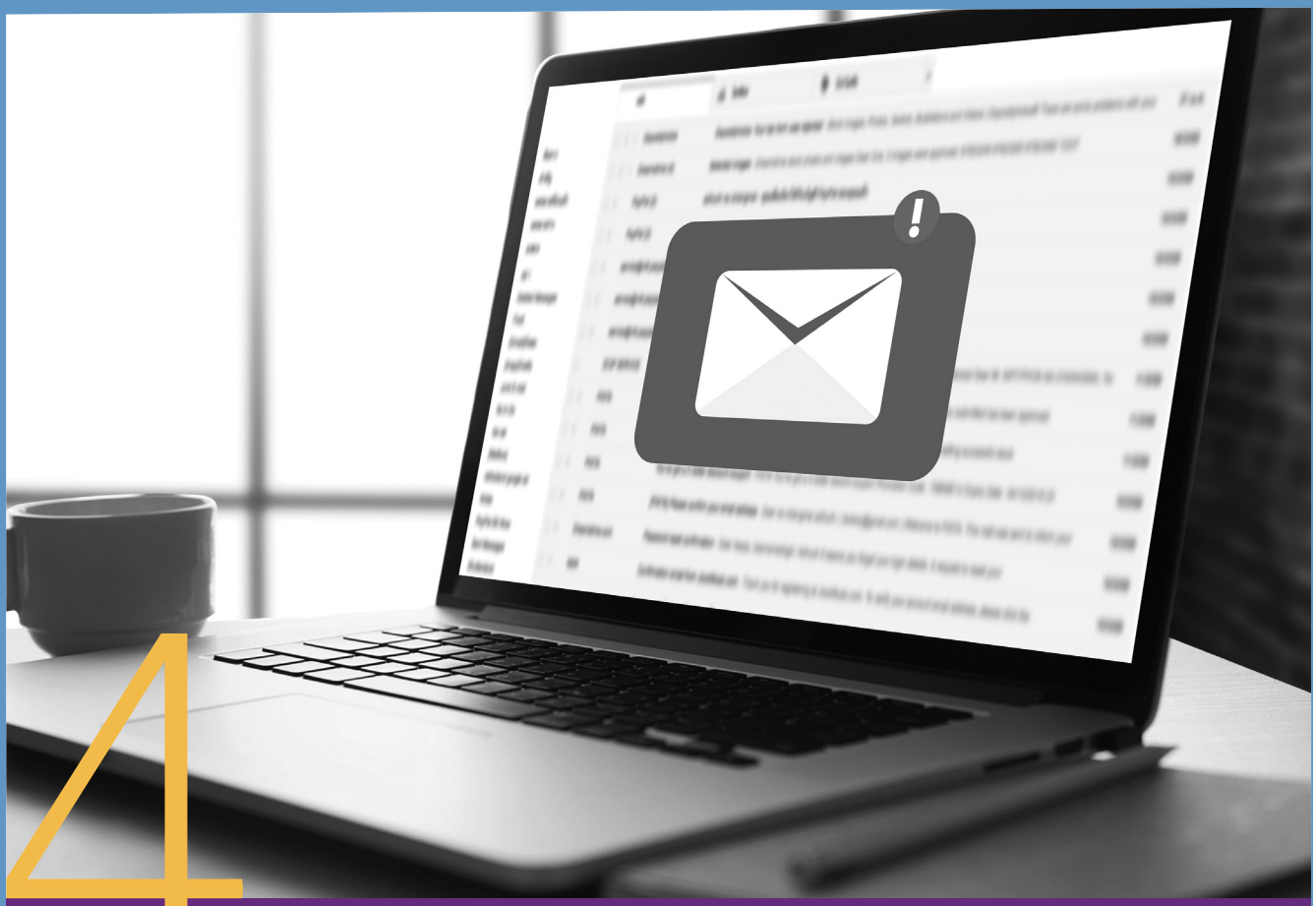
3 REPORTING FRAUD

In terms of where to report payments fraud—any type of fraud—D'Antuono recommends going to the **Internet Crime Complaint Center (IC3)**. "It's not just for internet crime; it's for all financial crimes," he said. "So the first thing to do is go to IC3.gov. Sometimes we might be able to get the money back by some of the mechanisms that we can put in place, like calling the banks. But you should definitely contact your banks yourself. It amazes me that people don't call their bank when their money is taken. So contact the bank, then contact IC3. If you wait to do any of this, it's like a kidnapping—24 hours go by, the less chance we have of getting it back."

