ADVERTISING SUPPLEMENT TO THE KANSAS CITY BUSINESS JOURNAL

FRAUD & RISK

HOW TO PROTECT CUSTOMERS & PROFITS

A BUSINESS JOURNAL ROUNDTABLE

MODERATOR

PANELISTS

RYAN WEBER

President, KCnext

Ryan currently serves as President of KCnext – The Technology Council of Greater Kansas City. Additionally, Ryan serves on the board of the Technology Councils of North America (TECNA), and is a member of the executive mentorship program for the College of Business at Kansas State University. Ryan further demonstrates the value he places on staying involved in the community by supporting several other organizations in the region and is a 2015 graduate of the Centurions leadership program.

AMY GROTHAUS

Vice President, Retail Branches, Community America Credit Union

With 18 years of experience in the financial services industry, Amy Grothaus is an influential leader at Community America Credit Union as the Vice President of nearly 30 retail branches. Amy is active in the local business community as a past board member of the Northland Regional Chamber of Commerce and plays a vital role in expanding the Credit Union's footprint and launching a new series of technology-focused branches across the Kansas City metropolitan area. As a young mother passionate about member service and teaching financial responsibility, Amy serves as a Community America "Savin' Maven" sharing ongoing tips about smart money management with Kansas Citians.

PHIL POJE

CEO, TechOrchard

A serial entrepreneur Phil has more than 30 years of executive leadership and ownership with four companies in the area of technology and financial services. His experience encompasses executive management, strategic planning, business process management, marketing and sales management. Phil primary focus is providing leadership and overall strategic direction for TechOrchard. TechOrchard is a Mobile IT Solutions company that assists organizations in securing mobile devices (smartphones, tablets, & laptops) and leveraging the productivity of mobility in business, government, education and healthcare. Phil is a native to Kansas City, and holds a degree in Technology and a BA in Business from University of Missouri-Kansas City.

SHAUNA WOODY-COUSSENS

Managing Director, BKD Forensics & Valuation Services

Shauna is a managing director in BKD's Forensics & Valuation Services division. She has more than 20 years of experience performing forensics accounting, dispute analysis and consulting services in the fraud, abuse, complex commercial litigation, class action, merger, acquisition and valuation areas. Shauna's forensic investigative experience includes fraud investigations for internally identified company matters in response to inquiries by third parties and regulatory bodies as well as litigation in various industries. Services include funds tracing as well as forensics accounting and financial analysis. She has experience with Foreign Corrupt Practices Act (FCPA)/Anti-Bribery & Corruption investigations and is BKD's subject matter expert.

ADVERTISING SUPPLEMENT TO THE KANSAS CITY BUSINESS JOURNAL

FRAUD & RISK

Corruption, billing schemes, check tampering, card skimming — theft takes many forms in today's business world, and they all cost you time, money and even your reputation. Recently, the Kansas City Business Journal gathered area fraud and risk experts to discuss how business owners can prevent joining the ever-growing list of companies coping with data breaches.

Unfortunately, our experts agree that it is not a matter of "if" your company will suffer a data breach or technology-related theft. It's a matter of "when." Ryan Weber, president of KCnext, moderated the discussion to provide area business owners guidance about how to protect themselves and their customers.

THINKSTOCK

Weber: What are the biggest emerging risks you are seeing in the financial services and banking industries?

Amy Grothaus, CommunityAmerica Credit Union: The biggest risk right now is card skimming — when people illegally collect data from the magnetic strip of a credit card — at ATMs and gas stations.

But even data breaches at big companies, like Target and Home Depot, affect financial institutions and their customers and members. Financial institutions absorb a lot of the costs from those breaches. Everybody is affected — the retailer, the consumer and the financial institution.

Weber: We've been hearing a lot of about mobile payments and the ability to pay by phone. That seems to be an emerging opportunity and maybe a risk, too.

Phil Poje, TechOrchard: Nearly every technological iteration brings convenience to our lives. However, every time technology iterates, the bad guys iterate their ways to steal from others. Mobile technology is one of those areas that continues to be a challenge. Whether it's in your pocket or on your wrist, it is transferring data, and bad guys are finding ways to get to it.

Weber: What are other red flags or problem areas business owners should watch for?

