Regions Wealth Podcast

Episode 18: Protecting Your Finances After a Data Breach

According to Javelin's 2019 Identity Fraud Study, new account fraud is up 13%. And if your personal information has ever been exposed in a data breach, you may be at an increased risk. In this episode of Regions Wealth Podcast, Chief Information Security Officer Jeff Kennedy joins us to discuss the steps individuals should take if their information has been exposed in a data breach and provide fraud prevention tips.

Episode Transcript

Sarah Fister-Gale:

Welcome to Regions Wealth Podcast, the podcast that tackles life's challenges with financial experience. I'm your host, Sarah Fister-Gale.

According to Javelin's 2019 Identity Fraud Study, new account fraud is up 13%. And if your personal information has ever been exposed in a data breach, you may be at an increased risk. This episode will share tips on fraud prevention, while also covering the steps individuals should take if their information has been exposed in a data breach.

Joining me remotely is Jeff Kennedy. He's the chief information security officer for Regions Bank. Jeff, thanks for joining us today.

Jeff Kennedy:

Good afternoon.

Sarah:

In this episode of Regions Wealth Podcast, we're discussing data breaches and fraud. We've taken frequently asked questions from a bunch of people and developed a character who needs your help. Let's listen.

Barb:

"Hello, there! My name is Barb, and we've got my husband Mel here as well, although I expect he won't be doing much talking. We have some questions about a data breach that's really caused a lot of problems for us. We have always been concerned about the safety of our

information. We've kept our phone number unlisted for decades. We don't use social media websites or anything like that, and we always keep our antivirus software up-to-date.

Well, two years ago, Mel received an email saying our information had been exposed in a data breach. Of course, we were very alarmed. I called my daughter Susan and asked her what this all meant. Now, Susan told me not to be concerned, she said that these things happen all the time and they'd probably just nabbed no more than our mailing address. The company advised us to change our password, so we picked a new one. Now, Mel is a bit forgetful, so we use one password for all of our logins. We had to go around updating it on so many different websites!"

Sarah:

Okay. So to start, let's talk about data breaches, which are defined as a security incident in which data is accessed without authorization. How do data breaches typically occur?

Jeff:

This normally occurs either through poor password management, vulnerabilities on a website from a company, some form of human error, potentially a malicious insider at a company. I think, though, it's important to look beyond the textbook definition to the intent behind the event. Human error occurs all the time. Technically, that's a breach. On the other side, when there is a more malicious actor involved, and they circumvent security controls at companies, and they are able to steal information, that malicious intent, that likelihood of harm, really raises the response that an individual needs to have when they get those notifications, and a need to get more information and clarity around what happened in those specific events.

Sarah:

According to a report compiled by Risk Based Security, a whopping 8.4 billion records were exposed in Q1 2020. That's a 273% increase compared to Q1 2019. So it's safe to assume that many of us have either already been impacted by a data breach or will eventually. Now, when I get an email like the one Barb and Mel received, how can I find out what sort of data has been exposed?

Jeff:

The best way is to actually go back to the company that has reported the problem, because it's important to understand the date the event occurred, any perspective on how the event occurred, again, was it something malicious that was behind it? What type of information was taken. The more sensitive the information, like your Social Security number, your driver's license, then the greater risk that event is to you. But reaching out to them directly and trying to get some of that clarity is, in my mind, the best way to go. A lot of them will set up a dedicated 1-800 number, a dedicated website, and you can engage them and get that clarity that you need.

Sarah:

In Barb's case, her daughter said, "Oh, they probably just took your email address." Should you be concerned if someone has your email address, or do you have to worry only about more important information, like your Social Security number?

Jeff:

Any information that gets stolen, relevant to you and your behaviors, like an email address, your home address, heck, even where you went on vacation, can be used as an opportunity to social engineer other information from you. But when it comes to identity theft, it is that culmination of data. The more of that they get, the more they're able to either take action with that and use that to commit fraud, or sell that to someone who will want to commit fraud in your name.

Sarah:

Many of us have received these data breach emails, and most simply advise us to update our passwords. But are there other steps individuals should take when receiving an email like this?

Jeff:

Yes, ma'am. The very first thing is just making sure that you're clear on what information was stolen. If you see that as high risk information that could be used to take over your identity, then I would put a credit freeze on, so you could reach out to the three major credit bureaus, put a freeze in place. That way no one can set up a new credit product in your name. Or a credit monitoring service may be a good way to go to help protect you. Sometimes these bad guys, when they get information, they'll sit on it for several months and then use it at a later date. You may think you're okay, but then six months down the road, you may find out that you're not.

Sarah:

How do you know if a credit freeze or credit monitoring is the better choice?

