Sonal Bullard:

Hello and welcome. I'm Sonal Bullard, executive vice president and head of strategy for the Wealth Management Group at Regions Bank. We're very happy that you could join us today for this Regions Bank webinar on fraud and cybercrime, a problem that affects all of us. It's not just businesses that are being targeted, but individuals and families as well, as we've all shifted so much of our financial lives online and our social lives, too. Criminals have followed us and they're constantly finding and inventing new ways to try to part us from our money. And because of technology, scammers are now able to target far more people than they used to much more easily and in far more sophisticated ways. At Regions Bank we deploy the latest tools and technology to help you. There's a lot that we as individuals can do to protect ourselves and our families, and that's what we're going to talk about today.

We're going to hear from three Regions specialists who have years in this field, and they'll share ideas and insights about what we should watch out for and how we can protect ourselves and those that we love. We'll talk about four of the most common types of fraud, imposter scams, romance scams, investment scams – where losses hit almost $5 billion last year – and charity scams. Our panel today includes Diane Greifzu, Anna Peterson, and Matt Powell. Thank you all for being here. Could you all take a minute and introduce yourselves and tell us a little bit about your background?

Diane Greifzu:

Thank you, Sonal. Diane Greifzu, wealth management, risk control, private wealth liaison, working with the Private Wealth Group in all areas of risk.

Sonal Bullard:

Thank you.

Anna Peterson:

I'm Anna Peterson. I am the non-financial risk manager in the Wealth Management Risk Control Group, and I have a focus on private wealth fraud.

Sonal Bullard:

Excellent, and Matt.

Matt Powell:

Matt Powell, I'm the head of financial crimes, which includes enterprise fraud management.

Sonal Bullard:

Excellent. So glad to have you all here with us today. I want to start with a general question about fraud prevention. What's our role as individuals to prevent fraud? Let's start with you, Matt.

Matt Powell:

Sure. So at Regions, like most financial institutions, fraud's a top priority and that includes investments both in or in people, process and technology. But there has been quite a fundamental shift that we've seen as customers and consumers have wanted to become much more engaged in protecting their own finances. And so we've moved from, we talked a lot about protecting our customers and that's really moved to protecting with our customers. And so we've given tools and you talked about some of the technology investments, but things like online alerts, et cetera, and giving access to people's accounts so they stay up to speed much more on their financials. And so that's been really important for us. The downside is that the fraudsters have picked up on that, and that they've really focused on scam type activity. Understanding that to circumvent a lot of the fraud controls that we've put in place by going and actually looking at scamming customers as opposed to necessarily attacking the bank specifically. So because of that, having very well engaged customers that are educated is hugely important. And with scam activity being really one of the top vectors that has grown over the last few years, making sure that we're having these types of discussions really timely as well as making sure that we have very well-educated customers.

Sonal Bullard:

Excellent. Diane?

Diane Greifzu:

And I think adding to that is historically we thought the elderly were usually targets for scams, but the fraudsters, and scams, actually are impacting all. There's no discrimination against any type of group at this point. It's not just the elderly, it's everyone. We rely on our technology for our social lives, for our financial lives, and the scams and fraudsters are focused on that technology and

how to get things out of us, how to act quickly. And that technology gives them that ability.

Anna Peterson:

And I think it's obvious that the scammers want money, but they also want that personal information and that helps them to steal more money. And we're seeing in many of these scamming incidents that they're using multiple tactics to scam individual targets.

Sonal Bullard:

Wow. Well, it's extremely important context that I think is relevant for all types of the fraud we're going to be discussing today. Let's begin with talking about imposter scams. So the FTC says that this is the most common type of scam and is also known that the median loss has jumped up to almost $7,000 on average. So this is a good place to begin. Matt, imposter's a pretty broad term that applies to many situations, so maybe we can start with some definitions. What types of fraud do you think we're covering with this particular term?

Matt Powell:

Yeah, so we probably should start with what makes up a good scam and it's involving trust and it's also creating a sense of urgency. And so that's a lot of the reason why fraudsters lean in on imposters because there are certain functions like banking as well as your medical insurance, government agencies where there's already built-in trust associated with that as well as urgency. So if your bank's calling you and saying somebody just wired $5,000 out, that automatically creates that sense of urgency. So it's really their ability to already have trust that's built into the relationship as well as can create that immediate sense of urgency. So we certainly see it with banks and specifically within fraud departments within banks, we see it with government agencies such as the IRS as well as local police as well. But we've seen it with insurance companies, investments, et cetera. And that's really the imposter, what they're going after. And again for areas that already consumers and customers have trust built in.

Sonal Bullard:

Well, Anna, have you found that imposter scams depend on scammers really possessing or accessing sensitive, personally identifiable information? And we

call that PII, or do the scammers really start by harvesting publicly available information that they might find available externally to target?

