[music]

Sarah Thompson: Hello, and welcome to *Fraud Talk, t*he ACFE's monthly podcast. I'm Sarah Thompson the communications manager at the ACFE. Today I'm joined by Scott Ward senior vice president at Qlarant. Thank you for joining us today, Scott.

Scott Ward: Thank you for having me today.

Sarah: Scott you have extensive experience in the healthcare fraud field, especially investigating and auditing cases related to Medicare and Medicaid. I know that medical identity theft has become a hot topic over the past few years. Can you start us off by explaining what medical identity theft is?

Scott: Certainly. Medical identity theft is when someone or an individual uses your personal information by stealing it, such as your name, social security number, health insurance number, like if it's private insurance, Medicare number, Medicaid number to submit fraudulent claims to health insurers and to government-funded programs without your authorization.

Sarah: How does that differ from regular identity theft?

Scott: Well, with traditional regular identity theft, you most likely are going to realize it relatively quickly that it happens such as credit card, fraud, or theft. You might get an alert from your company that you have your credit card with, or you get an alert from your bank because there's a lot of checks and balances in place. In most cases when it comes to medical identity theft, you really don't know you may have been a victim until maybe you go for medical treatments or you have some life-threatening emergency procedure. It's something that can happen and can sit and grow for years without you ever knowing.

Sarah: That sounds just like the worst-case scenario if you're going in for something that you're already possibly stressed out because you have to make a serious medical decision and only to find out then when you're at your lowest [chuckles] that someone has stolen that. That's horrible. What is it about healthcare data specifically that makes it an attractive target for fraudsters trying to steal identities? Are there fraudsters that only target medical identity theft, or do they also do a regular identity theft or a mix of the two, but what is it about medical data?

Scott: Well, I think that what is a common misconception is that the public may or may not realize the value of what their data is related to medical care, the value of it. From a Medicare/Medicaid standpoint, a person's personal health information or your identifiers are valued anywhere from a million to $1.5 million in potential medical charges that could be billed to those contracts. Then private insurance, it could be even more than that depending upon what type of services that you may see that have been fraudulently billed.

From a standpoint of the types of frauds out there, fraudsters believe that it's a victimless crime because they're not impacting anyone, but that's really not the case. There are some other reasons why this is something that's really attractive or targeted is because with the compromised credentials, identity thieves can use that victims' data to even acquire medical treatments, receive elective surgeries, get prescriptions filled as well. They can also use that information to sell to other individuals that may not have healthcare benefits or things of that nature that another individual could actually get the benefits instead of who actually those benefits are intended for.

Sarah: What are some of the common schemes that you see with medical identity theft? Are there more common ways than others in order to access and steal that data? Is there more common ways for people to use that? You mentioned using it to get elective surgeries or get prescriptions filled. What are some of the trends that you see?

Scott: There's some of the common schemes that have been identified with identity thieves stealing individuals' protected health information. Probably one of the most common that people could relate to or understand is when you see the commercials usually at late-night television early in the morning telling you that there's no cost to you. All you have to do is call. Those are somewhat of a solicitation, but they get around some of the rules and regulations about solicitation because they're encouraging you to call them, and then give your information for-- it could be things like orthotic type, braces, or power wheelchairs or certain types of devices, catheters.

You see those types of commercials. Those are probably the most well-known schemes, but then other things where you have like healthcare fairs where they are offering to give you free health checkups, check your vital signs, maybe do blood work free, just preventative care, but it's all disguised in a sense just to obtain your information. A lot of times it impacts the Medicare programs and the Medicaid programs because those are federally funded and they're both good faith programs because the intent is to make sure that those providing the medical care are paid relatively quickly, not like your traditional insurance.

That's why the value of that information is so much, and people commonly don't realize that they're getting that information, giving it out unknowingly only to realize later on down the road that their information has been compromised. Usually, they find that out if they do look at their explanation of benefits or potentially get a bill for services they never received. Sometimes they're even contacted by debt collectors. You see that a lot in the private insurance for medical debt that they don't really owe. They had no idea that the services were actually rendered. It's one of those things that it's compounded so much because you had no idea it happened. Then once you realize it, it's somewhat of a mess that has to be undone.

Sarah: Yes. Out of curiosity, you mentioned that those late night/early morning commercials use a loophole because it's not solicitation because they're encouraging you to reach out and you mentioned the healthcare affairs. I'm curious, do you know if there is any push for more regulation in the government in order to put stricter measures or stricter oversight on those types of either events or advertisements?

Scott: Absolutely there is. It's something that's a constant discussion at the government level to try to implement more countermeasures to combat the fraud waste and abuse that occurs, especially with medical identity fraud. When I use the reference about the solicitation, and that is for like durable medical equipment those types of commercials, and that durable medical equipment could be anything like I said back braces, any kind of orthotics, power wheelchairs, ventilators, things of that nature.

There are standards and rules in place that those types of healthcare providers have to follow. One of 'em is about direct solicitation, so that's an example of how they have found a loophole or found a way to get around some of the regulations by putting the commercials out there, and then you call them. They usually have a go-between, an arbitrator, or a third party connecting you to someone that potentially is a fraudster to do those types of services. That's how they get around that.

They're constantly trying to put rules in place to do those things. There's also some organizations **[unintelligible 00:09:20]** say a Medical Identity Theft Alliance has been trying to figure out ways to escalate this type of crime when they do catch fraudsters this way and impose stiffer penalties when they get the convictions as well. It's something that's an ongoing, as most of the fraud arena, once you get ahead of something, you're having to constantly shift or pivot because once you put countermeasures in place, they figure out other ways to defraud these types of programs.

Sarah: Yes. That makes sense. I feel like every year, around June or July, I see a big story from the Department of Justice about their big Medicare, Medicaid fraud round up that year or cracking down. Every year that I've seen that, that big press release of, oh, I can't even remember how many millions or even maybe billions that they managed to catch in these different roundups but it grows every single year. Each year it's the largest amount that they've captured. I've noticed a lot of it having tie-ins like you mentioned the durable medical equipment, but it just seems like a really rich area for fraudsters to prey on vulnerable people that need it and are desperate. If they're offered a potentially-- what seems like it might be an easy way to access that, necessity takes over I think sometimes red flags when you're in that situation.

Scott: Yes. Oh, absolutely. