M&T Bank
Fraud & Cyber Threats to Business in a Remote Environment

August 5, 2020
12:45 PM EDT

Operator: At this time, let's begin today's M&T Bank webinar, Fraud and Cyber Threats to Business in a Remote Environment. It is my pleasure to introduce your moderator today, Frank Lago, Group Manager, Treasury Sales.

With that, Frank, I'll hand the floor over to you.

Frank Lago: Thanks, Jessica. Good afternoon and thank you all for joining us today. As Jessica said, my name is Frank Lago and I'm the line of business sales manager for treasury management at M&T, and your host today.

A couple of housekeeping items for me before we begin. Today's program has been approved for up to one CTP and FPNA recertification credit by the Association for Financial Professionals. The certification letter will be available in the resource center at the close of the session. Also, as Jessica mentioned, the webinar is being recorded and following the presentation today you will receive a follow-up email that includes a link to the replay as well as additional resources.

We are living and working through unprecedented and uncertain times. The disruption caused by the global pandemic has been absolutely devastating for many businesses and individuals. We cannot overlook the fact that many businesses will never recover.

However, the disruption has resulted in tremendous innovation. It has been a test of our adaptability to a changing environment. An enormous number of workers have, not always seamlessly, of course, moved to a work-from-home environment. Countless others are working in offices with minimal staff to avoid clustering. We have collectively risen to the challenge to keep our businesses afloat and continue to be productive and competitive. Some have even been able to increase productivity and are thriving in a remote work environment.

Unfortunately, those changes were thrust upon us with a rapidity that has created vulnerabilities. And while we continue to adapt and improve, bad actors have also

adapted and are increasingly attacking our vulnerabilities.

We've come together today to alert you to the changing threats in our new normal and provide (inaudible) you can take back and reduce the likelihood that you and your employers will be victimized by the fraudsters.

M&T is pleased today to have two experts joining us to inform and educate you on how you can better prepare and protect yourselves. Leigh Balcom joins us today from our financial crimes division. Leigh has regularly been called upon as an expert in cyber security and bank fraud. He performs countless educational sessions like this one for the bank's customers and our employees. Leigh has many years of experience in financial crimes and performs tireless work to weed out fraudsters, protecting the bank and our customers.

Kristen Karkau is a commercial product manager with an expertise in digital payments. She played a key role in product development at M&T and has led our journey to fraud-proof our payments networks to the extent possible.

Leigh and Kristen will walk you through the risk matrix, new threats that a remote work environment has exposed, and provide concrete steps you should be taking right now to tighten controls and protect yourselves and your businesses from fraudulent activity.

At this point, I will turn the presentation over to Leigh to get it started. Leigh.

Leigh Balcom: Thanks, Frank, and good afternoon, everybody. Thanks for attending. We appreciate it.

Let's start with this slide, here. This says 81% of companies were targets of payment fraud last year, so 4 out of 5 businesses are targets of payment fraud. That doesn't mean you're necessarily a victim. A lot of that is going to depend on you. But four out of five were targets.

So if you're one of the 19% that hasn't been -- that don't think you've been targeted already, it maybe means that somebody in your office hasn't told you that somebody tried to scam you, or the fraudsters just haven't gotten to you yet. But I would (inaudible) is they probably will try.

Now, a lot of that (inaudible) check fraud still reigns supreme. There's always a lot of check fraud, whether it's altered checks, counterfeit checks. What we're finding is they're getting these checks, stealing them from the mail is a lot of them. Or they received a check, somebody received a check, they copy it, they wash it. There's many different ways that they do check fraud.

ACH fraud has been up. 40% of companies have experienced wire fraud and we are seeing three out of every four customers have experienced a business email compromise. We're going to talk about that in a little bit.

One of the trends that we've seen is when we first started tracking business email compromise, that it was targeted really towards larger companies. Why? Well, they had more money. But what fraudsters found is that they also have better security systems and better controls, so they targeted smaller companies. And now they even target

individuals.

So let's go to the next slide. The cyber crime landscape, $2.1 trillion in 2019, that's from Juniper Research. Now, because of these data breaches, data is so much more -- that's so easy to get, so easy for a fraudster to get their hands on. Every data breach we've seen from Equifax to AOL to Sony, etc., they get little bits and pieces of information and then they can create a story, create a profile of a company. Now, what do you have that they want?

So you've got money of course. Even if you don't think you have a lot of money, you still have money and they -- and you're transacting and creating bills and receiving money. You are creating something the fraudsters want. But let's not stop there.

You also have your intellectual property, the reason that you're in business, what you sell, what you've created. You have your customer information. They're going to want that. Employee information, there's loads of information there, and even medical records. Now, they take this information. They package it up and then sell it and a good package will go for $15 but a credit card number or a license number or a social security number can go for as little as $0.20. But the more they have on somebody, the higher those packages go for.

On the next slide, get there -- sorry about that -- there we go. Kristen, you want to read this one?

Kristen Karkau: Yeah. So really, the biggest threat is who can expose your business, and unfortunately, it's both internal and external threats. So internal, it could be employees. And a lot of it's even inadvertently. They could download software, they could accidentally share something that they're not supposed to, you know, by being negligent. There's -- you know, it's out there, that vendors share information. They may notify that they're doing business with you, and there's a link, and it kind of opens up the gateway for fraudsters to realize -- hey, this vendor does business with company X and let's see if we can impersonate the vendor and try to get money out of company X. And that's really a lot of what the external threats are.