Shauna Woody-Coussens, BKD: In the banking industry, ACH, wireless and electronic funds transfers have been around a long time. But the way fraud is being perpetrated in this area is changing. The red flags we're seeing for this type of fraud are the age-old red flags. The financial institutions have appropriate internal controls, but their employees and clients aren't following them.

Weber: Why do you think that is?

Woody-Coussens: A lot of people think, "This can't happen to me, this can't happen to my institution, and this can't happen to my company." So they just get comfortable, and they don't stay on top of the actual risk that this represents to their organization. And that's why I think ongoing training of both your employees as well as your clients is crucial, particularly in the banking

ADVERTISING SUPPLEMENT TO THE KANSAS CITY BUSINESS JOURNAL

FRAUD & RISK

area.

Grothaus: It's also important for the frontline staff and members (customers) to understand how to communicate carefully. Never assume email is secure and going into a branch or calling has a higher rate of security success and member-service.

Woody-Coussens: Some of the controls are the old-fashioned controls. In that example, the staff person should call the customer back to verify the request.

Weber: The most popular stories about fraud seem to usually start at the top. The leadership's devices get compromised or something similar. It sounds like it could be a cultural thing. Have you seen best practices where the top leadership leads by example?

Poje: In the mobile space, a lot of those best practices and policies are not put into place. And employees lack training. Employees need to know what to do when a phone is lost, for example. We use phones without thinking much about them. And yet there are so many different places and ways that people can hack into them and get information.

Even today, half of the people in the United States don't have a pass code on their phone.. Now, think about that, and think about what's on your phone. My guess is that none of us here would give our phone to a stranger for 24 hours.

We're seeing the same thing — a lack of policy and procedure across the board. And the size of the organization doesn't make any difference. You would think the larger ones would be better prepared, but they're not.

Woody-Coussens: I think the culture with regard for data has to start at the top because our employees are like our children: They listen to what we say but they do what they see us do.

Weber: If you had a magic wand, what three things would you mandate?

Poje: In the mobile space, I would have businesses set up policy and procedures first. I would then enroll all of those devices into an enterprise mobility management solution. It gives you a single pane of glass where you can manage multiple operating systems and devices, personal and corporate-issued.

Training would be the final piece for us. Training people on how to use these devices responsibly and the steps you take if yours is one of the 7,000 to 9,000 devices that is going to get lost today.

QUICK FACTS

DATA BREACHES

A partial list of companies that have suffered data breaches:

- Primera Blue Cross
- Anthem
- Sony Pictures
- Staples
- Home Depot
- JPMorgan Chase
- Michaels
- EBay
- Target

Woody-Coussens: At BKD, we've got 2,700 employees throughout the country. We have a chief information officer, and we have formalized written policies and procedures. I have mandatory security training come to my computer on a very frequent basis, and I must change my password every 90 days, or I can't get in.

Changing that password is so ultimately important. In many of our investigations in which data has been involved or computer forensics, we have found that the password is sitting on somebody's desktop in a little file that says "passwords" or on a sticky note on the underside of the keyboard. Or the password is just "password."

Weber: The organization needs to have a policy, but really the individual is a component in all of this. Is there a trend to increase individual responsibility for security in consumer-facing organizations?

Grothaus: It's always been there. In the financial services industry, we encourage customers to check their account statements. The sooner you catch it and inform your financial institution, the more likely you are to mitigate the damage.

Weber: Do we do a good job explaining why diligence is important?

Poje: No. The average consumer isn't paying attention to all of this. They don't think it's going to happen to them. Data is really the most important piece of an organization — not the building that they are in and certainly not the furniture. It's the data and the customers, and with this new technology, people are finding new and creative ways to exploit all of that.

Weber: How can companies proactively monitor fraud?

Woody-Coussens: They can do a number of different things. One of the areas I specialize in is occupational fraud — fraud that is perpetrated against an employer by its employees. We use the data the company already routinely collects to help us investigate fraud or to look for it proactively.

With fictitious vendor fraud, for example, an employee sets up a company that doesn't exist and then bills the employer. It is very easy to data mine proactively. You can pull up your employee master file and vendor master list in Microsoft Office Excel, sort, and look for duplicate addresses, phone numbers and tax identification numbers, You'd be shocked at how many times the fraudsters don't bother to use something other than their own information .

So data is a risk with regard to fraud. But it is also a huge way to help combat it. Use what you've got. Look for anomalies and unusual patterns.

Weber: What other steps can companies take to monitor mobile fraud?

