So Money Podcast Transcript

Farnoosh:

This podcast is brought to you by Chase.

Don't let scams steal your holiday spirit. Help protect your money and shop with confidence this season.

Welcome back to So Money everyone. I'm Farnoosh, and guess what? News flash: the holidays, they're here upon us, and they're expensive enough without someone trying to steal our money.

But while we're shopping for gifts, booking travel, tracking packages, and donating to causes that we care about, scammers are working overtime, and they're getting more sophisticated. I'm talking fake delivery notifications, fraudulent shopping websites, phony charities, and travel deals that seem too-good-to-be-true.

Here's the thing, scams can happen to anyone, even people who consider themselves financially savvy or pretty good with technology. We are all vulnerable. So, today we're going to learn how to be proactive and get ahead of the scammers' games.

Joining me is Diedra Porché. She's the National Head of Community and Business Development at JPMorganChase, where she leads a nationwide network of community managers helping individuals, families, and businesses build financial confidence and resilience.

This November, Chase is marking Chase Fraud and Scam Prevention Month, an initiative focused on helping consumers identify scams and take simple, practical steps to help protect themselves during the holiday season. Chase is also hosting free fraud and scam prevention workshops across all lower 48 states and Washington, D.C. to empower consumers with practical tools to help protect their money and personal information.

Now coming up, Diedra and I are going to discuss the most common holiday scams, the red flags to watch out for, simple habits that can make a big difference, and what to do immediately if you think you've been scammed or your account has been compromised.

This is a thing to remember, fraudsters want us to act fast, so our best defense is to slow down, verify, and think twice before clicking or sending money.

Diedra Porché, welcome to So Money.

Diedra:

Thank you. So glad to be with you all today.

Farnoosh:

We're so grateful to have you because this is go-time. I know we are spend, spend, spending right now, and as I said earlier in my intro, we're doing it quickly.

A lot of us are procrastinating our shopping, and so it's much easier for us to miss the warning signs of scams. But first, let's talk about why this time of year, this holiday season even in particular, that scams are on the rise.

Diedra:

Well, I love the holidays. I mean, who doesn't, right?

Farnoosh:

Right.

Diedra:

But we're so busy. When you think about that we're spending time with family, we're doing a lot of shopping, we're traveling and spending time with family as well, and so it's busy. When you think about how you're moving when you're busy, you're not slowing down and paying attention, and scammers know that.

So, it's not even really so much that scams are up. It's really that there's more of an opportunity for scammers to take advantage of people who are busy, who are focused on the spirit of the holiday, and maybe not paying attention that they may be a victim of a scam.

Farnoosh:

Or multitasking. Raise your hand if you've shopped online on your phone while your food is cooking…

Diedra:

100%.

Farnoosh:

…and your kids are talking to you…

Diedra:

That's right.

Farnoosh:

I will be honest, there are days where I get packages and I'm like, "When did that happen?" "When did I hit buy on that? Okay, let's see what the surprise is going to be."

Diedra:

100%.

Farnoosh:

Why are the scams so effective, though? Even for people who consider themselves to be financially savvy, technologically savvy?

Diedra:

Well, first, let's just keep in mind, scams can happen to anyone. It's not really about how savvy you are. Scams don't necessarily target certain categories of people. It's really about catching people when they're in a rush and when they're not aware, and taking advantage of the fact that they're busy.

So, it's really important to slow down pay attention and focus on the matter at hand so that you don't become a victim.

Farnoosh:

Yeah, and really, this message is for everyone in your family. You're listening, but you need to share this with your friends, with your parents. Listen to it with your kids, because now one of my kids has a phone.

The holiday season, though, it seems like the scams are of a certain, like, flavor. What are the scams during the holiday season that are maybe more present that we really need to be watching out for?

Diedra:

Well, again, it goes back to, what are we doing during the holidays? So, we're shopping a lot more. I shop online a ton.