Seres noted that going to your local FBI field office after a fraud incident can help, however, going to IC3 first is the best way to go. "[The field office] might not be dealing with these issues on a day-to-day basis," he said. "When you contact your local field office, they will try to help, but they don't have the same expertise as our IC3 location. So that's the best vehicle if you want to get action."

When a fraud incident occurs, there is often a question of whether a company should even report the incident. Given how bad reputational damage can be to a business, some organizations feel it's not worth taking the hit. However, as fraud has continued to increase, the FBI has observed an uptick in companies reporting.

D'Antuono doesn't see reporting to the FBI as a major reputational risk to companies. "We're not going to tell anyone, so why wouldn't they report it to the FBI? If it's a publicly traded company they'll have to report it eventually, and if you're a small company, reporting it to us doesn't mean it's going to be out there publicly. We don't say anything about ongoing investigations, ever. That's our policy."



4 CONFRONTING BEC EVOLUTION

Payments fraud trends generally have not changed much in recent years. Everyone is on the lookout for a new scam that will catch everyone off guard. But the truth is much more nuanced. The majority of methods currently being deployed aren't particularly new. Instead, fraudsters are constantly refining the old methods so that they continue to work. Therefore, treasury departments need to familiarize themselves with the tried-and-true methods and be on the lookout for slightly tweaked versions of these threats.

One type of fraud that continues to evolve is business email compromise (BEC). When this scam first began making waves several years ago, it took a lot of companies by surprise. Since that time, treasurers have become very proactive in applying protocols to avoid this type of fraud. Yet this scam continues to work against even very prominent companies, largely due to the ingenuity of the fraudsters.

According to the **2019 AFP Payments Fraud and Control Survey**, underwritten by J.P. Morgan, 58 percent of treasury and finance professionals reported that payments fraud at their companies came as a result of BEC scams. Furthermore, 80 percent of organizations experienced these scams in 2018, continuing an upward trend observed over the past four years.

“Back in the 1960s or 1970s, you’d just walk down to the CEO’s office and make sure they wanted this payment. But that personal approach is gone, and now these criminals have just taken advantage of that.”

The most common type of BEC scam is also known as CEO fraud, in which a fraudster spoofs an email from a high-ranking executive, instructing someone at the company to make an urgent payment. Though these scams are well known to treasury and AP departments, they’re still effective.

These scams still work, largely due to how impersonal office communications have become. D’Antuono insists that companies should have a policy in place in which someone in AP or treasury actually calls the individual who supposedly sent the email. “That’s how a lot of these BECs happen; it’s gotten so impersonal,” he said. “Back in the 1960s or 1970s, you’d just walk down to the CEO’s office and make sure they wanted this payment. But that personal approach is gone, and now these criminals have just taken advantage of that.”

Additionally, BEC scammers are aware that companies are recognizing the signs and as a result, they are refining their methods. For example, a few years ago, it would be fairly commonplace for a spoofed/fake email to be full of misspellings and grammatical errors. These days, emails tend to be a lot more convincing. “I think they got some people to actually look at their emails and not misspell things,” D’Antuono said.

CHANGING METHODS

In another sign of evolution, the methods that criminals are using to execute BEC scams appear to be changing in a surprising way. Although wire transfers remain the method most commonly used for BEC, wires were used against 43 percent of organizations last year—down from 54 percent in 2017. However, BEC scams targeting ACH credits surged from 12 percent in 2017 to 33 percent in 2018, according the AFP survey.

So what conclusions can we draw from this dramatic shift? The survey notes that this change may support the theory that more fraudsters are gaining access to internal systems though account takeovers and are using the data gathered to generate ACH files. Indeed, account takeovers also saw a sizable surge, jumping from 13 percent to 20 percent.

But this change in the method used may also be an indicator of several other things. First off, it could be a sign that fraudsters are evolving. BEC scams are known to nearly every organization out there right now. The telltale signs are obvious to most treasury departments, and many of them have put protocols in place to ensure that no one is sending a $50 million wire transfer to China, based on an email that supposedly came from the CEO. Although the survey revealed that the majority of BEC scams (81 percent) involved a fraudster impersonating a senior executive, fraudsters are also targeting routine vendors. Forty-four percent of respondents reported that criminals had impersonated vendors in emails, changing payment instructions that directed funds to their own accounts.

Additionally, the shift to ACH may be an indication that fraudsters are targeting domestic transactions, rather than international ones. While wires are used for most international transfers, the majority of ACH transactions occur domestically.

