Sonal Bullard:

Hello and welcome. I'm Sonal Bullard, Executive Vice President and Head of Strategy for the Wealth Management Group at Regions Bank. We're very happy that you could join us today for this Regions webinar on fraud. An extremely important topic for everyone, whether you're a business, a nonprofit, or an institution. It's an old problem of course, but there are so many new ways that criminals are using to steal and they're constantly changing. Fraud security nowadays is deeply entwined with cybersecurity, so it's more important than ever to be up to date on the latest scams and ways to stay vigilant. We're fortunate to have two Regions specialists with us today who are ready to help us all understand how fraud persists, the methods that fraudsters use, the types of systems and platforms they target, and how organizations can improve their defenses. These two bring years of experience to the table and they've spent time studying fraud tactics and trends and working directly with Regions clients to build awareness and robust protections. Randy Wilborn and Billy Smith, thank you so much for being here. Could you both take a moment to introduce yourselves? Randy, we can start with you.

Randy Wilborn:

Sure, I'll be glad to go first. My name is Randy Wilborn. I work with Regions Bank where I've been for about 19 years. I've been in the banking industry for almost 30 years, but I work as a product manager within our Treasury Management Group, so that means I get to build and develop products that help prevent our clients from becoming victims of fraud.

Billy Smith:

And I'm Billy Smith. I've actually been with Regions seven and a half years, 25th year in the industry in financial services. I'm an institutional relationship consultant, so I work directly with clients, and I can see how some of these fraud tactics actually affect the clients that we work with.

Sonal Bullard:

Thank you both. We're excited to have you here because your insights into people and processes should really help us cover a lot of ground today with this very important topic and this persistent challenge. Let's dive in. Every institution we know is a potential target. The Association of Finance Professionals have stated that both larger institutions and smaller institutions have reported fraud attacks equally so, and they're all being targeted. So one thing that makes fraud tricky to understand is that the perpetrators often combine a few different tactics in order to target an organization. So we're going to talk about three of these tactics today. One of them is business email compromise or BEC. The second one will be whaling, and then the third one will be payments fraud. And this will help everyone understand what these fraud tactics really are and what does it take to succeed and what we can all do together to create solutions that protect the institutions that we work with. Let's start with BEC. It's a really stubborn problem and it's one that is still very common among cybercrime in general, and it so often factors into the other two crimes that we're going to be talking about today, whaling and payments fraud. Randy, I think we should start with you on this one. Most organizations have probably been aware of business email compromise or BEC for years because it's been so prevalent. Can you give us your point of view on what is meant by BEC and how it's evolved and how it remains a persistent threat?

Randy Wilborn:

Sure, absolutely. I'd be glad to. When you hear us talking about BEC or business email compromise, at its basic core, we're talking about a case where a bad actor has somehow compromised the email applications could be belonging to one of your partners and then sending an email to your organization convincing someone at your organization to make changes so that future payments, instead of rightfully going to you, could be redirected to an account that belongs to a bad actor. What we've also seen is they may target certain people at your organization, those who have the ability to send a wire transfer or an ACH transfer; at the very core, that is what we mean by BEC or business email compromise.

Billy Smith:

And I'd like to add to that, Randy, is also, it's the processes in which they're requesting funds coming through email. Sometimes it can be difficult to tell that the email coming through is a fraudulent email.

Sonal Bullard:

Yeah, wow. So that's good to know and thank you for helping us unpack that. You bring up several points that I think are relevant to my next question. Part of the problem it seems is that the supply chains and the vendor ecosystems have become increasingly complex in recent years. We're so connected through email and payments and other ways sometimes to many third and fourth parties along the way. Randy, tell us how you think that might elevate the risk of BEC fraud.

Randy Wilborn:

Sure. Absolutely. Most of us do a pretty good job knowing who our vendors are, the vendors that we do business with every day that we have a contractual relationship with. But what we don't know is we don't know who our vendors' vendors are. We do not have a contractual relationship with them. What we've seen in the industry is that that fourth party vendor is what we call them, may actually use some type of a tactic to get into the email platforms that belong to our vendor and then send that email to an organization. Sounded like it actually comes from our legitimate vendor who we have a relationship with, and then convincing them to send a wire transfer thereby executing the business email compromise attack.

Sonal Bullard:

Wow. Okay. Well, not only that, but it sounds like technology continues to keep evolving, so can you explain how BEC has become kind of a hybrid attack and how it extends beyond maybe an employee's inbox, Randy?