There's (inaudible) organized criminals, you have people in nation-state, you have individual threat actors, and their entire goal is to steal your information. And they'll do that utilizing viruses, malicious code, disrupt business via cyber vandalism, sometimes they're in pursuit of social or political agenda. So really, it's anybody and everybody can be exposed, and they're out there to gain whatever information they possibly can.

Moving on, and (inaudible) the next slide. Leigh, are you back in?

Leigh Balcom: Yeah. I'm there. First poll question.

Frank Lago: Okay. Well yeah. We're at our first poll question so I'll actually jump back in here. I apologize to those on the line for having a little bit of audio issue. Hopefully we get that taken care of, though. Working on that.

But -- so we have a poll question up here. We'd ask everybody on the line to go ahead and submit your answer to this question. Has your company been a target of financial

fraud in the past 12 months? While we're waiting on that, Leigh, I've been around a long time, long enough to remember when positive pay was a brand-new tool to combat check fraud back in the late 80s. I know you haven't been around that long, you're a much younger man than me. But how would you say the current environment measures up compared to the fraud presence in the last couple of decades?

Leigh Balcom: Well, like I said before, check fraud is still extremely popular amongst fraudsters. Probably it's the number one vehicle that they use. But the internet has made things much, much faster, and not only that, but it's given the fraudsters a much bigger sandbox to play in. You know, it's harder for fraudsters to get involved in wires now via email, phone calls, and impersonating somebody else they can insert themselves in the conversation and divert payments. So it's just a bigger sandbox for fraudsters to play with.

Frank Lago: Okay. Well, thanks for that. I think we've probably given folks enough time now to answer the poll so I'm going to go ahead and advance it here. And everyone can see on your screen here that now we've got 61% of this audience -- I'm not quite sure exactly how many folks we have on the phone, but it's in the several hundred -- so that's a -- a pretty telling statistic there that 61% of those who have joined us today have experienced financial fraud. Hopefully again as we go through the remainder of the presentation, you'll learn some lessons and we can help you to combat potential fraud issues in the future.

So with that, I think I'm going to move the presentation forward, and Leigh, I'll ask you to jump back in here.

Leigh Balcom: Sure. Yeah. That 61% number is very impressive for everybody on the phone, because as we said at the top, the number of -- by a study from associated -- Association of Financial Professionals said that the number was 81%. So you guys are doing a good job protecting yourselves.

So let's talk about what cyber criminals do with the information that you have. The web as we know it, the news sites that we go to, everything we can do on the web, is known as the web. There's also a deep web, that your company has an internal site, that would be considered the deep web. And the dark web is a large, giant -- can be a large, giant marketplace. Think of like an Amazon, but you can buy all kinds of good things and bad things. But some of the things that you can get is credit card information. You can get usernames and passwords; you can buy hacking service kits such as like a ransomware kit. You can share fraud schemes. You can -- a lot of people will trade back and forth on potential victims. This person has very low security and might be ripe for a fraud.

So there are listed goods as well, drugs, guns, people. So one statistic that I saw said that the web as we know it, the web that we use every day, counts for about 4% of what is on the actual internet. So the other 96% is that deep web and dark web. So that just gives you an idea of how big that the internet really is.

Leigh Balcom: So fraud has increased during these troubled times, and here's why. We've got distracted management, we've got depleted staff, people working from home, cash flow struggles, new jobs for money mules. So there's a lot going on with things that are happening right now. You're not seeing your staff every day, so you know, we trust that everybody's working but we can't talk to them and see if a payment is going to the right place or if it isn't. So again, it's -- and the other thing about it is, it's a new way of working for all of us. I'm not used to having my staff working from home. I'm used to basically being able to walk outside of my desk and going over to their desk and seeing what's going on. It's a new world for us, and I think people are adapting to it very well, or at least I feel like I am. I feel like my team is. But it's still new.

So on the next slide we're going to talk about what has changed with switching to a remote environment. So we've got employee requests change in direct deposit at HR, vendor faxes changed account information, manager requests in person for employees to send wire.

Frank Lago: Hey, Leigh. While we're waiting to see if Kristen comes back and joins us, let me just ask you a question. So you're talking about the increased risk in remote work environment. Can you tell us, talk to us for a moment, about how the bad actors are exploiting those changes that you're describing here about these remote environments versus an in-office environment?

Leigh Balcom: Yeah. They're taking advantage of -- they're taking advantage of certain things. Like your company, you probably have a pretty good, secure system. Your internet is pretty secure and you've got protections on your computers. That might not be the case at home. So you know, and I think that the Verizon or Spectrum, whatever system you use, is pretty good but you're still also susceptible to things that might be on your computer. And these could be cookies that are placed by -- by very good websites. But -- or you may have been a victim and you don't even know yet, of a phishing -- target of a phishing scam, an email. So those things could be on your computer. So mostly what's going on with this right now is that the system that we use at home in some cases are not as secure with what we have in our offices, and that kind of creates a potential problem for the business. Because if they can get at me, then maybe they can get at things that I have within my business.

Frank Lago: Welcome -- welcome back, Kristen. Sorry about that.

Kristen Karkau: Thank you. Sorry about that.

Frank Lago: Yeah.

Kristen Karkau: Moving on, so I'll go to the next slide. Thanks for taking it over. So business email compromise, it's changed a lot as Leigh mentioned at the beginning. You know, a few years ago we were kind of hearing that fraudsters were impersonating vendors, using email addresses that look similar to an existing email address and emailing an employee of the company who may be responsible for accounts payable saying, hey, can you send a wire, you know, the $20,000 to this account number, I need it to go out fast.