“We do a see a trend in money moving domestically, versus internationally,” Seres said. “Bad guys are always moving their operations to get around law enforcement actions. So typically, in the past, you would see everything go internationally. Now you’ll see a little of it going domestically and then internationally; there’s definitely some changing methodology in that regard in terms of ACH or any other type of payment fraud.”

The shift to domestic transactions could stem from the FBI getting better at clawing back money that was transferred internationally, D’Antuono noted. “We got very good at taking money away, because there is a

lag," he said. "So if it was reported quickly enough, we were able to pull that back."

One might also assume that the individual dollar amounts of these fraudulent transactions are going down, but that does not appear to be the case. "We see fluctuations from $1,000 to $50,000 to more," D'Antuono said. "The BEC real estate scams can be hundreds of thousands of dollars."

Carlsson noted that AFP has observed a recent spike in $2 million-plus transactions. "We also see that larger organizations have been targeted more over the past year," he said. "I find it very interesting that ACH credits have seen such an uptick as a vehicle used for domestic BEC. You can't hide behind the time difference and use that to your advantage. But I can see how you could request an ACH just so it wouldn't raise any red flags. Because if you ask for a wire, typically that's a red flag."

D'Antuono agreed, noting that fraudsters simply react to what the FBI and proactive companies are doing. "That's why, a lot of times, we don't like putting too much information out there, because then they'll know," he said.

He added that the amount of information that is out there to the public is a virtual treasure trove that allows criminals to execute these complex social engineering scams. "A lot of the BECs, a lot of the frauds and swindles, are social engineering, not computer intrusions," he said. "People have their whole lives on the internet, between Facebook, Instagram, etc. Corporations put all of their information out there for their financial reports, and the backgrounds of their executives. Criminals have always been very good con men."

"You just send out a payment and you don't even know there's an issue. You're not going to know unless the vendor contacts you at some point and says, 'Hey, you're 30 days late with your payment.' And by that time, it's too late. So even though it's an ACH, by the time you're figuring it out, it could still be too late."

VENDOR BEC UPTICK

Larry Tolep, CTP, treasurer for Volkswagen Group of American and a member of AFP's Treasury Advisory Group, believes that the typical CFO/CEO fraud version of BEC has not been much of an issue as this scam has been circulated within the organization and people recognize it. "When you send out this email request to do something really strange—sending $1 million to an account in China—it's going to get more scrutiny," he said.

What continues to be a problem though is the supplier version. Volkswagen has been a target of a couple of these fraud attempts. ACH has been used for these payments.

"For our payments, we have master data inside of an accounting system," Tolep said. "So when a payment comes, all the information on that vendor is already locked and loaded. So there will be a PO, the payment will be generated, and all of the information is already there. So a fraudster we think is a supplier will have communication back and forth. They build the relationship, and then they give the company new settlement instructions. And if we accept those settlement instructions, we'll update the vendor master data. So if that request gets approved, it will be generated automatically with what is inside that system. So that has been, from a fraud perspective, an area of concern."

These types of BEC scams are harder to catch because they're not one-off transactions in the way that the traditional CEO fraud scams are. "They're making you believe that they are the supplier you deal with, and now they're just trying to get you to update the data. It's just a normal transaction," he said. "You just send out a payment and you don't even know there's an issue. You're not going to know unless the vendor contacts you at some point and says, 'Hey, you're 30 days late with your payment.' And by that time, it's too late. So even though it's an ACH, by the time you're figuring it out, it could still be too late."

Typically, by the time all this has been figured out, the fraudster has

collected their money and closed the bank account. So when you go to the bank and try to claw the money back, the bank informs you that the money isn't there anymore.

Based on this information, one might conclude then that BEC scammers are focusing more on ACH than wires. However, Michael Herd, Nacha senior vice president, ACH Network administration, doesn't see these changes necessarily as a sign that fraudsters are shifting to ACH over wire. Instead, he views this as fraudsters tailoring their schemes to the methods that work. In the case of domestic suppliers, most of those transactions are going to be ACH, so that's why they're going after that method. And if that method is working, then it will continue to increase.

"We don't see that fraudsters by and large target specific payment methods," he said. "To the extent that they do, it's typically when wire transfers are used to send very large dollar amounts out of the country. What we've seen is that fraudsters use ACH in certain scenarios that already make use of ACH. So a lot of vendor payments are made using ACH, and when a fraudster tries to redirect those payments, they use ACH."

Nacha has a **list of current fraud threats** on its website, as well as a list of recommendations that treasury professionals should review. "We have prepared materials that we issued about two years ago, and they're available to anyone, at no cost, who wants to avail themselves," Herd said. "Generally, it's a lot of common sense things. One is simply awareness. Educate yourself on what these scenarios are and how they're executed. Because if you know, then you can defend yourself."