Anna Peterson:

Yes, that's a great question and point. So typically they will go for that publicly identifiable personal information. So that could be maybe a social media profile that you have. It could be your professional profile; it could be real estate documents that are online. It could be a 'meet the team' page that's on a business website that identifies you. And what they will do is take this public information and combine it with the information that you have told them to gain your trust.

Diane Greifzu:

And then they take that information, they continue to build it on it, so it's "hi Anna," and you're like, oh, they know my name, they must know who I am. And then they'll ask, "can you verify your identity by giving me your pin?" And then all of a sudden, Anna, you give me your pin and now I have an additional piece of information. And so they'll continue to build on that information and gather for a long-term use as well. They can use that into tricking you in a way to have you give them a payment. So not only may they gather some money right then and there, but now they have your credit card information, and they can go and do other things as well quickly. So they use that public information to then harvest a little bit more information from you to do something else with it and build upon it.

Anna Peterson:

And I think to Diane's point, when they reach out to you and they know your first name, you automatically think this is someone who has engaged with you in the past and you have that automatic sense of trust.

Sonal Bullard:

Yeah, someone you might know.

Anna Peterson:

Exactly.

Sonal Bullard:

Well, so should alarm bells sound whenever you receive notice that you need to take steps to protect your assets from scammers. How can we really tell the difference between legitimate communications from say, Regions or scammers who are trying to engage our emotions and prompt us to act before really thinking things through? Matt, let's start with you.

Matt Powell:

Sure. So the short answer is yes, there should be alarm bells. Some of what we used to see is potentially misspellings or grammar errors in emails, those types of things. I will say with generative AI and some of the tools that have come out that certainly fraudsters have used that which has eliminated a lot of that, which just continues to go about more sophistication with these scams, which is challenging because it does get very hard to split between what's coming from Regions and what's not. I think what's important is really looking at the full interaction. So it's not just about that immediate, somebody called me, they said they're from Regions and they said all the things that you would expect them to say, but it's then what's next? And are they asking me for credentials or why would they be asking me this? Or they're asking me to make a payment to send myself a refund. Those kind of things. Those are the alarm bells that we should really be thinking about that if it just doesn't feel right, it's likely not.

Diane Greifzu:

So the number of data breaches, so your personal information is up 78% and or 350 million people have experienced a breach of their information. So this information is out there, they've been able to gather it, and that's where these data breaches occur. They then use that information to build on it and build on it, and they want to create that level of trust. Oh, they know this information, they know me, this is legitimate. But there's always typically that sense of urgency that's occurring. And so we always say, stop. Slow down. Does this sound right? Look for those spelling errors. Look for something that just doesn't feel right. And typically there isn't anything urgent. There's a cause maybe to stop, think about it, is this right? Contact someone, say, "Hey, I got this message, is this correct?" Because they have most of our information out there already and they're going to use it to their benefit.

Sonal Bullard:

Yeah. Well, of course not all scams have to do with someone trying to impersonate your information and act as if they're from a legitimate source. Our

next topic actually covers a different type of scam that has two terms associated with it. They tend to overlap each other. So I want to talk a little bit about what these are, and they're romance scams and investment scams. So Anna, I actually want to begin with you. Can you tell us a little bit more about what each of these mean?

Anna Peterson:

Yes, absolutely. So I think typically in the past, people associated romance scams targeting the elderly, which really that's not the case anymore. Any demographic can be a target of a romance scam. And what we're seeing is that people will typically meet someone on a dating app or on a dating website, and they end up building a relationship with this person and this person is targeting them typically to get money from them. So what we'll see is they will meet the person online, they have the person who they've met will say to them, let's talk off of the platform. So they will want to exchange phone numbers or exchange email addresses. And once they get them off of the platform, then they will declare true love for that person even though they've never met in person. And they will say that they're not able to meet them in person because they work overseas or perhaps they're in the military and they continue to build trust and build this relationship. And then they start asking for money. So it could be money to offer to buy them a plane ticket to come and visit the person that they're targeting, or maybe they have a sudden need because they have an emergency surgery that they need money for or something urgent that will target that person. And now that they've built the relationship with them, they feel that they will give them the money and that they're obligated to engage in this behavior. For the investment scams, typically what we call those, they're known as pig butchering scams.

Sonal Bullard:

Wow.

Anna Peterson:

Yes. And while that is an unpleasant name, it is derived from the comparison to fattening up a pig before slaughter. So in these instances, the scammers will try to build trust with their victim or their target and get them to invest in cryptocurrency exchanges. Sometimes they will do a short return letting the

victim think this is actually a great deal, and then that will then encourage that person to invest more money. And we're seeing cases where victims are losing thousands and even millions of dollars.

Sonal Bullard:

So a real differentiator here between the imposter scams is that the sense of urgency is missing, but the fraudsters are going to rely on that emotional connection to get to the individual.