I don't know about you, but most of my purchases now are online. So, when you think about that, online shopping scams are one of the biggest scams that we see. So, this is where a scammer will post maybe a fake website, or maybe they will dupe a website that you're familiar with, seeking to get you to click on a link or to send personal information.

Another scam we see a lot of is travel scams. So, this is where the bad actor will post a fake website with fake deals, with really deeply discounted rental properties, and there's no rental property behind that. They're trying to get you to send money up front. Those are signs that this might not be legitimate.

So once again, it's important to slow down, make sure you're going to the official site, make sure that you are maybe even hovering over the URL to make sure that it is a legitimate URL. But the idea is to slow down and make sure you're dealing with the official source of the information and doing your homework.

You may be visiting an area that you've never been to before, so doing your homework to make sure that it's legitimate before you send money or before you click on a link is really important.

Farnoosh:

Yeah. Speaking of, I think a lot of times we are led to websites because we clicked on a link or an ad, or we were searching online and we clicked on a link that led us to a website. I would always say go type in the website yourself in the browser.

What are some other telltale signs that the site is a dupe?

Diedra:

Well, when you look at the URL, the URL should be constructed as a proper URL. Oftentimes you'll see that it's a personal site as opposed to the official dot com site.

There's one other holiday scam I want to make sure that I mention: missed package delivery. We see many scams during the holidays that you missed a package or you missed a delivery. We're all waiting on packages, we do so much shopping online, and it's the holiday season, so you may in fact be waiting on a package.

What the scammers will do is send you a text message or an email that claims that you missed a package, and they want you to reschedule your delivery, or they want you to send some personal information. The point there is don't click on the link or message. Once again, go to the official website or go to the app and look up the delivery information with data that you have obtained on your own rather than clicking on the link that may have been sent to you in a text message or an email. We really see a lot of missed package delivery scams during the holidays.

Farnoosh:

That I did not know about, and I'll be on the lookout for that.

What are the common red flags that consumers should look for when evaluating whether a message, or an offer, or request is legitimate?

Diedra:

One of the biggest red flags is a false sense of urgency. Scammers and bad actors want you to act quickly. They may suggest that you will miss out on a deal, or that you'll lose access to your information.

Slow down. That's the most important thing to do. And always seek to verify the information on the official website. That's a great way to make sure that you're protecting yourself.

Another big red flag is deals that seem a little too-good-to-be-true. Oftentimes, they're offering deep discounts on popular merchandise. That's a red flag that something just might not be right.

In worst case scenario, stop by your local Chase branch or your local bank and ask. They're more than willing to help you verify if something isn't quite right.

Farnoosh:

Yeah, and I want to give everyone permission to listen to their instincts, you know?

To your point, when you're running around doing 20 things at once and working fast, the voice in your head gets quiet. You may not even realize something is off until you actually give yourself the time and space to get quiet and learn that maybe this is not legit.

Diedra:

That's so true. Take 10 minutes. What's 10 minutes in the grand scheme of things to make sure that you feel good about what is happening in that moment and listen to yourself.

There is so much information available to help protect yourself and to protect your family members. Chase.com/security is a site that we have that offers so much information and so many tips on how to help protect yourself.

Farnoosh:

Yeah. I know this is about holiday shopping, but I feel like around tax season, this is also another high season for fraud and scamming. If the IRS is texting me, that's a red flag. That is not how they communicate officially. You know, so we'll do more of that in April, but, I just want say, if anyone's asking you demanding money via text, that's just wrong. That person can wait, I feel like.

Diedra:

100%. No legitimate entity is going to demand that you send personal information or that you send money.

That is a big red flag that something is not quite right. The scammers and bad actors have gotten really sophisticated with their fraud attempts, particularly in the age of AI.

So, we are seeing deepfakes. We're seeing where scammers are cloning your voice. They're using technology to make it appear to be really legitimate. So, how can you tell the fake from the real? Again, the point is to just slow down.