Volkswagen's Tolep advises treasury departments who are hit with these types of scams to be very clear when going to their bank to inform them of what happened. "Tell them that there has been fraud—use the "f" word," he said. "As soon as you do that, it brings everything up to a much higher elevation at the bank and it makes them say, 'We have to address it.' That's different than just saying, 'I need to reverse an ACH that I paid out.'"

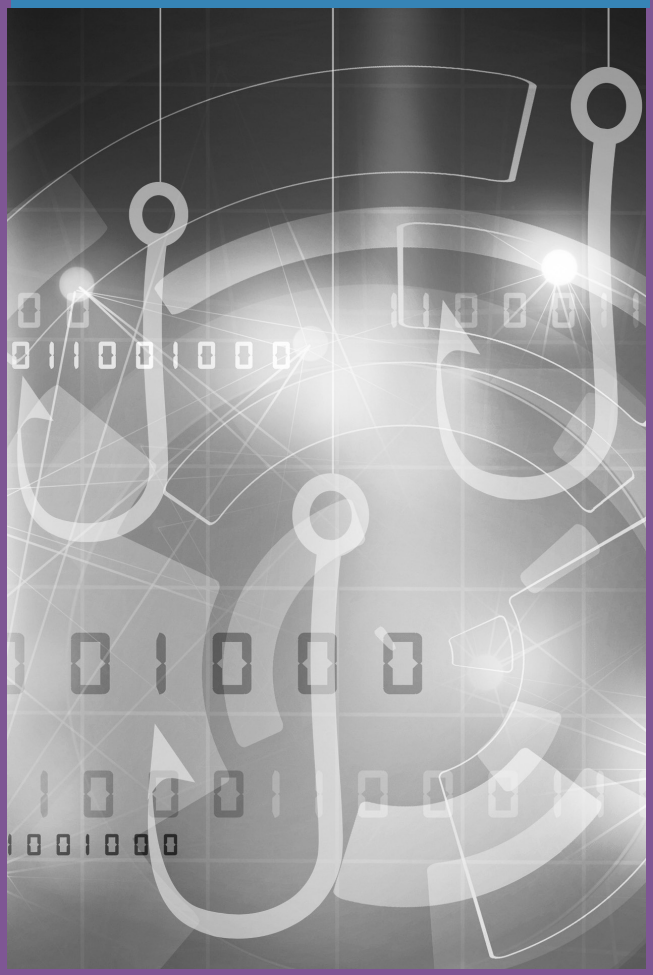
Tolep also stressed that any time companies update their vendor master data, they had better make 100 percent sure it is legitimate. How can they do that? Again, the solution is simply picking up the phone. "I have accounts payable underneath me, and we do have a process in place—be it an invoice that comes in, an email, whatever—if they are asking to update banking information, we will go out to our database and look up the phone number we have on record," said Sarah Schaus, assistant treasurer and AVP for Allianz Life Insurance Company and also a member of AFP's Treasury Advisory Group. "We don't use the phone number that's on the invoice or in the email, because if it's bogus, they're just going to have us call them, and they'll have their speech ready."

Schaus has had AP under her since the 1990s and even when invoices were coming in via snail mail, these protocols were still followed. And they've been incredibly successful; Allianz has never been duped by any of these scams. However, many companies have, and she believes it could be because many AP teams aren't directly under treasury. "There isn't always that strong connection or relationship; AP is often under controllers and they may not even know if there was a duplicate payment because that falls back to treasury to be responsible for. So by having it all underneath me, my wire desk knows to talk to AP, and we have those controls in place, so we have that thorough communication all the way around," she said.

Additionally, the industry that a company operates in can also determine its vulnerability to supplier BEC scams. A company like Allianz has a handful of vendors that they work with, and that makes it easy to thoroughly check every request that comes through. But a manufacturer with a multitude of suppliers would have a much more difficult time vetting every single change to payment instructions. Therefore, treasury and AP departments in those sectors need to be extra careful.

"If you're Hershey's, you've got a huge database of vendors and you probably get a lot more pings to change banking instructions," Schaus said.

5 RECOGNIZING PAYROLL DIVERSION



According to the **IC3 2018 Internet Crime Report, the IC3** received more than 100 payroll diversion complaints that totaled $100 million in losses. In these scams, criminals target an employee directly via a phishing email that captures their login credentials. Once these are obtained, they can access the employee's payroll account. From there, they typically add rules to the account that prevent the employee from receiving alerts, and then change the employee's direct deposit information so that the payroll funds go into their own account (often a prepaid card). Industries hit by these scams have most frequently been education, healthcare and commercial airlines.

