Commercial Insights with Regions Bank
Episode 2: Safeguarding Your Business from Financial Fraud

Fraudulent attempts on businesses have been on the rise — and steadily evolving — since COVID began. But even as the topics change, fraud typically still comes in tried-and-true forms that have worked for years, from business email compromise to impersonation. On this episode of Commercial Insights with Regions Bank, we explore how the pandemic has escalated fraud, and how well-prepared businesses can spot the warning signs to stay ahead of criminals with shifting targets.

Episode Transcript

Chris Blose:
What are the conditions that create an environment ripe for fraud? Jeff Taylor, SVP of Commercial Fraud Forensics and Payment Strategy for Regions Bank, has seen enough examples throughout his career to have an answer.

Jeff Taylor:

The bad guys, the fraudsters, thrive on chaos. They love it. And so anytime when confusion, fear and greed are present, then that's what they thrive on.

Chris:

Welcome to Commercial Insights with Regions Bank. I'm your host, Chris Blose, and today we're sorting through a little of that chaos Taylor describes to make sense of it for the future.

Pandemic conditions certainly resulted in a rise in instances of fraud—everything from early PPE scams to increasingly elaborate email ruses. But Taylor makes an important note: The topics and tactics of the day might've been new but tried-and-true types of fraud remain the same.

The good news? This means a well-prepared business that knows the warning signs of fraud can stay ahead of criminals, even as criminals shift their targets.

Chris:

Let's start with some context. Why do events such as the pandemic that we've all been experiencing in the last year create the conditions that lead to more fraud?

Jeff:

Well, I think, Chris, there are certainly more people working remotely. They're working from home. They're working from locations outside of their office. They're using unprotected networks or personal email to conduct business that they might normally use the company resources for. And, and just the overall environment makes them more vulnerable because of distractions of other situations that are occurring within that home environment that would not be occurring if they were in an office environment.

Chris:

And what types of fraud are actually increasing during this time?

Jeff:

Well, business email compromise is still number one. You know, it used to be where you had the impersonation of a company executive. But now they have progressed into more intrusive and, quite frankly, more difficult to detect forms, such as the impersonation of an employee or a vendor.

Jeff:

Secondly is ransomware. Ransomware incidents have increased 715% in 2020. In many cases that ransomware is delivered through malware or malicious code where employees are distracted, not paying close enough attention, and click on a link in an email or a website that downloads that code into their machine. And that information's based on a mid-year threat landscape report by a company called BitDefender.

Jeff:

Thirdly is the internal and employee fraud, and the way that increases during economic difficulties where you have more people that are struggling to make ends meet, then that makes them more susceptible to, to perpetrating fraud themselves, or actually even becoming the victim.

Chris:

What types of systems or employees have been most vulnerable in the past, in normal circumstances?

Jeff:

Well, certainly no one is immune. We typically see employees who are involved in accounting, or accounts payable, or payroll. Those tend to be the most vulnerable because of their ability to impact a payment or a transfer of funds. And, of course, that same report that I mentioned earlier indicated that 40% of all COVID-related emails were actually fraudulent. And 55% of overall emails are reported as being spam. So email is obviously the most popular channel. And,

of course, whenever there is a lack of internal controls, that opens the door for business email compromise to be successful.

Chris:

Well, I'm curious, too, how can a business safeguard against that sort of impersonation, you know, or in general for those vulnerable systems or employees, particularly when conditions are so different?

Jeff:

Right. Well, the first thing you have to do is guard your house. The companies need to set up extensive firewall systems to safeguard their networks and, and ensure that they have built a perimeter around those networks to keep the criminals from being able to access their systems.

Jeff:

Secondly, if you can do this, just to be able to prohibit the use of email for changes in payment terms, or the origination of a payment. And if that's not possible, then you wanna verify all of those payments and changes in terms by calling a number known to you and putting in some process of dual control.

Jeff:

Thirdly, I would say conduct employee training and, and create an education campaign for employees, so that you're helping them to understand more about the red flags, things to look for in an email, or ways to help protect themselves. And I'd even suggest testing employees on phishing campaigns and with phishing exercises to just determine how well your education campaign is working, but also to help employees to understand what to look for.

Jeff:

Uh, and then finally, developing and implementing a risk governance plan. Understanding that you need to have some sort of plan in place of how I'm gonna react if and when this occurs.

Chris:

I'm curious, with the the idea of training employees to spot fraud or to spot phishing, for example. Let's just use that as an example. What are some of the elements that you might tell someone to look out for? I mean, I think we all think of ourselves as smart and savvy, but people obviously do get caught in this.

Jeff:

Well, it's just so easy, really. When we go back and look at the emails that are coming from a criminal that are a part of these business email compromise schemes, depending on the font that's being used in the email address itself, think about how easy it is to not recognize a one as opposed to a lowercase L. Or a potentially even other types of, of domain impersonations where

the name on the email domain looks very similar. So maybe an S is left off the company name. Those kind of things are very difficult to pick up on. What we would encourage clients to do is review those email addresses, and if it looks suspicious, then certainly report it or verify the change before it's made.