And that was initially I think the first start of this business email compromise, vendor impersonation type fraud scheme that started going on. Over the last few years obviously it's changed a lot. Initially they were just hitting up large corporations for large dollar amounts. And now unfortunately they're moving on to everybody, so it goes down as far as to small companies, mid-size companies, even retail customers they'll try and get information. Not only are they spoofing emails, which results in (inaudible) more email address. They will actually take over a fraudulent email, send an email. And they do this with vendors and with payroll so they will pretend to be an employee, saying hey, can you change my direct deposit account information. I need it to go to this new account number. And then -- or they do it for vendors. They might know that one of your vendors that you make payments with -- they'll fake an email and say, hey my account information changed, I need the payments going forward to come here. And so you'll make that payment, it'll go out to the vendor that you thought that the vendor's new account information and then two or three weeks later you'll hear from your vendor like, hi, you know, you had a payment due three weeks ago, we haven't gotten it. And then at that point you realize -- point you realize that you probably were hit with fraud.

So fraudsters are getting a lot smarter. They're moving on and they're trying -- you know, as our business changes, their tactics change. So we'll go to the next slide.

Leigh Balcom: If I could just say something, just cut in there real quick. I think fraudsters just realized in the beginning that this business email compromise scam was extremely successful for them and extremely hurtful for customers. So they -- they went on to -- well, if we can hit large customers, let's go look at smaller customers. And they evolved this scam over the years. And I think that you know, you're going to (inaudible) about that, Kristen, so I'll stop and let you go on.

Kristen Karkau: All right.

Frank Lago: Hey, Leigh, before we -- before we move on you actually raise a good -- you raise a good point there and I was actually going to ask you, you know, there's a lot more understanding about the -- there's more compromise, there's more awareness out there. But it continues to increase. So I suppose that suggests the frauds are adapting their approach to continue to do this effectively? Is that what's happening out there now?

Leigh Balcom: Yeah. They're adapting and growing, and expanding because like I said, it's successful amongst larger companies. Not (inaudible) successful against smaller companies and medium-size companies. They -- with -- as software grows and as hacking skills increase, instead of just changing an email address to a -- to a couple letters in an email address, now they can -- through a phishing scam they can get into the back of your computer and actually read your emails and do their -- and study and see how your invoices are and what you send out and who you send them to, and what your name is, and what your clients' names are, and what you had for dinner last night, different (inaudible).

So they study. They're very smart and they've evolved, and they're involved in personal customers as well. So they certainly are adapting.

Frank Lago: Okay. Thanks. Sorry to cut you off, there, Kristen. I'll bring you back on.

Kristen Karkau: Oh, no problem. Thanks. So as trends tend to change, you know, the AFP did mention that 81% of businesses were targets of BEC last year. And unfortunately, we don't always find out. So typically customers only report to the bank if funds are lost. But honestly, it's good if you believe you've been a target, save that email, save the fax, however they've notified you and just contact your bank and let them know. It gives us a better idea of what's going on in the world, helps us possibly develop better tactics internally to help protect businesses. And we have a better idea of what's going on with our customer base and how we're being affected, how you're being affected.

Some of the changes that happened, so money mule bank accounts are now being opened in the name of the company. Used to be they'd post an ad on LinkedIn or somewhere and say, hey, you know, hey retail person, consumer, I need your account information in order to send money to. If it sounds like it's too good of a deal to pass up, usually it is. And in this case, it's being a money mule account.

Now the accounts are getting opened in the same name of the company. Banks used to be able to look at it and say, okay, here's a payment to ABC corporation going into John Smith's account. The names don't match, this could be a potential threat. So it makes it even more difficult for financial institutions and banks to determine if an account could be fraudulent when the same company name as you, (inaudible) transaction and the bank account.

One very popular one that's probably been big for about the last year has been a direct deposit scam. So for payroll, this typically is effective with ECH payments. People, you know, typically you would -- to notify that you need your direct deposit account information, you need to fill out a form, you may have something internally listed on your company's intranet site that you know, employees can submit their information or maybe you're a small company and you can just take an email. Sometimes even a text.

So fraudsters get this information, find out what company you're working for, and say, hey, I need to change my payroll information over to a green dot card, over to a new account information. Payroll comes around, Friday comes around, employee doesn't get their pay. Obviously, this is critical because you need your paycheck to live week to week.

So they've gone through smaller dollar amounts where it used to be just the large companies, large dollar amounts. You'll see small companies, small payrolls. They'll take what they can get. Sometimes a couple weeks go by, somebody hasn't realized they haven't gotten their payroll. All of a sudden, they've missed three checks. The money's gone, you know. We're unfortunately unable to recover it.

Deepfakes are new, and they're an emerging threat. Leigh, can I ask you to speak to deepfakes if you don't mind? I think you can do this one a little bit better than I can.

Leigh Balcom: Sure. Deepfakes, a couple years ago there was a deepfake on -- more than a couple years ago because it was around 2014. But there was a deepfake video of at the time, President Obama. And they also created one for President Trump. And basically what they do is, they use that person's -- an impersonator or they take snippets of speeches from those people and they will put together words that they want. So usually these are used -- unfortunately, they're used in the adult entertainment business, as celebrities and different

things like that. But what we -- what we have seen is a case that happened out of Germany where fraudsters took a deepfake of a CEO's voice and put together a tape, and called the CFO to get a $243,000 payment made. Now, it worked.

Now, what they think happened is this CEO had numerous YouTube videos talking about his business or whatever, and they took those, snipped them together, and created a pretty good conversational snippets that fooled the CFO.

This is emerging. It's -- some of the ones that we have seen at the bank have been very crude. They wouldn't fool anybody. But as the software develops, they're getting better and better at it.

