EPISODE 310

[ASK FARNOOSH]

[0:00:34]

FT: Creating opportunities by starting your own business is one of the most empowering things you can do for yourself. However, it can also be overwhelming at times. The secret to getting more done isn't about finding more time, but rather finding the right tools. Our friends at FreshBooks couldn't agree more!

FreshBooks has created an amazingly simply invoicing tool designed for small business owners who need to focus on their work, not their paperwork. Oh, and invoicing is only the start! FreshBooks lets you know instantly when your client has viewed your invoice, and even imports your expenses directly from your business chequing account. Get ready to say "goodbye" to searching for receipts when it comes to tax time.

If you do have questions, just contact the award-winning FreshBooks support team and get help from real live humans, no phone tree, no "let me escalate that", just helpful service at the drop of a hat. To try FreshBooks for free for 30 days, just go to FeLMBooks.com/somoney and enter "So Money" in the "How did you hear about us?" section.

[ASK FARNOOSH]

[0:01:37]

FT: Welcome back to So Money everyone, I'm your host Farnoosh Torabi, it's Friday, so what does that mean? It's time for Ask Farnoosh. As we know, it is the busiest shopping period of the year. Tim and I are still attacking our gift list and we're doing a lot of our shopping online. Some in stores, we want to support the Brooklyn small businesses but we're going to spending a lot this year because families are getting bigger, and you know, I like the holidays. It's a good time to be generous and fun to get gifts.

But also a busy time for fraud attacks. This is something that I know because I cover this industry and this area closely but for a lot of consumers, we might take for granted just how protected and safe we are. What can you do to protect yourself as your swiping and as you're shopping online this holiday season?

For some of you who come to this podcast consistently, maybe you remember, I had my wallet stolen over the summer and this thief quickly rang up several hundreds of dollars' worth of merchandise within the hour. I only discovered this because, well I went to go pull up my wallet and it wasn't there. And I came home and frantically checked my credit card statements and lo and behold, there already had been some purchases.

Now I was like anybody else, fearful of my identity and I filed a police report, I notified the credit bureau so they could monitor my credit for a period of time, knock on wood, nothing crazy since then, but it is unnerving. I personally know just how vulnerable you can feel when your identity is potentially stolen or at least your wallet is not with you.

So that brings us to the importance of today's special edition of Ask Farnoosh. There was a point to that story. Today we're dedicating Ask Farnoosh to credit protection, identity protection. As you know, I've been working with a team at Chase Slate to bring credit awareness and financial literacy to audiences all over the country, large and small. Card fraud is an important and timely topic right now.

So very excited and honored to introduce my special guest today who is going to Share with us some best practices for shopping safely and protecting ourselves from various types of card and identity theft. You have to listen to the end of this episode. Lots of important information and of course we do have the transcripts online. But Leslie Malone is here with us, she is the executive director of credit and debit card fraud prevention at Chase.

Leslie, welcome to Ask Farnoosh.

[0:04:06]

LM: Thank you, I am thrilled to be here.

[0:04:08]

FT: Well I should say, “Welcome to Ask Leslie.” [Laughter]

[0:04:10]

LM: Right.

[0:04:12]

FT: You’ll be answering these questions, I’ll help along the way, I’ve got some personal anecdotes and some background on this but you are the imminent expert. And so let’s start with what is new this holiday season, and it’s not new as of yesterday but as of October, there was a big push to get retailers and banks on the same page when it comes to the chip cards and the chip machines.

This is supposed to be a way to really prevent card fraud. How should we approach this new trend? I know when you go to Target for example, they require it that you dip and you don’t swipe. Some retailers don’t have the technology yet. So how do you navigate this as a consumer, what’s the most important thing to know?

[0:04:58]

LM: Yup, great question, the chip card, you’re right, is absolutely the most exciting thing this year and many of us who have been in Fraud for a long time had been waiting for this day. Chip cards are the real game changer for the industry when it comes to more secure spending this holiday season.