Randy Wilborn:

Yeah, sure. I'll start with AI is the one that comes to mind–generative information–that's out there. We know that more and more of these bad actors are starting to use AI to create tools to simulate what may appear to be a vendor that we do business with all the time, but it really is not only do we see it with emails, we see it in phone calls where it could actually have a voice that sounds like somebody that you're used to doing business with, but it is not, or a text message that used the same type of language that somebody you wouldn't normally do business with, but it's really not them. We just may depend on that thinking that it's the person that we've always done business with will make changes to the payment information or someone in our company will. The next thing you know, the future payment that takes place is not going to someone that you use as a vendor, but it's actually going to a bad actor.

Billy Smith:

And I'd like to expand on that. They're also, when you get these fraudulent emails, they're also using tactics in which they put pressure on the person receiving the email to be hurried. They need this to be done quickly. They need this to be done right away, and sometimes that pressure can make somebody overlook something that would normally seemingly look improper.

Sonal Bullard:

Right. Wow. Any other details you might offer about what your clients might be seeing when it comes to be business email compromise and maybe how they've fought that?

Billy Smith:

We're seeing emails coming through where they're just simply making a change to an account number, and so you may not notice that a 10-digit code has been changed. And so following processes to make sure that we're confirming that these emails are correct is one of the ways that many of our clients are being able to protect their accounts by having a secondary process or a secondary approver to make sure that what's coming through is actually valid.

Sonal Bullard:

Wow, that's great. Good to know that that's what the tactics they're using. What are the few best practices that organizations can use to prevent these kinds of incidences? Billy, let's start with you.

Billy Smith:

So as I was just mentioning, having proper standards in place, policies in place to make sure that you're following a process to confirm that these requests are right. As a matter of fact, I'll share with you that I just recently learned of a survey in which less than 60% of companies actually put standards and policies in place to be followed, and less than half of those are actually testing whether or not those policies that are in place are actually working. And so having proper standards and policies to follow really could make a huge difference.

Sonal Bullard:

Okay. Right. Randy, what are your suggestions?

Randy Wilborn:

Sure. Just to add to that, and I agree with everything that Billy said here, but education, I just always go back to education, educating the employees at the organization from the top to the bottom and what the scheme looks like, how it's carried out, and how they can make decisions to make sure that we don't become a victim of, in other words, making sure they don't click on a link that's in an email or respond to an email that seems like it's from a legitimate company that we do business with, but it may not be. So education is the first part of it. Also with business email compromise always say, make sure that they verify that if there is a request to make changes for future payments that you verify in a way different from which you receive it. So if there was an email that requested somebody at your company to make changes for future payments, verify it through a phone call or if the company's upstairs or something like that, walk up there to them and speak to the person. Same thing if there's an executive officer who asks you to send a large wire transfer that they wouldn't normally do, verify that they really did ask for that in a way different from which they received that request.

Sonal Bullard:

Yeah, that's great advice. Billy, you were saying about an attack starting with an employee anytime kind of sets us up perfectly to discuss the next topic, which is whaling. Randy, could you set us up with a definition of what this type of fraud really is and how do we know if it's similar or different from a term we might be familiar with called? Right. Right. Can we start there?

Randy Wilborn:

Sure, absolutely. I agree. Whaling has been around for a while and phishing is much more broader, but when we start talking about whaling, that's when it's getting very specific. In other words, the bad actors really trying to target a very specific group of people. These are normally some people who may have the authority to send very high or very large wire transfers or to authorize that a large amount of data be released to someone who requested, or it could be someone who has an executive like title. They're on the board of directors, CEO, CFO, and these bad actors spend a tremendous amount of time when they're targeting these particular positions much more time than they may spend at just the average employees within the company, but because these guys have a much larger authority to originate a payment, that is really where we see the whaling being different from what we've seen in the past. The target, the amount of time that it takes to go out to them, and the ability to access transfers or amount of data that can somehow benefit the bad actor.

Billy Smith:

And actually the sophistication around whaling is much different than you would expect with just email compromise. So you might think if someone compromises the email, the first thing they would do is request funds to be transferred right away. But in a whaling scenario, as Randy's pointed out, they're trying to get to the CFO or the COO who can request large amounts. And so what they're doing is they're actually taking their time to watch communications going back and forth between these people that are in charge and the people that have to move the money, and they're saying, how are they communicating? How do they sign their emails with a TY instead of a thank you? And getting very sophisticated with that, and I'm actually aware of a scenario in which a third-party administrator's email was compromised and the bad actors were sending emails from the third-party administrator, and what they were doing is they were actually reaching out and speaking as if it were the CFO using the same language that CFO would use. And so they sent an invoice to be approved, and if it weren't for standards and processes being followed, that invoice could have gone out. And so they sat in there for quite a long time, very sophisticated in how they sent that email through.