Frank Lago: So Leigh, this is Frank. I'm going to break in here for a minute. This is all very informative obviously. And we're starting to get some pretty good questions. And rather than wait until the end I think a couple of these we could probably answer right now if you don't mind.

We've got a question here, regarding getting into our emails, how do they do this? Leigh, could you give us some ideas on how the fraudsters are faking the email?

Leigh Balcom: Yeah. I'm going to spend a couple slides on this in a little bit, but it's basically, you've heard me mention phishing. It's p-h-i-s-h-i-n-g. There's phishing, there's smishing, there's vishing. And we're going to get into that. But basically, they send out emails, maybe 2 million emails. And if they get a 4% return on those emails that means somebody clicking into it or clicking on a link, what they do is then they put some bad software on your machine, some malware on your computer. And that will allow them to enter the back end and become part of your email system. So now maybe they can get your login and your password for your email.

Then they can read your conversations. They know that -- that Kristen goes by Kristen and not by Kris. That Steve goes by Steven and not Stevie. They've studied, they read these things, they know that you send out invoices in usually in the amount from $30,000 to $75,000. You never send out an invoice for $100,000 because that's not the shape of your business. You very seldom send out an invoice or a payment for $3,000. So they study those things, and then they act.

So they give it -- they -- let's get back to the question, Frank. They've been in 91% of (inaudible) because of a phishing campaign and we'll talk about that in a bit.

Frank Lago: Okay. Thanks. Sorry to steal your thunder there a little bit. I have another one that came in and I'm not sure if you're going to have an answer for this, Leigh, or not. Hopefully you will. But the question is, given the Patriot Act requirements, how are the fraudsters able to get around that to open accounts?

Leigh Balcom: Well, some of the things that we have seen, and when -- we have a pretty sophisticated way that we can detect them. But at the beginning it's challenging. They just create fake state paperwork.

I'm ABC company, and ABC company is in Maryland and they open up -- or maybe they're ABC Co, you know, company-period. But there's actually a real, an ABC

Company in another part of the country that is legitimate. This is a scheme that we've seen, I'll just kind of go into what it was.

They opened up an account under a fake company name, ABC (inaudible). There's a real company called ABC in Michigan somewhere else. They stole checks. But they opened up a company name in the -- with the fake name that's real close to the legitimate one. They stole checks, they washed those checks, they deposited those checks. And then they created more checks.

So they do -- so what happens is they'll deposit those checks and the back-office fraud department or our AML team will catch those, eventually. And you know, and we'll basically shut them down and turn them over to law enforcement. But fraudsters are sophisticated. They're extremely intelligent people and they know banking rules. They know the rules, they know how your company works, so the type of -- or your type of company works. So they're (inaudible) people.

I don't know about the Patriot Act and how they get around those rules, but just by being swift and moving around a lot.

Frank Lago: Well, one thing I think that we're definitely hearing a lot from you, Leigh, and from Kristen, is about how sophisticated and smart these fraudsters are. I do have another question and then I think we need to move on to the presentation, but we're getting great questions from the audience.

This question is, if we have a UPIC account can we give that information to the perpetrator of the initial fraud and try to get funds returned without exposing our actual accounts? It's an interesting question. Kristen, do you want to tackle that one?

Kristen Karkau: Yeah. That's a good question. So for those who don't know, UPIC stands for Universal Payment Indicator Code. So it's basically an account-masking service. And you use a false routing number and -- not false, but I'll say, masking routing number and account number that will hide your actual account number. But it is tied to it. So unfortunately, it's only for credit only, so you would be receiving that money into your accounts.

If there is fraud, I think this is where even if you do have a UPIC, because it's a credit that may be fraudulent, or if -- you know, you know somebody else that this happened to, (inaudible) you can work with them and have them dispute the transaction. Typically because it's a commercial transaction, corporate transaction, there's usually only about a 48-hour return period. So again this is why it's good to -- you know we'll talk more about verifying information and (inaudible) compromised. But that's why it's critical to stay on top of things to verify payments before you send them out.

You can reverse transactions that were sent through a UPIC account, just like you can with a standard ACH payment so that is something that I think we could try to do.

I hope that answered your question.

Frank Lago: Yeah. Thanks, Kristen. And keep the questions coming, folks. Getting a lot of great questions here. We'll try to answer as many as we can.

But let's jump back into the presentation because I think Leigh's got a really interesting slide here on a real scenario.

Leigh Balcom: Yeah. The fraudsters are, like I said, they're involved in (inaudible) companies and smaller companies. Now they're going after individuals as much as they are the other size companies and people. Because again, maybe our security systems aren't -- our home computer system isn't, doesn't have as much security.

So in this case, what happened there is, a fraudster inserted themselves in the middle of a conversation of a real estate transaction. Just a (inaudible) -- empty nesters up in Western New York who were moving to Florida because they were retiring. They were buying a home in Florida. They were on the phone with the title company and got the payment instructions for their final payment on their new house. They called it in. They called back to the title company and verified them. They got the instructions via email, called the title company, verified them.

Then they went into the branch and they made the wire payment. What they didn't tell us was that after they verified the instructions, the fraudster sent another email to their email address changing the payment instructions. So for instance, they said they were going -- maybe the payment was going to -- I'm not picking on any bank, but you know, maybe it was going to M&T, or Chase Bank, and then they decided to divert it and it was going to Citi or PD or another bank.

