TABLE OF EXPERTS

Protecting Against Fraud

Many businesses aren't aware of their vulnerabilities when it comes to check fraud and wire transfers

GETTY IMAGES/KENNY YOO

MEET THE EXPERTS:

LYNEEN FISCHER
Vice President of Security
North Shore Bank

Lyneen has been with North Shore Bank for 43 years, now leading efforts to protect businesses and consumers from fraud and scams. She's passionate about helping people stay safe and informed, and stays active in groups like WAFI, IAFCI, and FAST TEAMS to stay ahead of emerging threats.

JASON NAVARRO
Vice President, Specialty Lines
R&R Insurance

Jason Navarro, Vice President Specialty Lines for R&R Insurance has been in the insurance industry since 2000 holding multiple underwriting roles with several National Insurance Carriers. He joined R&R Insurance in 2015 as a commercial sales executive and in 2018 he created the Cyber Insurance Division specializing in helping customer implement stand-alone cyber insurance programs with Cyber Risk management Strategies. Since that time, R&R Cyber has helped over 1400 customers implement specific cyber insurance programs to protect their organizations from the devastating effects of cyber-attacks.

JOHN REICHERT
Shareholder
Reinhart Boerner Van Deuren

John Reichert is a shareholder in Reinhart's Banking and Finance Practice where he provides counsel to banks, bank holding companies, and other financial services companies on matters including navigating and mitigating fraud, governance, capital formation, M&A, asset sales and purchases, regulatory/compliance matters, commercial lending transactions and general securities.

MODERATOR:

KURT BAUER
President and CEO
Wisconsin Manufacturers and Commerce

Kurt R. Bauer became the fifth head of Wisconsin Manufacturers & Commerce (WMC) in 2011. Founded in 1911, WMC is the combined Wisconsin State Chamber of Commerce, Wisconsin Manufacturers' Association and the Wisconsin Safety Council. WMC represents 3,800 employers of all sizes and from every sector of the economy, and is referred to as "the state's most powerful business and manufacturing group" by the Milwaukee Journal Sentinel.

Prior to joining WMC, Bauer spent 18 years working for financial industry trade groups, including serving as CEO for both the Wisconsin and Arizona Bankers Associations.

Federal and state laws provide a fair degree of fraud protection for consumers – but that protection does not extend to businesses. Financial institutions will work with businesses to provide protection, but ultimately, businesses will bear any financial loss. The Business Journal of Milwaukee recently brought together a panel of experts to explain the differences between business and consumer protections, the areas where businesses are most vulnerable and what they can do to protect themselves from losses.

KENNY YOO

The Fraud Factor panel event was sponsored by North Shore Bank, R&R Insurance, and Reinhart Boerner Van Deuren.

KURT BAUER: Let's start our discussion with a level-set. Lyneen, what types of fraud are companies seeing today?

LYNEEN FISCHER: It's all over the board, but right now, check fraud is big. You would think check fraud would be declining because the number of checks that clear has dropped from 20 million 10 years ago to 12 million today, according to the FDIC. But the value of those checks has increased from an average of $1,500 per check to $2,700 per check. Who writes those larger checks? Small businesses. In addition to check fraud, we are seeing deep fakes and business email compromises that are costing businesses money. If you have not experienced fraud as a small business yet, you probably will because there are so many emerging ways to do it.

BAUER: At WMC, we have noticed that insurance rates have actually come down a little bit, but incidents have gone up. Jason, what are you seeing?

JASON NAVARRO: I think frequency has increased tremendously over the last five years. COVID was a gold mine for cyber criminals because people were working remotely and had a lot of other things on their mind. Criminals used that to their advantage. Insurance rates have come down a little bit because carriers are requiring businesses and individuals to implement a lot more protocols up front.

BAUER: Are there specific sectors of the economy being targeted?

NAVARRO: It's across the board, and for each sector the approach is different. For manufacturers, the criminals' mindset is to shut down your machines because that is your pressure point. If I shut down your source of income, you're generally going to do what I want. For financial institutions and health care, criminals are after customer information.

JOHN REICHERT: Criminals do tend to look at mid-size targets – what I call the "Goldilocks Space." If you're a large public company, you're going to have resources to defend against attacks. If you are very small, it's probably not worth it for the criminal. There's a mid tier where you're big enough to be attractive, but you're not big enough to deploy all the defenses large companies can.

BAUER: Let's talk about the difference between consumer and business protections.

FISCHER: There are consumer protection laws that specifically protect consumers. If you experience fraud, you may get your money back within a certain amount of time. But the rules are different for businesses. Tell us about that, John.

REICHERT: Most people who have experienced consumer fraud think that because the bank reimbursed me, my mom or my aunt, my business will get the same deal. That's not the case. The law treats consumers differently from everyone else. Without getting too far into the weeds, banks have a duty under the law to deploy commercially reasonable security procedures, so they'll offer you tools and tips and products. If you use those, fraud will be very rare. But the fact is that many business don't use the tools. They don't use positive pay or dual control because they think their bank will take care of things. Banks have insurance to cover fraud, but it covers the bank, not you.