Poje: Having a mobile strategy as part of your overall strategy is a good first step. The security piece is key. You've got to think where the holes are. We have to change the way people think of mobile devices. We think of them as more of a convenience item. And they can be so much more than that both on the good side and the bad side.

Grothaus: With the recent slew of card-skimming events, we've put devices on all of our ATMs that shut down the machines when fraud is detected. And we have done extra training for our staff. Education and training are very important.

Poje: One of the biggest challenges we have is convincing our prospects and clients to do this training piece. We go back to training people on how to use the mobile device. We train them how to use it more fully and how to use it securely. So not only does their knowledge expand and their ability to get their work done with a mobile device increase, but their security level and awareness of what's going on around them goes up. And yet, most organizations want to scratch that line out on the cost on implementing a good

CONTINUED ON PAGE 4

ADVERTISING SUPPLEMENT TO THE KANSAS CITY BUSINESS JOURNAL

FRAUD & RISK

THINKSTOCK

CONTINUED FROM PAGE 3

mobile strategy.

Weber: If you had to pick one control, what would it be?

Poje: Our No. 1 priority is always securing the device. You have to make sure that's done and happens 24/7. You can set up alerts to know when a device is being compromised.

Woody-Coussens: Training is a very good control. Another one is creating a fraud/ethics hotline, if the organization doesn't already have one. The training educates the employee so they can be your eyes and ears to all sorts of fraud or ethical issues. The hotline gives them a very convenient way to let you know the minute they suspect something is wrong. The company can then more quickly investigate, which limits both the duration and the financial loss of fraud.

Grothaus: I'd say training.

Weber: It seems like fear drives a lot of this topic of risk or fraud. Many companies are either afraid to announce that something has happened, or they'll review it, analyze it and process it internally many months before sharing that information with the public. What should businesses do about sharing information, both internally and externally?

Grothaus: For us, as soon as we find out something has happened — either a skim or an attempt, we contact the members who have been targeted. We also inform our employees. We don't hide what has happened from the member, but we don't alert the media, either.

Woody-Coussens: With any type of fraud, the reputational risk goes well beyond any dollar amount that you lose. You can't really quantify the loss of customers, the people who will no longer do business with you or the contracts you don't get in the future. So the way we talk to our clients about this is we would really prefer everyone take a more proactive approach to it. Put these things in place, and use them as a marketing tool to tell people: "We know fraud is out there and any company — any company of any size in any industry — is at risk. We cannot do away with it. We're trying to do something about it. If it happens to us, this is what we are going to do." Let people know it's on your radar, and if it happens, you're more likely to find it sooner and take care of it quicker with less disruption to everyone.

Poje: During the past 12 months, more companies are asking their vendors to give them verification and evidence that they have security policies in place all the way down to the endpoint — all the way down to the mobile device. Several clients recently have come to us to meet conditions and deadlines they signed in contracts with a large organization.

Companies are realizing that everyone they work with may have access to sensitive information and they're exposed. On the whole, we're behind the curve, but we're starting to see some real movement in this area.

Grothaus: We have very tight controls for any vendor relationship, especially when we're adding new technology that supports the frontline staff.

Weber: We read that many of these attacks are coming from a foreign source. Obviously this is a complex issue. But how can companies and people protect themselves internationally?

Woody-Coussens: This is often dealt with in contracts. It is common for companies to require in the contract that foreign or third-party vendors have procedures in place.

Grothaus: Contact your financial institution if you are going to travel abroad so they can put a flag on your account. Again, look at your accounts and statements every single day. Be diligent.

Poje: We make sure there are policies in place for employees who travel with mobile devices. We help companies manage and change what's on the device depending on where employees are traveling. Laws and countries vary. So being able to manage devices according to specific laws is also critical.

Woody-Coussens: Don't reply to emails from foreign sources.

Grothaus: That's a good point. Those still do happen. If it's too good to be true, it is. You can always go to your financial institution to ask them. I know our staff has warned lots of customers about existing scams.

Poje: Often, we see older people being preyed on. I got a phone call yesterday from my son, and his friend was just taken for about $2,500. So here's a young person who grew up in technology taken by a scam. So it's happening to everyone.

One thing I would tell organizations is to think and plan for this: It's not going away. It's going to continue to iterate. Bad guys have always been bad guys. And this is going to continue to happen, unfortunately. Be ready.