Some of the things that you can pick up on are a mismatch with the voice versus the language that's being spoken, so there's a slowdown in the video. It's not linked up. You also may see odd, unnatural facial expressions. There are things that would make you pause. If at the end of the day, it causes you to go to the official site and make sure that it's legitimate, then that's just the best course of action.

Then for phone calls, set up a family password. Again, with deepfake and voice cloning, it may appear to be legitimate. But if you set up a family password, you can always ask that family member, because once again, they try to create a sense of urgency. They may even make you believe that your family member is somewhere unsafe. That can cause a lot of fear. So, setting up a family password is a great way to just immediately verify if things are legitimate.

Farnoosh:

That's a great tip. What I do sometimes is I show something to my tween, my 12-year-old going on 13. He's a digital native, right? These younger kids, they can spot what's AI versus what's real better than my parents, right? I would say I get a B+ in this area, A-, but my son has the instinct.

I haven't done a survey, but I feel like younger people who have grown up with the internet can sniff this stuff out better perhaps. I don't know. But I always show it to a friend or show it to a family member. I feel like getting a second opinion is always a good idea, too.

Show a friend. Phone a friend, right? "Does this look legit to you?"

Diedra:

100%. By the way, my daughter is always telling me, "Oh, Mom." I'm a real sucker for the puppy ads online. So, when I see a really cute puppy Instagram, she's like, "Mom, that's AI."

But I'm getting better. So, to your point, sometimes those who are digitally native can pick that out, but I agree 100%. Ask a friend, phone a friend, ask someone you trust: “What do you think?”

Farnoosh:

I loved your tip about coming up with a password with your family. Are there other sorts of practical ways that we can prevent this and implement this in our day-to-day lives?

Diedra:

Yeah. So using a credible source to verify if this is legit or not. Make sure that you change your passwords frequently. It's really important that you're constantly updating your passwords so that information isn’t common.

Then monitor your accounts consistently for identity theft. One great example we have is Chase Credit Journey®, where you can monitor your identity. It's actually free to use, even if you're not a Chase customer, and it's a great way to be conscious of anything that may be happening on your account.

You can also set up transaction alerts. I love transaction alerts because you can set it up for $5 or $50, but it makes you aware if there are transactions taking place on your account, and many banks have that feature. You can also do that on your Chase app.

Farnoosh:

As you're speaking, this is encouraging me to shop more in stores, to actually leave my house and go buy something in real life.

You know, obviously, it's not possible to do that with everything, but I think it's also a great reminder to support small businesses during the holidays.

Diedra:

100%. Shopping with retailers that you know and trust, to your point, is a great way to lift up local businesses and give them your support. But recognizing that even if you have to shop online, making sure you're dealing with a legitimate source.

One of the other scams that's really prevalent during the holidays is gift card scams. Part of the reason is that gift cards are such a popular form of gift. It's very accessible for bad actors and scammers. Once again, go to the official site. I know I've said that 10 times, but making sure you're dealing with the official retailer and that you're going to their site or their app.

Farnoosh:

Can you illustrate the gift card scam for us a little bit, actually bring it to life? How does it work?

Diedra:

So, gift card scams work with the bad actor advertising a gift card at a really steep discount on social media or on a marketplace. Typically, this will be a fake website or a duped website where they're advertising a gift card at a really steep discount.

They want you to click on the link in the social media marketplace where they advertise, and either get you to send money or get you to provide personal information for social engineering purposes. Again, it's a bad actor. If you see a gift card that you want to purchase, go to the official site of that retailer or go inside to a local brick-and-mortar retailer and purchase it. It's the best way to make sure you're dealing with a legitimate gift card.

Farnoosh:

Yeah, great reminder. I know everybody wants those gift cards. It's always like the number one gift people want. I get it.

Diedra:

I think people choose gift cards because they want people to have the flexibility to purchase, and gift cards are easy to send and mail to those that you care about. But there are ways to help protect yourself and make sure you're staying safe.