NAVARRO: And if you have insurance, it may not be enough. Let's say you are covered for wire transfers up to $250,000. What if you transfer $500,000? You are potentially uninsured every time you do that. You should review your insurance coverages with your agent at least once a year to make sure they are up to date.

REICHERT: You also need to do what your agent recommends and then determine who in your shop is going to be responsible for doing it. Fraud insurance can be voided if the business doesn't do what they were required to do.

BAUER: What are some of the more concerning tactics out there?

FISCHER: Texts and emails are getting more sophisticated. You used to be able to identify fake emails because of grammar or spelling errors. But now the texts and emails are spot on. And with AI, you've got to be careful about voices.

BAUER: AI only needs 10 seconds of you talking to be able to not only mimic your voice, but also your cadence and the way you speak.

FISCHER: It's pretty scary. You can have dual control for fraud protection, but that doesn't protect you from faked messages. We recommend setting up internal passcodes. If someone gets a request to wire, they should ask for that passcode.

REICHERT: There are two types of fraud. There is fraud where you didn't authorize a transaction. Someone impersonated you, originating a transfer without your approval. That's one set of rules and laws we follow. The other type of fraud is where you authorized

the transaction, but you were duped into doing it. Because it was authorized, we're dealing with a different set of rules.

NAVARRO: More than 90 percent of the fraud claims we have are due to social engineering, which is me as a bad guy tricking you into doing something. Give me five minutes and I can go out and find a lot of information on most people. I just need one piece of information to trick you into opening up that email or giving me what I want. We should be able to eliminate almost all of those incidents because it is controllable if you follow best practices.

BAUER: Lyneen, what is the most common approach you see customers falling for?

FISCHER: It is check fraud because many businesses are still using checks as their preferred method of payment. U.S. postal inspectors are trying to make sure mail isn't stolen, but it is still a huge problem. There is a heightened opportunity because of this summer's flooding. Payments are going to contractors and others a consumer or business may not typically write checks to. There also certain times of year when check fraud does increase – tax time and so on. If you still need to write checks, make sure you talk to your bank about positive pay with pay match, because that check for $60,000 originally made payable to the IRS could end up being a $60,000 check to Joe Smith.

NAVARRO: For us it's a little bit different. It's not necessarily the checks, it's the payment of fraudulent invoices. It's transfers of money. It's duping someone in that social engineering setting to get them to move money.

REICHERT: We see the whole spectrum – wires, checks and duped vendor payments. And it goes in cycles. We'll have a week when 10 checks are washed, and then we'll have a month with three bad wires.

BAUER: What are some of the most effective tools out there?

FISCHER: Besides positive pay for checks, there's ACH, there's check reconciliation through ACH. Those are great tools. Make sure you use some sort of tokens. Tokenization is key, because many people use the same passwords across channels.

> "You want to make sure you have a product that is designed for your business. There are three main ways you can be attacked and you need coverage for each."
>
> **JASON NAVARRO**
> R&R Insurance

BAUER: There is LifeLock, Aura and other online tools that protect consumers. Is there something like that at the business level?

NAVARRO: There are some different tools your service provider or IT team can and should be providing. It's going to cost some money. If you have an insurance product with your cyber insurance policy, the carriers are going to be scanning and monitoring you on a real-time basis.

REICHERT: Back when you received bank statements, you had 30 days to review them. Today, you should be logging into your online banking and reconciling on a daily basis. Banks will often help each other if there's a wire that's sent or bad funds being held at another bank, but time is of the essence.

BAUER: Jason, what are some of the insurance coverages that everybody needs to be aware of?

NAVARRO: You want to make sure you have a product that is designed for your business. There are three main ways you can be attacked and you need coverage for each. I can break into your business, steal your information and hold it for

GETTY IMAGES

Fraud Protection TOOLS

Account & Payment Protection – (monthly charge)

- **Positive Pay**
  Matches checks presented for payment against issue check files (detects altered or counterfeit checks).
- **ACH Positive Pay / ACH Filter**
  Controls which ACH transactions are allowed, helping block unauthorized debits.
- **Payee Match**
  Ensures the payee name on the check matches the company's issued file.
- **Debit Block / ACH Block**
  Prevents unauthorized electronic withdrawals from specific accounts.

Authentication and Access Controls – (minimal cost)

- **Dual control / dual authorization**
  Requires two people to approve high-dollar or sensitive transactions.
- **Role-based access in digital banking**
  Employees only see or act on what's relevant to their role.
- **Multi-factor authentication (MFA)**
  A second layer of login security.

Monitoring and Alerts – (often, but not always free)

- **Real-time account alerts**
  Text/email notifications for account activity, balance changes, or large transactions.
- **Fraud detection monitoring**
  Bank systems flag unusual account or transaction activity.