Chris:

I think a lot of that comes down to the distraction you mentioned earlier, too, right?

Jeff:

That's right.

Chris:

I think people are trying to capitalize on (laughs) someone not being able to make that distinction between a one or a lowercase L because they're pulled in a million different directions.

Jeff:

That's right.

Chris:
I know a lot of these phishing email scams in particular, they're, they're preying on human impulses. Can you tell me a little bit about how that works and why that is so effective?

Jeff:

Sure. In the past when you had the executive impersonation—so a CEO or CFO supposedly sent an email that says, "Hey, we're buying a company in China, but you need to keep this completely confidential. But I need for you to wire 1.5 million to this routing and transit number at a bank in China because it's a down payment on this company that we're purchasing." And so because we've asked to keep it confidential, we don't share that with anyone. And because we want to be helpful to the CEO, we're gonna try to react quickly and move that money as quickly as possible. And the bad guys are counting on that. They're counting on us to want to be helpful. And they're counting on us to act quickly in those kind of scenarios without really going through the process and being as diligent as we should be.

Chris:

So you also mentioned creating a solid fraud and risk governance plan. I have to assume that companies out there are thinking about this now perhaps more than ever. What are the sort of elements, foundational elements of a fraud and risk governance plan?

Jeff:

Well, I think it's just like your business continuity plan. You have to know who's in charge, number one. Who is going to react and what areas are they responsible for? As you think about in a ransomware event, as an example, it's very possible that your entire email system could be compromised also, or, unavailable to you. So you've gotta know how do I get in touch with these key individuals that are part of this team?

Jeff:

I think secondly, to understand what your risk tolerance may be. You've gotta determine, am I going to validate every possible scenario or every situation, or am I okay with, with a certain level of, of exposure?

Chris:

I think we get into looking at resources when we're talking about this as well. And I know a lot of businesses are looking very closely at their budgets, for instance, right now. So how would you advise a company on, you know, where to begin with this and how they should be thinking about budgeting appropriately for fraud resources?

Jeff:

Well, you've gotta take this seriously, and you've gotta dedicate the right resources and the proper resources to this kind of protection. That one loss is going to far outweigh the amount of money and the amount of resources that you would dedicate to helping guard your house and putting the plans in place to protect your company. You just can't cut expenses there.

Chris:

How much more important do you think thinking about technology to prevent fraud is going to be in the new world, where clearly even post-pandemic more people are going to be working from home or having flexible hours?

Jeff:

I think that you're gonna see more artificial intelligence recognizing situations. Most email platforms have a way to put an alert banner at the top of the email that says, "This is coming from an external source. Take caution before opening any kind of attachment." Those kinda things that just remind you to take a little bit more care.

Jeff:

But I think you're gonna see a lot of things that are gonna happen within the industry where, more companies are going to put in place ways to try to filter email, maybe even controls that limit the use of personal email, installing a VPN, a virtual private network to connect to company

resources. You know, all those things that may not exist today depending on the size of the company, but I gotta believe they're investigating those now if they don't have it already.

Chris:

I think if you're a business decision maker, something that's emerging from everything you're saying is, a lot of this fraud is not new. It is ramped up because of conditions of the pandemic. But it's not new. It's something you should have been paying attention to before, as well. So, you know, what is the lesson for that leader and that decision maker-as we look forward to the remainder of 2021?

Jeff:

The lesson to me would be don't let your guard down, particularly as we begin to return to normal because the bad guys are going to change their approach, they're going to pivot based on what the environment looks like. So you've gotta stay abreast of what I call the fraud du jour or the fraud of the day to understand what are the new compromised vectors.

Jeff:

In most cases, these guys are going to use the tried and true techniques that have been successful for them in the past.

Chris:

So I think the ultimate message is be vigilant, stay vigilant, and watch for the things that have always worked.

Jeff:

Exactly.

Chris:

Well, thank you so much for your time today. It's great to get your perspective on this.

Jeff:

Well, thank you, Chris. I appreciate the opportunity and, I think you just can't overemphasize the importance-and the education around the risk.

Chris:

Here's what we've learned: The perpetrators of fraud thrive on chaos. And their techniques rarely change—just their targets and topics of opportunity. So stay sharp, analyse your companies risk management plans and overall technology structure, and be ready for what comes next, from minor disruptions to landscape-altering shifts.

Thank you to Jeff Taylor for joining us today, and to all our Commercial Insights listeners. Get related resources for commercial business and listen to future episodes at regions.com/commercialpodcast and be sure to subscribe on your favorite podcast platform.

The information presented in this podcast is general in nature and should not be considered, legal, accounting or tax advice. Visit regions.com/STOPFRAUD or speak with your banker for further information on how you can help prevent fraud.

Regions Bank, Member FDIC, Equal Housing Lender. The information presented is general in nature and should not be considered, legal, accounting or tax advice. Regions reminds its customers that they should be vigilant about fraud and security and that they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices, as the threat evolves daily. There is no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit regions.com/STOPFRAUD, or speak with your Banker for further information on how you can help prevent fraud.