Farnoosh:

So, so much on prevention we've covered. Now let's talk about in the event that you suspect you have been scammed, what should you do immediately after you realize this?

Diedra:

Well, one of the things is if you're dealing with a bad actor or a scammer, stop communicating right away.

Whether you're communicating over the phone or whether it's through email or text message, stop communicating with them. Then immediately document everything that you experienced with the bad actor. It will be an important part of making sure when you file a police report, which is another really important tip, that you have all of the information you need.

Contact your bank right away. So, once you've documented everything, you want to reach out to your bank. Again, flip over that bank card call the number on the back of the card and report. I've said, "report, report, report," but it's so important that we report when we have experienced scams or fraud because it enables law enforcement to figure out where that ring of scams or fraud is taking place and do something about it. So, it's really important to report when you feel like you've been a victim.

Make sure that you are protecting all of your personal information by changing your passwords and then stay alert. Stay alert. Just because you may have been a victim doesn't mean that they won't target you again. Again, that's where that identity monitoring comes in handy and it's really easy for you to access.

Then talk about your experience. We talked earlier today about how holidays are all about being with friends and family. It's really important that we normalize conversations about money

including protecting yourself from fraud and scams. So, talk about it with your family. It might be a little bit uncomfortable, but we want to normalize those conversations.

Farnoosh:

Talk about it.

Diedra, I had my business bank account hacked last year.

Diedra:

Wow.

Farnoosh:

It was fake checks getting withdrawn. Like from my bank, my business bank account. Come to find out that business bank accounts were targeted at the time, or are still targeted, just because bad actors know there's probably a good chance you have money in your business bank account, right?

Diedra:

For sure.

Farnoosh:

So that happened to me. I felt like it was my duty to talk about it, right? Because again…

Diedra:

I love that.

Farnoosh:

... here I am. I do this for a living. I talk about protecting your money as my job and to no fault really of my own, they somehow got a hold of my routing and checking information and created fake checks.

Diedra:

I'm so glad that you're talking about it, because unfortunately people feel ashamed at times, or embarrassed is probably a better way of putting it, and they don't talk about it. The only way that we can help people be aware that these things are happening is to talk about it.

You're a financial expert, and if it could happen to you, it could happen to anyone. It's not about how savvy you are; it's really about raising awareness. So, I love that you're talking about it.

And not just with a certain segment of your family, not just the older members of your family. One of the things we're trying to raise awareness is with those who are digitally native. They're very comfortable with technology, but they may not be aware that they're being targeted with social engineering. Younger groups are being targeted by scams more and more. So, it's really

important that we're raising awareness and that people are aware that it could happen to anyone.

Farnoosh:

Yeah. It's a great reminder for us. We have a nine-year-old and a 12-year-old. They're on their games, they're browsing, they're chatting. I mean, my big thing that I repeat a lot in our house is, "Think twice before you click on a link," right?

And I have to remind myself this, because you go to a news website or any website and all of a sudden all these ads, pop-ups, links, and it's almost impossible to not accidentally click on something, right?

Diedra:

Especially when you're in a hurry. Honestly, I don't think we could talk about this too much, because it really is about when you're distracted, when you're multitasking, and you're busy, and the scammer will come in and create a sense of urgency, and before you know it, you've clicked on something. So, we just have to continue to remind ourselves, and particularly during this season when we're so busy.

Farnoosh:

Yeah. Earlier, Diedra, you mentioned the transaction alerts. I do that. I think it's so, so helpful. It's also, for me I think, “Oh, my gosh, I need to stop spending so much money.”

Diedra:

Same way.

Farnoosh:

Or like, “Wait a minute, what was that subscription that I had?” I don't remember. I don't remember. Because, you know, sometimes it's automatic.

Diedra:

Yes.

Farnoosh:

Or, “Wait, I don't think I need this anymore.” So, that's good on a lot of fronts. But what are some other controls that we can put, whether it's on our phones, or any sort of technological bells and whistles to help us avoid scams?