By now, most people have seen or received their new chip card and some have had experience with them as they’ve traveled into Europe and Canada who have been on a chip card program for a long time. You’re absolutely right, use the chip whenever possible, don’t swipe if you don’t have to.

Let me quickly tell you what the chip is, it's an embedded chip into the front of the card and generally the cards are going to look very much the same, they're going to have the strip on the back, they're going to still have the three digit code that we're all used to giving when we shop online but now there's the chip in the front of the card.

What that does is it's a unique single use code to validate every separate transaction. It changes every time you use it. This process makes the chip much more difficult to steal and therefore much more difficult to counterfeit for the fraudsters. So that's really the unique and great part of the chip technology. You're right, not all retailers have the chip terminals up and running yet but again ask if you can use your chip card at those terminals.

When you use your card at the register, it's a little bit different than when we swipe our cards. You will be asked to insert your card into the chip terminal and you're going to leave it in there throughout the transaction, don't remove it until the system tells you to take it out. The thing about chip cards is, the process will take a little bit longer but the tradeoff is a much more secure transaction. This is a huge deal for the industry.

[0:06:55]

FT: And specifically, what type of card fraud does this help to prevent. IT's not all types of card fraud, right? It's the duplicity fraud.

[0:07:03]

LM: You're absolutely right. Counterfeit fraud is really what it's going to stop, it was rather easy for the fraud guys to counterfeit the mag strip on the back of the plastic and the chip technology is much harder to counterfeit. For those of you who had an experience where you were you get a phone call at home to say, "Hey, somebody's using your card in New York City," and you live in Dallas Texas, most likely there was a counterfeit card made and that's how they're spending at the same time when you have your cards sitting in front of you.

That experience in that situation should be much more diminished with the chip technology becoming more and more prevalent as retailers get up and running on the new system.

[0:07:56]

FT: Does this in any way, I guess as Chase found out in their own survey, 69% of people survey said that they were worried about having their credit information that's used at stores, stolen by computer hackers. With this chip technology, does that in some way create a barrier to hackers being able to access your card information now because you're dipping instead of swiping or is that just a whole separate issue?

[0:08:28]

LM: No, you're absolutely right. The chip will prevent the fraud guys from being able to steal that information and make credit cards in your name, absolutely. The chip is what's going to prevent all of that from happening going forward.

[0:08:42]

FT: Okay, great, that kind of makes sense now why Target was one of the first adopters of this. They were victims of the breach not too long ago. Great, I feel like I'm pretty good on the whole chip card technology. Even though it's relatively new, I feel as though it's in play to a lot of the bigger stores. If you're shopping at the big stores, at the mall, chances are, you will experience this and absolutely, if you have the opportunity to dip, do dip.

Now, you always get this question, debit or credit. Does it matter really? When it comes to making a purchase as far as your identity protection?

[0:09:24]

LM: Using your debit or credit versus credit card, it's really a matter of preference and what's worked for you. Many people really just want to use their debit card and have the money taken directly out of their account and many others are just very comfortable with credit card situation

and paying at the end of the month. It all depends on what works for you. The important thing to remember, whether you use a debit card or a credit card, you have that peace of mind that you have zero liability protection.

Meaning, if fraud should hit your debit card or your credit card, you are not liable for any of those charges. That's really the important thing to realize. Also, Chase monitors both credit cards and debit cards and this is predominantly what my team focuses on, 24 by seven monitoring. Seven days a week, holidays as well, we're watching to look for unusual activity on both the debit cards and the credit cards.

That's really important, so you should feel very comfortable using either your debit card or your credit card. Then add the chip technology on top of it and it really should be a very secure process.