Jeff:

In my opinion, it really kind of comes down to your need for access to credit and the amount of convenience that you're going to want in taking the freeze on and off. It is a little bit cumbersome when I did it a few years ago. So if you're going to be actively purchasing products and services, or you're going to need extensions of new credit, monitoring is probably the easier, more convenient way to do it, versus the credit freeze.

And then also, depending on the credit monitoring service, there may be other things that they can offer you, such as dark web monitoring. So if they find some of your information out on the dark web, they can report that to you, and you may see that as a value added service that comes with some of the monitoring.

Sarah:

Okay. So, let's go back to what Barb and Mel told us. They have been using the same password for everything, and, then they went around and changed all their passwords to the same new password. Why is this a mistake, particularly when something like a data breach comes into play?

Jeff:

There are a number of companies that ask for user ID and password. It could be a restaurant, it could be your fitness tracker, it's your financial services, it's your bank. If you use the same user ID and password in all of those, if one of them gets compromised, the rest of them are at risk. It would make sense that the security at a bank should be a lot tighter than, probably, the security on your fitness tracking app. So if your fitness tracker app happened to get compromised, because they were, for whatever reason, had a security incident, the bad guys would take that same user ID and password from one breach event, and will try that against other websites, looking to see where people have done that exact same thing and just reused it. If they happen to have the user ID and password for your bank website, that gives them a big step forward in trying to get access to your account.

Now, many other banks, like Regions, have layers of control, so you can't just login with the user ID and password. There are other security things that are happening behind the scenes to provide challenge questions or other things to make sure that you are who you are. But giving them a valid user ID and password does just put you at greater risk of a compromise on another website.

Sarah:

So it sounds like for Barb and Mel, using that same password for every site they access is definitely putting them at an increased risk. Let’s take a listen to what happens next.

Barb:

“Last month, Mel and I were pulling our credit and noticed there were some strange accounts that didn’t belong to us, going back a few years: three credit cards, a utility account, and countless credit inquiries, too, including one for an auto loan! Mel and I have always been meticulous about our credit, and were shocked to discover that our score had plummeted because the scammer had never made a payment on any of these credit cards. We don’t know where to begin.”

Sarah:

So, what are the next steps someone should take when they discover a fraudulent account on their credit report?

Jeff:

Unfortunately, there are several steps that have to be taken. The first one is to file a police report. That establishes a baseline of what happened, when it happened. And the likelihood that they're going to find anybody is very, very low. But when it comes to you restoring your good name and good credit, it's a great component to have in the journey that you're about to go through. Once you get the police report filed, if you haven't already put a freeze on your credit, go ahead and get that done with the different credit agencies. Then for the companies that were listed, go ahead and notify those institutions, send them a copy of the police report, so that way that they know that you're not the person that opened the account. That also allows them a mechanism to hopefully start to get some of this stuff off your credit report going forward.

Now, there are a couple of options to help with this journey. One, you can kind of do it all on your own. There are some government websites that can help you go off and do that, especially around the Federal Trade Commission. They have one specifically around identity theft. Or you can reach to some of the large credit bureaus. They have a service that is basically an ID restoration service. Of course, the cost on that, that's not a free service. But if you have a lot of work to do in restoring your credit, it may be beneficial to get a third party involved to help make that happen.

Sarah:

Okay. It sounds as though this fraud has gone unnoticed for years. How frequently should individuals review their credit report for fraud?

Jeff:

People will recommend that you review your credit reports annually. Sometimes people will look at all three reports at one time. I would recommend that you take an opportunity to kind of pull those reports for each of the credit unions throughout the year. Spread that out, so if there's a fraudulent event that's occurring, I think there's a greater chance that you could catch that.

Sarah:

That’s a great tip for monitoring your credit throughout the year. And how do I access those free annual credit reports from each bureau?

Jeff:

There's a website, annualcreditreport.com, that you can go to, and allows you to go and pull from each of them. But again, you don't have to pull all three of them at one time.

Sarah:

And that website you referenced — annualcreditreport.com — is that the only source for that free annual credit report from each credit bureau?

Jeff Kennedy:

This is the only source for your free credit report authorized by federal law.

Sarah:

Terrific. So, when it comes to spotting fraud, are there any other red flags that people should keep an eye out for besides simply checking their credit report?

Jeff:

There are a couple. If you start to get some phone calls from collectors trying to collect debts, and you know you haven't opened up accounts with those businesses, then you probably need to stop and say, "Hey, I think I've got a bit of a telltale sign here that I need to go take a deep dive." And if you get any notices from the IRS that seem a little bit odd, that may be an item that you want to look for as well.