Sonal Bullard:

Wow. They're observing behavior. It looks like when I think about whaling, I think of a campaign to trick a high-level employee into a very large transaction or into authorizing a very large transaction rather, or to trick someone into thinking that a high-level employee has actually authorized the transaction. Should we be thinking of this fraud and the people it might involve in broader terms, perhaps?

Randy Wilborn:

We absolutely should be thinking about it in broader terms. The idea of only going at the person who has the privilege just to send a high dollar amount or to send a wire or give the permission to send a wire or something like that. We need to be broad on that. Sometimes it could be the executive assistant to that person who is the one that controls the calendar and goes through some of the emails and things like that. If a fraudster is able to somehow take advantage of their email account and then send requests out as if those came from the person that she supports and works with, then someone is going to receive that email act to it really quickly, just like you were talking about and can send a large dollar amount that should not be going.

Sonal Bullard:

Right. Wow. So is there a tactic that focuses solely on work-related objectives, or are there instances in which scammers might blend personal and professional messaging to launch a more sophisticated attack?

Billy Smith:

So with social media and the way that we all communicate to everyone how excited we are about going on vacations and the things that we do, it could be easy for fraudsters to watch what's happening in a CFO's life and know that this person is out of the country at the moment and take that opportunity then to reach out to the executive assistant and say, Hey, I'm out of the country. There's an emergency. I need you to move these funds and take advantage of what they see on social media. So it's not all about what happens at the workplace. It can be what's going on in your personal life as well.

Sonal Bullard:

Have you heard about any incidences that might've taught you any best practices that can help an organization spot those very targeted scams before the damage could occur?

Randy Wilborn:

Sure. I've seen at least one that we've seen in the industry take place, and it was pretty clever as a matter of fact, and this is one where the fraudster was able to somehow get malware onto the servers of a particular organization and the way they executed, they basically used a jump drive, went to the parking lot the night before, and they noticed because they looked at the video cameras later on and they basically dropped a jump drive into the parking lot where the employees would park, and on the outside of that jump drive, it was written in small letters, annual bonuses for the year. And so the person employee who comes in that morning parks their car, they see the jump drive, they look at it, see an annual bonuses. All of a sudden they're really curious about what's on that jump drive going through the front doors, wave their badge to let them in, walk right past security, go up to their desk, log in with their user ID and 16 digit password, take that jump drive and stick it right into their laptop and think that they're looking at a real list of people who are going to receive bonuses, realizing they're not on that list, but in the background, they know what's happening.

Malware is being downloaded into their computer, and there are variety type of malwares that are out there. In this particular case, the malware got attached to some email that person later sent throughout the organization, and it began to spread. The next thing you know, this bad actor is able to take advantage of the email platform that's there and begin sending emails to different places, trying to get some of the vendors that the company works with to make changes for future payments that are going to be sent for invoices that are received.

Sonal Bullard:

Wow. That's quite a story. What about you, Billy? What do you think?

Billy Smith:

Yeah, so in my world, we get requests for funds to be wired out and changed out. And so sometimes what will happen is you'll have an invoice or an email come through that will have something changed on there, and we actually saw a scenario. I'm familiar with the scenario in which that happened and because of, as we mentioned before, and I'll say it again, having the proper standards and processes in place, we're able to recognize that those were improper emails.

Sonal Bullard:

Wow, that's amazing. Well, thank you both. And Billy, by bringing our discussion around payments, I think we've set us up to talk about something that might be surprising in this age of digital and cyber. Everything many banks are reporting, check fraud is trending up over the last few years where it had been declining significantly in the past. Why do you think this is happening, especially when institutions, their vendors and their customers are using fewer checks than ever? Randy, can you shed some light on this?

Randy Wilborn:

Sure. Absolutely. That AFP survey, we look at that very closely every year as well. In fact, we use it to help develop products so that we can help our clients not become victims of the different fraud patches that are out there. But I did realize on there that we see that check fraud compared to other payment types and it comes of volume is larger than those other payment types. And when I see talking about payment types, I'm talking about wire transfers, ACH debit, ACH credits and credit cards, but check fraud in terms of volume is much, much higher. But the reason why we think that has happened is because check fraud is pretty easy to execute from a fraudster's perspective. Every time that there's an organization who hands out a check to someone, whether they're paying a pizza guy or someone to do their job or another vendor, they're giving them a lot of information about their accounts, they're giving them an example of what their check stock looks like.