[0:09:24]

FT: Do you think that it's fair for consumers to feel that their bank will necessarily catch the fraud. I feel like I've been fortunate, I'm a Chase customer, I had at one point, my Chase Sapphire card had been hacked unbeknownst to me, only because Chase contacted me right away, did I realize it? I have this sense of comfort in where I bank but I feel like that could be a crutch for some consumers. They think that the bank is always going to be there to jump in and save the day but as a consumer, you have to be really vigilant as well.

[0:11:13]

LM: Absolutely. Each consumer's going to have to assess what kind of monitoring their bank has in place, right? One of the things I would recommend to anyone who has a credit card is, and the way I get the most peace of mind is, I have turned off all paper statement and I use my online tools. So Chase has some really nice online tools as well as mobile apps as well.

I go in and check my transactions, I try to do it daily but I do it quite often to make sure that — so I'm protecting myself and sort of being my own advocate to make sure that nothing unusual could hit my own credit card. I would really encourage people that aren't sure if their banks have

the same type of monitoring as Chase does, I would recommend that they do that quite often as much as they can to see what's going on, on their own account. I think that's one way that they can feel a lot more secure.

You can check your account like I said throughout the month to make sure you recognize all those charges. If you see anything you don't recognize, absolutely pick up the phone immediately and call your bank. Identify that charge and if it is fraud, they should be able to help you get a new card and get those fraud accounts credit off your account and credit to your statement. That's probably the best way to protect yourself.

But I really do love the new Chase mobile app for this purpose as well because I can do it anywhere. I don't have to be at home at night on my computer. I am easily frustrated with hard to use technology but this app really makes it easy to use and stay on top of that credit and debit account. And it also contains a lot of other neat features that you may want to check out. Hands down, have people go in and check on their own account to make sure there's nothing unusual going on.

[0:13:07]

FT: Besides downloading your mobile app, which I do. I think it's an easy free way to stay, monitoring your account but what are some other, since we're talking about good habits, what would you suggest some other best practices for just maintaining as much control over your financial identity, identity protection throughout the holidays, and for that matter, all year.

[0:13:31]

LM: Yeah, good question. We haven't talk about online shopping and we know the chip card really doesn't really play an increased security role in online shopping but there are definitely things you can do to protect yourself during the holiday season and all year long.

First, shop sites that you're familiar with. So I have my select group of merchants that I trust and I stick to as much as possible, that's one way to protect yourself online. Second, make sure that the letter's in front — so you'll see the https in front of the www. Always make sure that a

merchant you're shopping at has that "S" at the end of the https. That indicates that you are shopping at a secure site.

Also, if you're going to do online shopping, beware of the public Wi-Fi. The public networks are not encrypted and it's just the best way, it's just best not to key in your debit or your credit card when you're on a public Wi-Fi network. Then finally, don't give your card information or personal information over the phone or through email.

This is called phishing and it is rampant during the holiday season, the fraud guys loves to hide behind all of the increased shopping that goes on. We see a large uptick in this during the holiday season as well. Those are some of the tips you can protect yourself online this holiday season.

[0:14:53]

FT: I would add that phishing is rampant on social media, texting. It used to be just email, right? Now you can get a phishing scam through Facebook, through Twitter. Just be really careful, extra careful. If you're getting notified from someone that you're not familiar with or maybe, they're pretty savvy, they'll figure out from your Facebook profile that you donate to Unicef every year so they'll pretend to be Unicef and say, "We thank you for your contribution. There was a mess up in billing, please email us or contact us with your information."

So just be very careful because they tend to pose as the real deal, they'll pretend they're the IRS, they'll pretend they're with a nonprofit to get you to make a move. Just check the domain name of the email, I always find that is a good tell all like if the domain name of the email is not, doesn't look legit. If there's no contact information other than just an email, there should be a phone number, there should be a legitimate address, always red flags.

So thanks for bringing that up because not only is it rampant but it's really happening in new and creative ways where people are spending a lot of their time.