Anna Peterson:

Absolutely.

Sonal Bullard:

So Diane, what are some of those psychological triggers that scammers use to foster and encourage people to act and to trust them in these types of scams?

Diane Greifzu:

And that's, Sonal, what they're looking for, they're looking for that trust. They build it however they can. They're digging into that conversation of connecting to you to build that trust. They want to know your interest, and all of a sudden, they have that same interest, and they build that trust so that you are, wow, I can't believe how much we're connected. And they get them to just feeling that this is it, this is a great relationship and I'm trusting this person. And with the investment scams, they're coming across them as the expert. They build that trust. And then they're also going to expand on that and talk about how they're an expert in that area and build even having illustrations and returns. And as Anna's mentioned, even giving them a profit out of something already and saying, look here, give me more. I can do more with that. And again, they build and build on that trust and continue to gather. And that's where this type of scam is hard. It's hard for people to realize how much trust they've put into somebody and to realize, and usually by then they're so engrossed in this and trusting them, and that's where the imposters come across. They get that trust, and they've got them.

Anna Peterson:

And sometimes the romance scam can then lead to a cryptocurrency or investment scam, but sometimes those scams are also independent of the romance scam.

Sonal Bullard:

So these types of scams sound exactly like the types of scams in which Regions works to provide education to their customers. I think awareness is key. It's so important to be aware, to be educated and then be confident. Anna, can you help us recap some of those warning signs that a communication might be the beginning of an investment or a romance scam?

Anna Peterson:

Sure. So I think what you want to be wary about is meeting someone online by accident. A lot of these scams start with the message that comes to you that is unsolicited. Another thing you want to look for is this person who claims to be your true love. Have you actually met them in person? And then what is the sense of urgency when they're asking you to send money? So they will ask you to wire your money to them. It may come in the form of them asking you to purchase gift cards or some kind of a money transfer app to send them money. And again, it's focusing on that sense of urgency. And then when you're meeting someone online, they may then start to talk about cryptocurrency investments and trying to get you involved in investing with them. And what we want to be careful of there is not ever investing more money than we are actually willing to lose. So that's something to really keep in mind.

Matt Powell:

And I think what's interesting about some of the ways they want you to give them money, it's interesting because a lot of it is, there's anonymity to it, so it's very hard to trace, it's immediate. So they're looking for how do I get the money so that I can get the money somewhere else? So those should also be red flags associated with does this sound right? And why would I be paying somebody in a gift card that doesn't feel right. I think with cryptocurrency scams, it becomes that ability to move money and turn it into something else very quickly. That's very powerful for the fraudsters.

Anna Peterson:

Yeah, absolutely.

Diane Greifzu:

And then as well, just being aware that it may start with a small amount. So they may very well say, here, I'll invest this a hundred dollars and then actually give you a profit off of it. And so you think, okay, this is legitimate, now I'm going to

send 'em more. And then boom, they've got you right there. That was the intent. They wanted to show that you made a little bit of a profit, but then they're going to turn around for the bigger dollars and that's what their goal was to do.

Anna Peterson:

Absolutely. It's all about getting that trust and getting you to trust them, and then that's when they continue with their scamming attack.

Sonal Bullard:

Yeah, it's good warning signs. Thank you. So let's move on then to the next area. I want to say that our next topic really plays on the good nature of people and their generosity and interest in helping others. And these are charity scams, like some of the other scams that we've discussed. These are not new, but with the proliferation of digital platforms, charities are increasingly using online outreach to connect with potential donors. It's efficient, honestly, Matt, has that led to a corresponding rise in charity scams?

Matt Powell:

It certainly has. And this is a really unfortunate conversation because the fraudsters will really go after things that are happening real time. And again, it's about creating that urgency and just the good nature of folks. And it also goes back a little bit to trust. So you're going to see things that look like they're coming from legitimate charities that are slightly different or there's something about it that's different. And so no good deed goes unpunished because they have tried to make it easier because it's about getting funds to the people who need 'em quickly, which is great intentions. But again, the fraudsters use those same scenarios to exploit it. So, a lot of the things that we've been talking about for red flags and things that you should protect yourself about or with are the exact same. So, take that pause, do verify. There are a lot of good sites out there to go out and verify whether something is legit or not. And so, take that time. But we certainly don't want to discourage people from giving to very useful charities. But at the same time, this is a space that fraudsters have certainly looked to exploit because of that urgency and because of how easy it is now to move money.

Sonal Bullard:

So, like the imposter scams, it seems like that sense of urgency we often feel when we hear about natural disasters or conflicts around the world is ripe for

exploitation by these scammers. Diane, do you encourage people to be especially careful about how and which organizations they give to and maybe responding to requests to support a recent catastrophic event?