And they didn't tell the branch that. The branches are pretty sophisticated, and they asked them questions about how you -- how you received the instructions. And if you think about it and don't just answer the question, yes-yes-yes, and breeze through them, they make you think. Because we want to know how the payment -- how the transaction was initiated, how the instructions were initiated.

So anyway, so they moved those funds. They moved a little -- almost $200,000 and that payment went to a fraudster, and the money moved quickly.

Kristen talked before about contacting your bank. Most of the time if a company or one of our clients has been a victim of fraud where they actually sent money, they call us right away. No doubt about it. We want to know both sides. But if we can get involved in the conversation early, we've got a better chance of getting the money back because money moves quickly.

For instance, this money here went to another bank in Florida and then it moved overseas, and we couldn't get any of it back.

If we -- I'm not going to guarantee anything because like I said, money does move quickly. But if we get involved in a conversation same day, next day, there's a lot of times we can call that other bank and say, hey, this transaction was fraud, can we put a fraud hold on it. We'll give them some paperwork that they want, that they require, and we require as well. They'll freeze the transaction. And a lot of times, we can be successful in getting the funds back.

In this case we were not, because the money moved quickly.

And the next slide, this is the direct deposit scam. This is an example of an email. Basically phishing, we've said it before. So the recipient, a regular employee maybe received -- had answered or clicked on a phishing link, and the fraudster found out where they worked just by reading their emails, sent an email to the company's payroll department and says, hey, I'm changing my direct deposit. I'm not going to be with this bank anymore, now I'm going with this bank. That money is diverted, usually into like a Green Dot card or a, you know, an EBT card, employee benefits card, electronic banking card, and the funds are moved quickly.

Smaller dollars, but there's a lot of it going on. About three or four years ago, we used to see one or two of these a year. I see about eight of them a month now.

Frank Lago: Hey, Leigh. This is Frank. And Kristen introduced that previously but that's interesting because it must be extremely high volume to get a large dollar in such small dollar per transaction. So it is, this thing is crushing us in volume in these phony payroll transactions? Is that what's going on?

Leigh Balcom: Exactly. It's quantity over quality. It's a different organized crime ring that is going after smaller dollars, but yeah. That's really what it is. That's realizing that a couple thousand bucks or 500 bucks a few times over is -- you can do the math, is just as good as the 30,000 lighter, $30,000 later. So it's quantity over quality.

Frank Lago: Got it.

Leigh Balcom: So on this -- on this one here, this is where I talk about phishing ad nauseum. Probably would you shut up about phishing, but I've still got a few more slides to get to on it.

What the fraudsters will do is besides reading your emails, they will change filters. So they will go into your email and say, any emails that are sent by the fraudster to the bank or to the CFO, delete them because the fraudster is actually having a conversation with the CFO and they don't want me to be able to go back in and read those emails. They want them gone. So they can get into those filters and change things. They can say, anything that goes to the bank, delete or send it to their own personal email.

So if you are a victim of a phishing campaign or you think something like this happened, you really need to get your computer scanned. Because this was a -- this is a client of ours who was a victim. They did not send money, they caught it. So they weren't -- they didn't lose any money. But their IT team went back in and found some rules that basically said, delete a message if it goes from this email address.

So how did it start? 91% of these cyber attacks started as a phishing email. 91% is a large number. They prey on curiosity, they prey on greed, urgency, fear, you know, act now or you're not going to get this deal. Or you want to see pictures of something, or if you don't do this now something bad is going to happen. They prey on greed, urgency, curiosity, and fear. So if you see those types of emails and you don't know who the sender is, you probably want to just delete that email and send it to your IT department, whatever.

And a successful -- like a successful phishing attempter, they can get your credentials, your passcodes, and put malware on your computer.

I think we've got another poll question.

Frank Lago: Yep, we do, Leigh, so I'll go ahead and introduce this poll question, give folks about 30 seconds to answer. Has your company taken any additional steps to protect fraud since the pandemic hit? You see you've got three choices this time: yes, no, not sure.

And while we're waiting for that, Kristen, let me ask you a quick question. Overall, how would you rate the focus on fraud you see from the large payment organizations like Nacha and The Clearing House? How are they doing with their members?

Kristen Karkau: They're doing pretty good with their members, especially since the pandemic hit. Actually with Nacha, we had biweekly meetings that went through the end of June just to talk about fraud, just to talk about payments, just to talk about, you know, even the PPP and then the stimulus package that went out and payments effective with that. And I know Clearing House was doing that as well.

Nacha's actually created a pandemic page that's posted on their website. Nacha, which is N-a-c-h-a dot org, and from there they'll have links to certain schemes, fraud schemes that are going out. That's always good resource information. They update it as soon as we -- as soon as something comes out, they pretty much update it. So good to check out. Did a follow-on there and we try to post up to here at M&T when we know what's going on.

Frank Lago: Okay. Thanks, Kristen. That's going to be our poll results here.

So we've got -- I think it's the good news here is, the 49.1%, almost half, have taken some additional steps to protect fraud. No, 30%, so maybe you'll learn some idea today and you'll go back and you'll have some things to do. And 20% are not sure, so maybe you can start asking some questions.

In any event I'm going to go ahead and move things right along here. I think, Leigh, you were back up to talk about some hygiene tips. I think this can -- some very helpful information for those on the line today.

Leigh Balcom: These are hygiene tips related to phishing, not your -- not your at-home practices. So you've got to be wary of links or attachments. If you don't know who an email is -- comes from -- look at it warily. Like I say, do I know who this is? Is Microsoft really sending me an email? Call -- you know, call your IT person or if you have a phishing department or an IT person, send it to them. They can take a look at it.