Secure Payment Options

- **Electronic bill pay and ACH payments**
  Reduces check use which is a common target for fraud.
- **Virtual cards**
  Generate single-use card numbers for vendor payments, limiting exposure.

KENNY YOO
Wisconsin Manufacturers & Commerce CEO Kurt Bauer moderated the discussion.

ransom. That's a breach and it's going to cost you money to repair and remediate. You will have to hire lawyers and PR firms. The insurance policy provides the money to hire those people and will also pay for loss of income during your downtime. That's part one. In that same data breach, your customer information can be exposed. Those customers have the legal ability to come after you. That's a liability situation, and there is coverage to protect you from lawsuits and penalties. The third part is what we're talking about today. It's that crime section that protects you against fraud. You need to make sure you understand your coverage and whether it is appropriate for your business.

FISCHER: There is so much going on right now. You think you have business online for protection, but there's layered security within business online products. You can have non signers on your business online, including a tax accountant who can monitor and reconcile your account. These things can come at a cost, but it's better to protect yourself up front than dealing with a $60,000 fraudulent check.

BAUER: What do you do if you discover fraud? How do you try and get the money back?

REICHERT: You break the glass: You call your lawyer, bank and your insurance. If we all work together, we can sometimes get that money back.

NAVARRO: When we've been able to recover money it has been through an EFT or ACH. With wires it seems like it's pretty much done instantaneously. Best practice is to question whether you have to wire the money or are there other options, like ACH, that provide more opportunity to recover funds.

BAUER: So this is all a little overwhelming. Let's say we are starting a business or we just acquired a business. What are some best practices for making sure you are protected from fraud?

REICHERT: I would go to the bank, tell them what you're about, figure out the tools the bank has that can help you, and then make sure you're deploying them correctly. Review your accounts frequently, implement dual control and work with your insurance carrier to make sure that you have the appropriate coverages and you are doing what those coverages require. If you do that, it's going to be pretty hard for you to lose money.

NAVARRO: Train and practice for a fraud event much like you do for an active shooter or a harassment situation. It is a known threat that can expose, even end, your business. Have your employees train and prepare for it, from the lowest individual on the totem pole to the owner of the company. They're all an exposure point, so they all need to be made aware of their roles and responsibilities when an

KENNY YOO
The Fraud Factor panel gave the audience key takeaways to safeguard against financial fraudulence.

incident occurs.

FISCHER: It's important to know what tools are available and to use the tools you have.

REICHERT: Kurt, you mentioned acquiring a business. We have been preaching for years that if you are buying a business, part of your due diligence should be around their fraud and cyber protections. Do they have the right controls in place? Do they have the right insurance in place? Is there legacy fraud that you might be inheriting? These are important questions.

BAUER: What's the craziest experience that you've had that you're allowed to share?

FISCHER: There are so many to share. There was a recent one where a customer truly believed she was sending money, both wires and cashiers' checks, to herself and to other people to protect herself from the bank. This went on for three weeks before she finally realized that the people who were calling her were bad actors and not from the FBI. That can happen to a business owner, too, where the bad actors pose as your bankers or law enforcement. Don't fall for that. Call the banker you know and talk to them.

REICHERT: There was a family-owned business that had trusts. One of their trusted deputies who had single control fell for a scam and started moving money around. It probably took six months to unwind because you had some consumer, some business, and the money went to a dozen different banks.

NAVARRO: The one that drives me insane was somebody in our organization who sat through my presentations and then got an email supposedly from our boss to buy gift cards. Somebody who is in our industry can still fall for it, right? But it shows we're human and you can have a bad day and make a mistake.

BAUER: How does AI help and hinder fraud?

FISCHER: On the banking side, AI can help detect certain check frauds more quickly. I also see AI helping to identify unusual IP addresses. But AI will also help the bad actors stay one step ahead of us. As a company, you need to protect yourselves through education and reading as much as you can about these things.

NAVARRO: AI has helped to give us tools for real-time monitoring. We can use those to find the bad guys before they strike. On the flip side, AI absolutely scares the life out of me from a loss standpoint.

BAUER: I've got elderly parents, and they've already had a phone call from somebody who was claiming to be their grandkid who needed money because he got arrested in Mexico. They knew it wasn't him because they didn't recognize the voice, but that will change. AI is able to spoof not only your voice, but your mannerisms and the way you speak. My family has a password. So if someone calls up and it doesn't sound right, you can ask for the password.

BAUER: What question should I have asked you that you'd like to answer?

NAVARRO: I think the biggest piece of advice that I would give people is that you have to prepare for this threat. You have to have a game plan that says this is what we're going to do and this is how we're going to do it.

REICHERT: My takeaway is that a lot of people assume their bank is going to reimburse their company if they experience fraud. That's not the case. You need to work with your bank on the front end to put in protections. If you wait until you've been defrauded, they are not going to be as helpful.

FISCHER: Talk to your bankers. We're here to help. We don't want you to lose money. Time is money too. It takes time to recover these funds, if we can, and that impacts both you as a customer and the bank. So save that money and time up front by using the tools available.