[0:16:09]

LM: Yeah, the other thing as you mentioned, social media, that's a great segway into setting your password. When we set our password, always password protect your mobile device. Obviously we all have passwords on our online systems in our other accounts but use something that's not easily detected because the fraud guys and the hackers do go in to social media to look for your dog's name or look for your children's birth dates, to look for your children's names.

If you use those in your password, it's something that they can easily figure out. Really think hard about using numbers and symbols and words that aren't easily figured out, I think that's really a good thing to get in to.

[0:16:53]

FT: It's hard to remember all your passwords though.

[0:16:56]

LM: It is.

[0:16:58]

FT: There are some services out there that will help keep all your passwords locked up in a cloud service or somewhere accessible so you're not making all these false attempts or wrong attempts to get in to an account and then you're locked out for 24 hours, believe me, that's so frustrating. When you're just trying to log in to your favorite website and you're locked out because you forgot the password, it's happened.

[0:17:26]

LM: Happens all the time. Yup, to me and sometimes my husband goes and changes it for whatever reason and then…

[0:17:31]

FT: Right. Have you ever had your identity stolen or are your cards stolen?

[0:17:39]

LM: I'm sorry?

[0:17:40]

FT: Have you ever been a victim of identity theft or card fraud?

[0:17:46]

LM: Very infrequently which is, there were a couple of times, I can only remember two, yes, where I saw some transactions come through from text to the grocery store. Very seamless, I called chase, got my new card, got the charges reversed and back in line. I had not been a victim of identity theft but we do pull our credit bureaus on an annual basis to make sure that there's nothing unusual going on there as well.

[0:18:19]

FT: Let's talk about worst case scenario. In the event that you are, not only your card is stolen but maybe your identity is at risk as well or has been compromised. What do you do? Obviously the first step is to contact your banks but from there, what should you do in order of importance?

[0:18:40]

LM: Yup, you're absolutely right, contact your bank. Chase actually has a special identity theft unit where we actually help the identity theft victim put passwords on all their accounts, special passwords that if the fraud guy try to call in and impersonate them, they wouldn't have that special password. We asked them to run a virus scan on their computer to make sure that computer is clean before we go ahead and change their user ID and their password on their online account as well.

Definitely put alerts on your credit bureaus to make sure that if somebody does try to reach out to the credit bureau and get credit in your name that that freeze will be on that account and the bank will not move forward with the credit because they can see that freeze on your credit accounts. You can file a police report but definitely work with your bank as they can help you work through that and really secure all of your accounts. That second attack can't happen.

[0:19:50]

FT: Right, I think the freeze is really important and the police report too because let's say in my case, for example, my wallet gets stolen and yes they rang out some charges, did they try to open up bank accounts in my name or credit cards in my name, no but not yet. They could later and at that point you might have forgotten or you're not as concerned about your identity but this thief has been holding on to your information, waiting to strike when you're least expecting it and I think in most cases, for those reasons, it's really important to have a paper trail and the credit freeze for a while.

Especially if you feel like your card and your personal information's in the wrong hands. It's really important to be vigilant, not just for the next month but perhaps even for the following year would you say? Would you agree?

[0:20:39]

LM: Absolutely, yup, absolutely. With our special identity theft unit, for a period of time, we actually will have, whenever that customer calls in or anybody calls in on that account to talk to customer service or whoever, it will route to the special identity theft group so we can make sure that we're actually dealing with our card holder and that just puts another layer of protection on that customer while they work through the identity theft situation. We add that second layer of protection for them.

[0:21:13]

FT: Last question, as far as financial institutions go, how important is fraud protection right now as far as their list of priorities and how important is this to customers as they're choosing where to bank. Because I can only imagine in this era of technology, while things have gotten easier and more convenient, also, easier and more convenient for potential fraudsters.

How are banks addressing that to relieve consumers of the fact that yes, fraud is out there but there are some protections in place and we want to help you, how much service is there around this, do you think that there is enough or there needs to be more education?