Avoid using the same password across different sites. I'd highly recommend that you know -- we have so many passwords that we have to put in, whether it's for social media sites or news sites or something, banking sites. I would say for your financial transactions, create a totally different type of -- type of email. Let's just say you're in the Baltimore area and your password is GoRavens1 for all your social media. Don't make GoRavens1 or even GoRavens2 your password for your social media -- for your -- for your banking sites. Use something completely different. I'm going to explain why in a minute or two.

Avoid using public Wi-Fi. I use my Wi-Fi at work or my Wi-Fi at home when I'm doing transactions, making sure that I'm actually on the site that I need to do by typing in the MTB.com or whatever -- whether you're -- your retirement account, whatever it is that you use. Type in those as opposed to clicking on a link from an email campaign.

And my marketing department doesn't like when I say this, but yeah. I -- it's easy for me to type in www.mtb.com as opposed to taking a chance of clicking on a link. Probably most of them are good, but that one that's bad is going to create a lot of problems.

And if you do receive a suspicious email that appears to be from us, please send it to our phishing@mtb.com site.

So here, credential re-use. I talked about not using the same passwords that you use for social media sites, for your banking sites. Credential re-use is, fraudsters will have bots, computers, that just plug into a website, whether it's an Amazon website, banking website, any financial type website, and they will take usernames and passwords that they've got from different breaches. So for instance, on the LinkedIn breach, they got usernames and passwords. So what they would do is take my username and my password from the LinkedIn breach and plug it into Chase's online banking, M&T's online banking, and see if they get a hit. If they get that hit, now they can go in and they can change my security questions, or maybe they can create a web bill pay. So they can pay their own credit card out of my account. Or they can set up a whole new vendor, something like that.

So that's what credential re-use is really, taking your own passwords that they've had stolen from a breach and they plug it in at thousands per second, to see if it works.

This is a smishing scheme, an example of a smishing scheme. And I'm not afraid to put M&T up there because I think every bank and credit union has been a victim of something like this. But you've got -- instead of phishing where they send an email, smishing is where they send it to your text, SMS. It's a system that's used to send a text. So in this particular one, you know, they used MT bank as opposed to M&T bank, and I think that they said on here that my account was going to be locked and they needed me to plug in here and put in my username and my password. And then they changed my security questions. And sorry enough, but people did this.

People followed these instructions, and fraudsters got away with a lot of money. So again, be -- I don't think your -- your bank is never going to ask you to log in off of a text that they've sent you, so be wary of those things.

So some cyber security hygiene tips for mobile phones. Install the anti-virus software on your phone if you don't already have it. Apple is a little bit different than other phones. So you really need to, you know, to study Apple or get a Samsung phone. I'm not sure what the best ones are out there for antivirus software, but you know, Apple is a closed source. Other ones can be an open source. I'm not saying here either one is better or not, but you're probably going to find more antivirus software for Android than we would for an iPhone.

Subscribe to your mobile carrier's anti-spam service. If you can utilize two-factor authentication -- so let's just say you're checking your 401(k). If the company offers you

the opportunity where you're going to log in and then they're going to send you a text with a 6- or 8-number code, use it. It protects you a little bit more.

Avoid using public Wi-Fi. You know, I would never check my banking if I'm not -- at the mall in Buffalo. I would never do that. You know, you just -- you want to rely on a Wi-Fi network that you know is secure. Use the auto-lock. If you can use VPN, use VPN. You get tons of calls from people who don't know the number, you know, they may be waiting for you to say hello. And that way when they call in and try to create some sort of a profile of you, they can have you saying, "hello" or "yes" as the company you're -- or think you're talking to on the other end tries to ask you a question, and they get your approval to do something.

So a lot of things there that you can do with that. I'm going to -- we're going to cover more tips towards the end but in some of these (inaudible) we'll be passing out to you at the end.

Go ahead, Frank?

Frank Lago: Yeah. Hey, Leigh, yeah. We're getting a little short on time here, so maybe we could just quickly hit those next couple. I know we are going to share these hygiene tips with the audience afterwards.

Leigh Balcom: Okay.

Frank Lago: But just maybe the highlights and we'll get to some of the solutions.

Leigh Balcom: Sure.

Frank Lago: Towards the end.

Leigh Balcom: Okay. Voice assistants. Hey Siri, that type of a thing. Microphones are there and they can be listening if it's powered on. You can turn it off. There are ways to turn it off, same thing with like an Alexa, Google Assistant, Android phones. They all have settings to turn off your microphones. I highly recommend that you do that, as well.

Now, I don't -- I'm not saying that this type of fraud is running rampant. It certainly isn't. But there is something that a fraudster can do.

Ransomware. Ransomware attacks lately are way up. Ransomware is where a fraudster gets in your computer and locks down all your files, everything. You'll just have a screen that looks like that, and they want you to pay money, where maybe if you pay them, they'll send you back the encryption code to get your information back.

The problem with this is besides the ransom, if you pay it -- and now, law enforcement recommends that you don't because there's no guarantee that you're going to get your money back -- you are going -- you're really going to need to update your computers, you're going to need to update your network. It's going to be very, very costly.

Some things that you can do is backups. Back up your stuff and then take it offline so it's not all connected to the network. Antivirus software. Be vigilant when opening emails.

Change your default credentials. When Microsoft has updates or your IT department says you have updates, get those updates done.

So protecting yourself in a remote environment. I'm just kind of flying along, here. Keep all your network devices updated. Those -- those Microsoft updates and those Apple updates are extremely important. Secure your router and don't give your router an easy password. That's the way that they can get in. Use strong passwords and keep your regular backups.