And I think the other thing is if there's any notable changes on any of your existing accounts. So if you receive an alert that your mailing address was changed or email address was changed, there was a phone number changed on your account, and you know you didn't do those things, don't just ignore it. But if you're getting some of those alerts and notices of changes on your account, that may also be another sign that a bad guy has gotten access to your information and is trying to make it their own.

Sarah:

And what about through the traditional mail?

Jeff:

If you get something that looks like it has potential to notify you of an issue or concern, don't go just login to a website, call, talk to them directly, be sensitive to the information, validate who they are. But if you get something in the mail, and it has your personal information on it, take the opportunity to shred it.

Sarah:

Always validate who they are. That's an important step. OK, let's take a listen to the final portion of Barb and Mel's story.

Barb:

"...To make matters worse, we've received three more of those data breach emails over the years. Each time, they tell us to just change our password! We have always been so careful, and aren't quite sure what we should be doing to better safeguard our information in the future."

Sarah:

Okay. So we know data breaches are becoming increasingly common. What steps can consumers take to protect themselves against being seriously impacted by a data breach?

Jeff:

The first thing that they can do is limit the amount of information that they provide to the company that they're interacting with. When you sign up for that fitness tracking app, if they're asking for your Social Security number, date of birth, where you live, that's not really relevant. You don't think you need that to take advantage of that service? Then don't give that information.

Sarah:

So, that's really good advice. I feel like every interaction I have with retail or any vendor, they ask for personal information. Even when I'm buying clothes at a retail shop, they want my email address. Can I just say no?

Jeff:

Sure! You can absolutely tell them no. It may mean that they can't send you an email of the receipt, so you may lose a feature or capability that they're offering, but I think that's a matter of personal choice, of how bad do you think you need the service that they're offering, and would you give them your email or other personal information to that company.

Secondly, actively monitor your credit throughout the year. Not just once every 12 months, but spread those reports out over multiple times. And then lastly put a freeze on your credit. If you don't think you're going to need an immediate need to get credit approval, then put a freeze on it. It's the best, safest way to make sure that no one is taking advantage of your good credit. And then go ahead and actively monitor that credit. I think what's important when you think about how to protect yourself is you got to understand there's a bit of a risk trade-off. Make sure that you're kind of thinking about the data that you have, who you're interacting with, and how you're going to be consuming those services, and make sure that all those things align, and I think that will really help kind of minimize some of the risk, if the company you're dealing with has a bad day and has a data breach.

Sarah:

There's always a trade-off, isn't there? So Jeff, at the end of each episode, we like to ask for

some key takeaways — some quick tips for our listeners. When it comes to preventing fraud, what are some key takeaways you'd like to share with our listeners?

Jeff:

A couple of things. First is, don't share information with businesses that you don't believe that they need. Where you can, go ahead and put a freeze on your credit, and if not, maybe monitoring makes the most sense. And then throughout the year, make sure you're checking your credit reports. I think one of the items that I'd also say is that you have got to use good security practices. You need to make sure that you have antivirus on your computer, that you're updating the software on your PC. Try not to use public networks. If you don't know or trust that network, don't get on it. Make sure that you have the right security on your home network, so change default passwords, things along that line. Make sure that when you're using bank websites, use a different password than you generally use on others. Make sure it's a nice strong password. So there are a number of things there that you can do to better protect yourself and make it less likely that, if there's a problem on the business side, it might less impact on you.

And then the last item I would remind people is that it takes both you and the company that you're interacting with to be safe. If you're not patching your computer, if you're not using strong passwords, if you're using an email service that allows you to do what's called multi-factor authentication, where they send you a text message, for example, to log in. If you're not taking advantage of those types of things to better secure you and how you interact with that company, then it just makes it harder for that company. It takes both sides of the folks in that transaction or in that business relationship to be secure, to help make sure that the overall relationship is secure.

Sarah:

Thank you so much, Jeff Kennedy, chief information security officer at Regions Bank. This has been incredibly useful information.

Jeff:

Thank you for the time. I appreciate the opportunity.

Sarah:

And thank *you* for joining us today. Each episode of Regions Wealth Podcast covers a different financial challenge, so be sure to check back, and maybe introduce us to a friend you think might benefit from these insights. For more, visit www.regions.com/wealthpodcast.

financial advice. Although Regions believes this information to be accurate as of the date written, it cannot ensure that it will remain up to date. The people and events are fictional, but represent real issues. No identification with actual persons is intended or should be inferred. Statements of individuals are their own—not Regions'. Consult an appropriate professional concerning your specific situation. References to a company or security or links to third-party website do not imply endorsement or recommendation.