Diane Greifzu:

Absolutely. I always say as the people in that natural disaster area, if they're preparing for it, scammers are preparing at the same time just in a different way, and they utilize a lot of the same footage and things like that to capture. So you can have a legitimate charity with the footage and it's the same footage being used by an imposter. So, it's so important to verify the information. Where are you sending that money to checking those email addresses, checking the content, are there spelling errors? Are there something, is there something off in that? And it's just being vigilant in making sure typically there's no emergency in getting the money to a charity that's going to help out. So again, it's that urgency that the fraudsters want to impress upon you to do something now, but if you were to wait a day, you're still going to have the same impact for that organization and helping those that are in need. So again, pause, make sure it's right, and they're using this information and they, it's mass, they're gathering it quickly. Just take that time, extra time to make sure it is legitimate.

Anna Peterson:

And I think even with that, even though we are looking at contributing to a legitimate resource, we want to just always make sure we are protecting our personal information. That has to be at the forefront.

Sonal Bullard:

That's right. That's right. I can imagine that you all have seen scams that are very grab and go, the fraudster set up a quick link for donations and then they pull in the dollars that they can and then they take the link down. But can playing on the philanthropic impulses be a tactic for other types of financial fraud or identity fraud?

Diane Greifzu:

Absolutely. I mean, anytime there's that sense of urgency, people will do anything. It doesn't make sense. But again, if they can do it in that urgent matter, you'd be surprised what information they can gather. And so, they may not be looking for your $50, but they're looking for that additional information that you now just gave them with that $50. So it's that building of information.

Sonal Bullard:

So this type of fraud I imagine isn't going to go away. People want to make a difference and help others. Matt, can you provide our listeners with practical guidelines that can help them make sure that their charitable donations are going to the organizations and causes that they want to support in a safe way?

Matt Powell:

There is the verification if you're wanting to send something, and like I said, there's lots of different ways to validate that beforehand. Be careful that donate now button seems very easy to push, but in a lot of cases that's what they're doing and they're collecting other information to the points that Diane was making. So really be careful about that. Also, be careful about your digital hygiene with that too, because that's certainly ways that they exploit that with your phone, your laptops, et cetera. So it's really important. And then I think lastly is take a minute deep breath and really verify, and if it doesn't feel right, then go through and make sure to do that incremental step to ensure that the intent of what you're trying to do to give to charities is actually going to happen. Yeah,

Sonal Bullard:

That's a lot of great hands-on advice. Thank you. We want all of our listeners today to have confidence and feel educated about what's going on out in the world, and we want them to know that they should identify those with whom they trust. And take a pause for a minute, Anna and Diane, are there any other final thoughts that you would like to share that can help everyone increase their awareness of potential fraud scams that are out there and how they can protect their own family and friends?

Diane Greifzu:

I mean, just reiterate, slow down. If you feel stressed, you feel it's not right. Go with your gut, slow down, reach out to somebody, ask someone else. Does this seem right? Does this feel right? Don't fall for that sense of urgency. Check for those goofy spelling errors that may be out there. They're a leading indicator that there's something not right here, but talk with others and then trust others. If they say maybe you should look into that further, take their advice. Slow down, take that extra step to make sure that your money is for a charity going to the good cause that you want it to go to and not going to a fraudster.

Anna Peterson:

And I think we need to realize no one is immune from this. The fraudsters are targeting everyone, including savvy individuals. So you really want to stop and think. I think the fraudsters are also looking at people to say, this can't happen to me while it can happen to you. And so we want to make sure, like we've heard here today, we have to be vigilant really stopping and pausing and thinking before we act.

Matt Powell:

I think it's important. We've talked a lot about digital money movement, and I think I'd be remiss if we didn't talk about that is when done correctly, that's one of the safest ways to transact. And so we don't want to discourage the use of that. I think we're wanting to say, make sure you're doing it for the right reasons. The digital payment rails are much safer than things like writing checks or in some cases other more traditional types of money movement. So I think it's really good advice to be cautious and really understand, but not to shy away because it really is one of the most secure ways to move money.

Sonal Bullard:

Yeah, that's excellent. That's terrific advice that can help us all stay ahead of fraud in our day-to-day lives. We want you all to feel educated and confident about handling your financials every day. Don't ever forget that you can reach out to a trusted advisor and get their opinions as well to help you out. And I want to extend a collective thank you to our panelists and a special thanks to everyone who's joined us today for this webinar. We hope that you feel better prepared to spot fraud before it happens and keep your communications online and otherwise safe. We encourage you to visit Regions', help and support where you can read through our fraud prevention and security frequently asked questions. And you can also read through the articles that explain Regions security features and what you can do to better protect your personal and account information. And you can always stop by a Regions branch to speak to a Regions advisor or banker and make an appointment by phone or via Regions.com. Thank you all for joining today.