Diedra:

Absolutely.

So, many banks, including Chase, have a card lock feature, so that you can lock your card if you feel like there's a scam. So, that's one feature.

Also, having a Trusted Contact Person. We talked earlier about a family password. Trusted Contact Person is someone you name on your account, and if there is something awry, the bank can reach out to that person that you've listed and just make sure that something that looks out of the ordinary is in fact legitimate.

So, that's a feature that we offer at Chase Bank. You could have a family member, a Trusted Contact Person, listed on your account that we could reach out to. It's just one more thing that you can do as an extra precaution to help protect yourself and have someone looking out for you.

We have caught so many things, like when someone has been duped to believe that they're a part of something legitimate, and it is actually a scam. Being able to call the contact person on their account has stopped people from losing thousands of dollars because they didn't realize that they had been scammed, or that they were in the midst of a scam.

Farnoosh:

Wow.

I'm even just thinking if you have an aging parent who lives alone—and everyone needs this, but especially those in the sandwich generation. They've got their young kids on the devices. They have their parents they're looking after. This is brilliant.

Diedra:

100%, and again, the scammers and fraudsters are so sophisticated these days. Farnoosh, we see people of all ages and stages and all levels of sophistication become victims of scams.

The moment the scenario that was socially engineered to get their attention has made them afraid and made them believe that it's legitimate. So, the extent to which you have someone that can say, "Hmm, maybe something about this isn't right." Giving you time to figure things out can make a big difference.

Farnoosh:

You've given us so much to think about, and also talk and ask from our financial services companies, our credit card companies, our banks. Even just that one tip about adding someone onto your account as a backup witness.

What do you wish more people would ask their bank about fraud and scam prevention before something goes wrong? Because I feel like sometimes there are these services and ways to look out for yourself that you don't know what you don't know.

Diedra:

100%. So, you said it. It is to ask your bank for help beforehand.

So many times, when customers reach out to us, it's after the scam has taken place. And frankly, whether it's a scam or whether it's fraud, oftentimes the bad actor has been working this

scheme long before your money ever leaves your bank. So, it's really about reaching out to your bank.

At Chase, we offer free workshops in our branches. We do over 1,000 workshops per year. That's like three a day in our branches all over the country, and it's free whether you're a client or not. You can come in and attend a workshop and make yourself aware. Whether it is coming in and talking with someone about how you can help protect yourself or going to our website: chase.com/security.

Chase.com/security has all kinds of tips around how to help protect yourself and your loved ones from scams or fraud. You can also stop by one of our Chase branches and ask how you can attend one of our many workshops. We have them for all ages and stages of life, and they're free whether you're a client of Chase or not. If you're a part of our local community, you're welcome to attend our workshops.

But really seek out information on how to help protect yourself before the fraud happens and how to stay aware.

Farnoosh:

Diedra Porché, thank you so much for joining us for this timely, timely conversation.

Before you buy anything, before you click on anything-—like, I hope you were taking notes, everybody, and if not, you know, good thing this is a recording. You can go back and play it, send it to your friends, share it widely.

My biggest takeaway here is just that scammers thrive on urgency. They want us to panic. They want us to click quickly, respond quickly, send money before we've had a chance to even think about it.

You mentioned earlier about charitable giving this time of year. We're in this sort of season-of-giving mindset, right? So, we don't even think twice if we get asked for money. We think it's going to a legit source. It’s very easy to let our guards down during the holidays when we're already juggling a million things. Verify that message, website, or too-good-to-be-true offer before taking action.

If something feels off, trust your instincts, and let's talk about this with our families, older kids, younger kids, parents, friends.

For more practical tips, everybody, go to chase.com/security. Chase.com/security, to help protect your money and personal information.

Thanks again to Chase for sponsoring today's episode, and thanks to all of you for listening.

Until next time, I hope your day is So Money.