They're giving them their account number because that's printed at the bottom of the check. They're also giving them their route in transit number, which is used to direct a check to a certain bank that's at the bottom of the check. And also what people don't think about is they're also showing them what the authorized signature looks like. That's on the bottom of that check, and one more is the check number. They have an idea of the most recent check number that was written. So if that check gets into the wrong hand and a fraudster wanted to duplicate that check to create some counterfeit checks, they know what the check stock looks like, they know what the authorized signature looks like, they have a general idea of what the last check number was that was used as well, and they can use that to try and create a counterfeit check. So because it is so easy to execute that scam, that's why we said when we look at those numbers that you were just talking about and we see that check fraud in terms of volume is much higher than those other payment types that we see in the survey, that is one of the main reasons it's easier for a fraudster to execute that scheme.

Sonal Bullard:

Wow. Speaking of the most recent AFP survey, we've noticed that checks and ACH debits were two of the payment methods most impacted by fraud, while fraud via wire transfers is trending downward. Randy, can you shed some light on these numbers?

Randy Wilborn:

Sure, absolutely. For the past six years, we had seen that wire transfers was trended upward and didn't start to take just a slight downtick according to the survey that we looked at. We know that that is because that wire transfer uptick that we saw about five years ago was related to business email compromise. In other words, those emails that were being sent to someone at a company was basically asking them to make changes for future wire transfers that were taking place. What happened, a lot of the organizations became educated, like we just talked about the education piece, and they started putting tools and a process in place to help the employees recognize when there's a potential business email compromise attack going on that will be asking them to make changes for a wire transfer. So because of education, we saw those wire transfer numbers start to tilt downward.

At the same time, we start to see these fraudsters shift their attention from the wire transfers related to business email compromise to the ones that are ACH. In fact, what we start to see in that last survey is that we saw ACH debits related to fraud take place. We saw it start to tick up a little bit more. What we know is going on there is that these frauds are using that ACH debit to do four things. They want to send an ACH so that they can see if that account number is a good one, they want to send it, see if it's going to reject. A lot of times if it's rejected, it's going to say bad account number, or you should use another account number as well. They're also looking to see if there are any tools on their account to see if that organization has some tools that will prevent anybody from posting an ACH transaction against their account, whether it's a debit or a credit as well.

And then they're looking to see if they could reverse that ACH transaction. Normally with our NACHA rules, if there's an erroneous transaction, then the rules allows for certain reversals to take place. So if all four of those things can take place, the bad actor can then know that we have an account that is a good target for us to later send a large debit against that account. So that's why we're starting to see those numbers from the ACH credits and ACH debits take up a little bit in that survey that you're talking about.

Sonal Bullard:

Wow. Okay. Well, Billy, how are Regions' clients experiencing these trends? Can you walk us through what payment protections come into play when it comes to institutional banking?

Billy Smith:

Yeah, so what makes institutional a little bit different is the accounts that we hold aren't demand deposit accounts, meaning that they can't be transacted by anyone outside of Regions Institutional Trust. And so requests are made through email, through telephone to a Regions partner who would then send those funds out. And so we have that extra layer of protection as opposed to electronically being able to send in requests. We have to get physical requests, and then we can follow our processes to make sure we confirm with our folks that these funds should be going out. And so it's a little bit different level of protection in the trust department.

Sonal Bullard:

Yeah, that’s good to know. These are all important elements to institutional trust, and they help to illustrate the ways we can work together to help mitigate fraud, but ultimately, I think we all have to think of ourselves as part of the fraud protection solution. Perhaps we could end today with each of you sharing some of the best practices that you might recommend to your clients as well as your Regions colleagues.

Billy Smith:

Yeah, so first and foremost, as Randy mentioned, employee education is very important. Anybody who works within the organization really needs to know what’s happening out there, what types of frauds are being perpetrated. Many of the folks that might see this webinar might think to themselves, I had no idea about whaling or some of the things that have been happening out there. So education is hugely important. And then second, as I mentioned before, having policies and standards in place. And the reason that’s so important, at least in my opinion, is when the pressure is on to do something quickly. If you have standards to follow, you’re less likely to fall for something when you’re emotionally involved in trying to move money quickly.

Sonal Bullard:

Yeah, that’s a great point. How about you, Randy? What would you offer?