Securing your business information. I highly recommend that you use corporate-issued devices for work only. Try not to do business on your personal cell phone. Stick with approved third-party services and check them out, make sure that they're secure. Password-protected applications on mixed-use devices and if you're still using paper, shred it and get rid of it. Put it in different places, too.

So, tips, some more tips on protecting yourself. Establish procedures and let your staff know about these issues. Make sure your staff is well -- well-prepared and they know your procedures. Make sure, you know, give them an idea of what some of these threats are. Dual administration, very helpful. Dual administration is if I send a wire, it's over say $10,000, I want to make sure that Kristen reviews that information and back-checks everything that I'm doing to make sure that it's not going to a fraudster. So, a second set of eyes, maybe even a third set of eyes.

Review your transactions regularly. Personally, I check my bank account every single day. I check my credit card statements pretty much once or twice a week, not because I'm rolling in dough. It's just because I want to make sure that there's nothing funky going on in those statements. So if I see something on my bank account that says I paid $149 for mobility insurance -- this actually happened -- that I really did pay for mobility insurance which I did not.

So, two-layer authentication, I talked about that. That's getting the email -- or I'm sorry, getting a text back from your -- your financial company telling you that here's the 8-digit code you want to put in.

And explore cyber insurance. Explore fraud protection products, too. Explore cyber insurance -- is almost a necessity now. Sure, we hate to pay for any type of insurance. But look into it. Talk to your insurance agent, talk to your bank, and see what products are out there and how it can protect you.

Kristen, do you want to take the next few?

Kristen Karkau: Yeah. I'll take the next few, thanks, Leigh.

Other tips. Be aware. Verify emails. If you receive any emails that ask for (inaudible) that has any you know, account number changes, don't respond to the email. Don't call any phone number listed in the email. Reach out using information previously known. Is it for a vendor, is it for payroll? And call that person, call that company, and verify that their information was changed.

For the EC I think changing procedures and making sure you verify that information will

keep it to be (inaudible). You know, keep unique passwords and then for fraud prevention and detection, M&T's got a lot of products that we offer that can help with fraud prevention and protection. We have positive pay, e-positive-pay, ECH monitor, fraud review which we now have for both debits and credits. I mentioned UPIC earlier. So we also have check block and ECH debit block. So again if you -- contact us if you need any help with your services.

I think we go on to one more poll question. Frank, I'll turn that over to you.

Frank Lago: Yeah. Thanks, Kristen. So we're back here for our final poll question, and we'll get to some Q&A. So as a result of what you heard here today, do you believe your company is well-protected against fraud; somewhat protected against fraud but we have work to do; or oh, boy, I better talk to somebody about fraud prevention steps now.

Go ahead if you don't mind and give us a quick answer for the third poll question there. I'm going to give you just a couple of seconds to answer that question because we do want to take some Q&A from the audience. We'll do the best that we can to get through those questions today. I can tell you that so many have queued up, it's very unlikely we're going to get through in five minutes. Maybe the presenters can stay on for a few minutes after, if that works for everyone, so we will try to take care of those as best we can.

And of course, we invite you to contact your treasury management professional at M&T Bank for any questions you have at any time. They're well-trained in fraud protection, have access to experts like Leigh and Kristen who can come -- we can go to for more complex situations.

I'm going to go ahead and look at the results here. I'm very happy to see that nobody feels like they are in such trouble that they better get on their fraud protection now. But I'm not surprised to see that the preponderance of the answers here is that somewhat protected, but that we still have work to do.

So hopefully, we can help you and be able to inform you today. Just going to pass one more slide here. As I mentioned, if you suspect fraud, contact your treasury management consultant or M&T Bank's customer service immediately. I'll leave this slide up for just a second so everyone can take that number down.

Okay. And then we're going to go ahead and go to Q&A while I put my disclosure statement up there for everyone to take a look at. So Leigh, here's a good one. I've actually thought of this earlier and was going to ask you myself. Where do you recommend that I store my passwords? I need them to be secure, yet accessible.

I think there's probably some services out there that allow you to do so. Can you enlighten us a little bit there?

Leigh Balcom: Yeah. There are a lot in the -- in your phone's app store or your tablet's app store. I'm not advocating one or -- I use one called Splash ID. Most of them -- you know, if they're going to be in the App Store, they're most likely vetted out. They're going to be pretty good. So there are -- just go into your App Store, put in password protectors. Like I said, with Splash ID I have a unique passcode that I don't use for anything else, that I use to

get in there and that's how I store my passwords. It basically lets me open up a profile, so I'm going to say, M&T Bank, online banking, my username, my password, and you know, any other information that I need, and I store it. So if I forget it -- because we have so many passwords -- we're likely to (inaudible). But yes. As long as you're getting it from a reputable source, it's probably pretty good.

When I say reputable source, let's just say you're on your tablet and you're playing solitaire and an ad comes up and it tells you about the nice password protector. Don't click on that link. Maybe it's legit, maybe it isn't. But go to your provider's app store and look there. That's probably the best way to do it.

Frank Lago: Thanks. That's a good tip. We appreciate that. So here's a good question that I think gets to something we were talking about earlier, and Leigh, I think this would probably go to you as well. A handful of my staff received an email yesterday, that looked like it came from the president of the company. The email address was not hers, but it showed her name, asking the employee to purchase gift cards and to scan the docs back.

Leigh Balcom: Common (inaudible).

Frank Lago: Yeah. So the employee was able to identify that it was not -- it was not legitimate. But the question is, in this situation, who was hacked? How did that -- how did that fraudster perpetrate that particular fraud?