These scams could also account for some of the uptick in ACH fraud that was observed in AFP's fraud survey. According to Nacha's Herd, 98 percent of payroll payments are ACH transactions. But again, he doesn't believe these transactions are being targeted because they are ACH payments. "They are trying to identify easy ways into the corporate back office," he said. "Criminals will target wherever there is a weak link. And ACH is simply how payments are being made on the back end."

Herd added that scams like these represent a bit of a mind shift away from account takeovers. "In an account takeover, criminals would have to steal your account credentials and then they would log on as you. Now they just simply raise their hands saying, 'Send me money,' and they see if you will," he said.

As for advice, Herd stressed that companies should never break their own protocols. "It may sound kind of simple, but don't ignore your own procedures, practices and controls," he said. "Don't abandon your plan. We know of a case where a payroll department had proper controls in place, and then chose to ignore them because they thought the order was coming from the superintendent. So they ignored their own controls."

6 AVOIDING ACCOUNT TAKEOVERS

But even if certain criminals are favoring social engineering methods over account takeovers, that doesn't mean account takeovers are a thing of the past. As noted earlier, these attacks saw a considerable increase in 2018. But for treasury departments that want to protect their accounts, it's important to understand that they also have to be aware of who can access their systems.

"It's not just your own systems; it's your partners' systems that might tie into your systems," D'Antuono said. "Maybe your system is locked down, but your partner is logging into your system from their place of business and their system is compromised. So it's also knowing who has access to your systems."

He stressed the importance of downloading patches and updates. Missing out on just one can lead to an entire system being compromised. "People get a notification about an update on their phones, and it's easy; they usually do it overnight. But computer systems? Not so much. Some people don't even update their home computer systems enough, and there are a lot of businesses out there—not usually the large ones with full IT departments, but the smaller, mom 'n' pop businesses that would contract IT out to somebody—they don't get those patches and you have to."

Carlsson noted that companies must keep a log of any individuals internally or externally that can access their data. That way if something happens, you know all the potential people who either messed up or were involved in the incident directly. "It would be smart to have some sort of procedure so if something happens, you know exactly who can be in the system," he said. "And I don't know how well thought-out that is in corporations."

8

KEEP YOUR EYES OPEN

No two companies are the same, and therefore, every organization is going to have to deal with its own unique set of fraud threats. Whether a criminal is using sophisticated social engineering methods to launch an intricate BEC scam on your company, or you're hit with old-fashioned check fraud, you have to prepare yourself accordingly. If you've experienced a fraud incident, look at what your peers have done to avoid getting hit. Their situation more than likely won't be identical to yours, but there will probably be enough parallels that can be drawn that it can help you avoid being affected in the future.

KEY TAKEAWAYS

1

Treasury departments must ensure that any employees who touch company money are aware of the latest threats and learn to recognize the telltale signs fraud.

2

When a company is hit with fraud, the first step should be to report it to the Internet Crime Complaint Center (IC3).

3

Business Email Compromise (BEC) scams continue to thrive; 58 percent of treasury and finance professionals reported that payments fraud at their companies came as a result of BEC scams.

4

BEC scams involving routine vendors have been increasing, particularly because these attacks are harder to catch than the traditional CEO fraud scams.

5

The recent surge in vendor-focused BEC scams has resulted in a spike in ACH fraud. Nacha has a list of current fraud threats on its website, as well as a list of recommendations that treasury professionals should review.

6

Payroll diversion attacks have been surging, topping $100 million in reported losses in 2018.

7

Companies should not only monitor their own systems, but their partners' systems as well. This is key for preventing account takeovers.

About the Author

Andrew Deichler is the multimedia content manager for the Association for Financial Professionals (AFP). He produces content for a number of media outlets, including AFP Exchange, Inside Treasury, and Treasury & Finance Week. Deichler regularly reports on a variety of complex topics, including payments fraud, emerging technologies and financial regulation.

ASSOCIATION FOR FINANCIAL PROFESSIONALS

About the AFP®

The Association for Financial Professionals (AFP) is the professional society committed to advancing the success of its members and their organizations. AFP established and administers the Certified Treasury Professional and Certified Corporate FP&A Professional credentials, which set standards of excellence in finance. Each year, AFP hosts the largest networking conference worldwide for over 6,500 corporate finance professionals.

4520 East-West Highway, Suite 800
Bethesda, MD 20814
T: +1 301.907.2862 | F: +1 301.907.2864

www.AFPonline.org