Randy Wilborn:

Sure. Just a few things since we were just talking about check fraud and how easy it is to make changes to checks and to counterfeit checks as well. I recommend when you can replace send out a check with an electronic payment, then that’s always a good idea, use ACH or use wire transfers. If you have check stocks, make sure you store them securely so that everybody does not have access to those checks as well. Using dual signatures or dual approval for any checks that can be needed to make sure there’s not just one person who has the ability to write a check and also reconcile the accounts as well. The other one that we talk about is making sure that your employees know about emails and can spot emails that could do harm to your company. Most of those are going to be external emails.

There should be something that indicates that this external email and what we’ve seen a lot of companies do, they will actually test their employees from time to time by sending an email. That's not really a bad email, but it looks like it is to see how the employees are going to react. The last thing I'll mention is just making sure there's a good policy and procedures like you're talking about around password protection. It used to be a time that we wanted employees to use passwords that was six or eight digits long and changed them every 30 days. Now, what we see in the industry that employees within organizations should use pass phrases and they can be changed 60 to 90 days as well. Most of the things that we see out there is just human nature. Fraudsters know that people use the same email passwords that they use at home, they will bring it to work. In fact, we've seen the surveys, and we know what the top passwords that are out there. We know that they're the word password. We know that they're 1, 2, 3, 4, 5, 6, and we know that it may be your favorite school or your pet's name because we can get that information off of Facebook. The fraudsters know that already, so we recommend they definitely be cleverer in terms of the payroll password they use for their accounts.

Sonal Bullard:

Well, Randy, Billy, I have a question for each of you. Have you experienced personally any sort of business email compromise or phishing? And if you have, how have you handled it?

Billy Smith:

I actually had a very unique one where my antivirus popped up on the computer and said, it has expired, and you need to update your antivirus. And then it provided a telephone number to call. And so what I did, instead of calling the telephone number, knowing that a very good chance that that was compromised, it shouldn't have popped up to begin with. I actually went and searched out what the proper phone number was to my antivirus, and they weren't the same. And so interestingly, I called the phone number to find out, and when they answered, they started asking for things like my account number and then they could update it over the phone and could I just pay for it over the phone with the account information and all those types of things. So interestingly enough, you get nervous when your antivirus pops up and says, Hey, your computer's no longer protected, quickly call this number. But luckily, I had checked to make sure that that number was a right number, and certainly it was not

Sonal Bullard:

Preying on that whole idea of urgency to get you to act. Yeah. Wow. How about you, Randy? Have you experienced this in your personal professional life?

Randy Wilborn:

Yeah. Not necessarily business email compromise attempts, but I have seen phishing attempts, and most are on a personal life, for example, using social media. Sometimes I would get requests from someone who looks like they're your friend but may not really be your friend. And I realized that these frauds out there is a lot of times trying to get your password. They know a lot of times people may use the same password on their personal social media platform and use it on their work as well, which I strongly against that one. But once there was an instant message that came to me and say, Hey, click here to view the pictures from the party last night. Well, number one, I know that I wasn't invited to a party last night, and although I'd love to see the pictures, I'm not going to click on it because that's a great opportunity for malware to be downloaded onto my computer and somehow take over my own email platform and try and steal the credentials that I use at home. So no, I won't click on those and yes, the attempt has taken place.

Sonal Bullard:

Wow. Wow.

Randy Wilborn:

What about you? Have you ever had anything happen?

Sonal Bullard:

I actually have in the last few weeks. In fact, on my work email, I received a message that did look a little bit suspicious. The message indicated came from our human resources team, but it had a request in there to validate some credentials that it was just unusual. These were credentials that are known in my own profile in human resources, and so instead of clicking on the link or responding to the request for those credentials, in fact, I went out to my secure portal, a secure human resources portal looking for a notification, asking me for any of that information, and it didn't exist. And then I was able to validate that that request was not actually real by calling to my HR professional. So I was glad to have avoided clicking any link that would have taken me perhaps into the hands of some fraudsters.

I think it's super interesting that all three of us have recently have seen some of this phishing activity within our own lives. Thanks for sharing. I want to extend a collective thank you to our panelists. And special thanks to everyone who has joined us today for this webinar. We hope that you feel better prepared to spot fraud before it happens and keep your communications online and otherwise safe. We encourage you to visit Regions' help and support, where you can read through our fraud prevention and security frequently asked questions. You can also read through articles that explain Regions features for security and what you can do to better protect your personal and account information. And you can always stop by a Regions branch to speak to a Regions banker, relationship consultant or advisor, or make an appointment by phone via regions.com.
Thank you for joining today.