Leigh Balcom: Well, they just have a list of emails. I mean, it's not -- I mean, the email domain is out there whether it's on LinkedIn or Facebook, depending on what your company is, or emails that have been -- that you've sent to your companies, or your -- I'm sorry, your clients, your vendors, your customers. And those emails, maybe they've been hacked. So you know, it's hard to protect your email domain. It's out there whether you've freely given it or whether they've hacked into somebody else's computer that has your email domain.

So -- you know, and then it's probably -- it's not hard to find individual emails of your employees as well. I don't know if everybody got it. If everybody did, you might want to have your computer checked because maybe they have a way to send it to all. So that means the fraudster could be in the back end of your computer. But you know, emails are out there.

I mean, it's --

Frank Lago: Part of the -- part of the dark web problem I imagine, as well.

Leigh Balcom: Yeah. Exactly.

Frank Lago: Okay. The next question I'm going to direct to Kristen. Kristen, for direct deposit would you say that we should get a hard copy of a voided check or bank letter containing the employee account number rather than have them scan it in email in case somebody could read the emails? Or is it safe if the email's encrypted? Any thoughts on that?

Leigh Balcom: Yeah. I think it'd be okay if your email is encrypted. Best action would probably be to get a voided check or (inaudible) offers a standard bank letter that contains the

information that -- you know, basically when someone opens an account we have a letter that we -- they can fill out and take in and give to their employer.

So I definitely say best would be a voided check or bank letter.

Frank Lago: Thanks. I'm going to take this next question myself. The question was, what can we do to try to prevent any of this from happening to our company? Now, this -- this question came in about a half an hour ago so hopefully you've learned something since then. But I would go back to suggesting that you contact your treasury management professional here at M&T bank and we can walk you through a wide variety of tools and products that can help you protect -- protect your company. So thanks for that question.

Leigh Balcom: I want to quickly jump in there too, Frank. (Inaudible) off the treasury, (inaudible). One thing that you can do is color-code your emails. Have your IT department color-code your emails. That means anything that's internal doesn't come in with a yellow bar, but any email that comes in externally, maybe it has a yellow bar or red bar that says, this is from an external source. That way, you know emails that are coming from the outside.

Now, it doesn't mean that all of them are going to be fraudulent, but it's going to make you pause for a second and say, all right, is this legit. I might have to really take a deeper look at this one. So it's one of the best tips I've learned over the past couple years is that if you -- emails, we all get flooded with emails. So if we can know the difference between an external and an internal, that would probably make it a little bit easier for us to -- to be more diligent.

Frank Lago: Thanks, Leigh. Hey, we're just about out of time here. In fact, I think we're one minute over. I think I'm going to ask one more question and then I will just let everyone know that there will be a full list of questions available after the event. And we'll try to get answers out to as many of those as we possibly -- we will keep track of all these for you.

But Leigh, this one I thought was interesting. How often are spam email unsubscribe links malware?

Leigh Balcom: Can you say that again?

Frank Lago: How often are unsubscribe links, linked to malware? In other words, should we use that link to unsubscribe to an email that you don't want, or should we just ignore it?

Leigh Balcom: I don't know the answer to how often, I don't know any statistics on that. But I will say this. If it's something that you legitimately subscribed to, and now you don't want it anymore, it's probably going to be okay to click the unsubscribe. But I get them Kohl's all the time, the department store. I have nothing against Kohl's. But I get -- I never signed up for Kohl's ads or statements or anything like that. So I suspect that that might be fraudulent. And if I do click unsubscribe, I might be -- I think what I'm telling the fraudster is that yes, this is a legitimate email, which means that they can try other phishing types of campaigns.

So if you did actually subscribe at some point in time, and you don't want it anymore, it's probably legit. But if it's something you just have no recollection then I would just keep on deleting them or I don't know how, but you can block a -- you can block a user from

sending emails to you.

Frank Lago: Okay. Well, some folks are starting to log off, but we still have quiet a few that are on the line. So I think I'll just stay on for a couple of minutes and ask a couple more questions. Kristen, here's one for you. When customers pay us via ACH, what should we send them, and is sending it by email okay? I'm assuming that this is referring to an acknowledgement of some sort. So do you have an answer for that one?

Kristen Karkau: Yeah, I do. So if you want to send via ACH, obviously you need to give the customer your banking number and your ACH number. Send it via email if you can encrypt it. I know a lot of companies that have a standard form and (inaudible) on. A lot of times, this is where I think customers (inaudible) UPIC service so you can email -- you know, you sign up for the UPIC service, you're not actually giving out your own account information. You're giving out a masked account information.

So I would send that out. And I think if you encrypt the email you should be fine. (inaudible) they get (inaudible) instructions to (inaudible) a previous known contact number just to verify. But I think sending email encrypted is pretty standard.

Frank Lago: Thank you. I think that is a prudent step to take. As you mentioned, I think that's probably the best thing that we can do with the emails.

Actually it looks like we've got just a -- a few more here. Since it's almost 5 after, I think why don't we go ahead and wrap it up now. So I appreciate everybody's time. I appreciate everyone staying on for a few more. Great questions from the audience, I appreciate that.

So I think I will turn it back over to our operator Jessica at this point in time to wrap things up.

Operator: Great. Well, thank you so much, Frank, and thank you again to all of our speakers today. This does conclude our webinar, Fraud and Cyber Threats to Business in a Remote Environment. We do welcome your feedback on today's webinar with a survey that will pop open on your browser window momentarily. Again, thanks, everybody, for joining us. This concludes the webinar and have a great rest of your day.