[0:22:03]

LM: Well, you know, it depends on the institution and the bank on how much they want to invest in the security and the fraud tools. Chase has obviously been very focused on the chip cards. We are also invested in something called tokenization for our online and mobile payment. This essentially creates a random string of letters, characters, numbers for a secure transaction to replace the account number.

So if the fraud seeker is trying to get your account number, it will get this random string of characters and numbers and really protect your account. Chase is really looking to see how much more secure we can create our online systems, our mobile systems and we're constantly focused on that.

But they absolutely should be because the fraud guys get smarter and more savvy. We as bunks owe it to our customers to get more savvy as well. We need to be focused on this all the time.

[0:23:08]

FT: I know I said that was the last question but I have one more because I'm such a nerd but I'm curious because you're such an insider and you have a perspective that the average person/ consumer doesn't have, what should we be particularly concerned about in the new year, if there's anything that's trending as far as how fraudsters are getting our information, that

consumers don't really realize or aren't really aware of something that you're seeing that maybe isn't in the public eye?

[0:23:43]

LM: I mean, first thing comes to mind is the chip card, right? That has really shut down and minimized probably our biggest issue, which was the large reaches and large merchants, right? That was a huge pain point for customers because they would have to get new cards reissued and this will really take care of that situation for our card holders.

I think that is the biggest thing. Scams are another one, you mentioned it when you talked about your college scholarship search and scams. Scams are out there right? You need to always be very careful when people are asking you to put in your social security number or your birth date or all of your PII information. They're not — a bank or an institution, it's not going to ask you to do that.

Clicking on links and having viruses put in to people's computers, that's still very prevalent as well but people can protect themselves with antivirus software. Again, I think just being aware and being vigilant about all of these things that are happening out there, they just need to be very weary.

And even getting emails from somebody you know right? From a niece or nephew, often times doesn't come from that niece or nephew until you really have to scrutinize everything you receive and open and if it just doesn't seem right, go with your gut and don't open it and delete it.

[0:25:18]

FT: Great advice and I would just say that you should report out there, let people know what's happening. The other day I got a voicemail from an automated person, an automated voice from the "Internal Revenue Service" and they claimed that I had to call them back because I my name was attached to tax fraud evasion and I have to say, I got a little nervous at first because it was a 202 number, which is Washington DC which is where the IRS is headquartered.

But I thought, A, I'm not evading my taxes but also, why would they leave me a voicemail. Usually the IRS communicates via snail mail and it's notarized or on a letterhead. I told my accountant what happened and he goes, "Yup, that's fraud, we're going to let the IRS know."

Parting advice, I think we're all going to have, we're going to run into these shady experiences, whether it's now or in the future, just share these stories of people because I think we'll be able to help each other out that way. Because one person's experience can be another person's saving grace. Just be sure that you're sharing these occurrences with either the organizations themselves, your friends, your family because I think it does take a village sometimes to protect yourself from identity theft.

[0:26:52]

LM: Absolutely. I'm glad you brought up that the fraud guys absolutely use scare tactics and fear tactics, right? Your bank will not do that, they're not going to send you a threatening letter, they're not going to say, "If you don't change your password, you're going to lose access to all your accounts." They're not going to do things like that. The fraud guys will use those tactics often. I think that's a great point you make is the fear tactic are consistently used.

[0:27:22]

FT: Well, I'm less afraid now after speaking with you, thank you so much Leslie for joining us and giving us your insights and really this important information for all of us as we head into the heavy, heavy busy shopping season and of course this is advice that we can use all year round.

Leslie Maloney, executive director of Credit and Debit Card Fraud Prevention at Chase. Thank you so much and happy holidays to you and your family.

[0:27:48]

LM: Thank you and you have a relaxing holiday season as well and just keep in mind that Chase has you covered against fraud this holiday season.

[0:27:55]

FT: Thank you.

[END]

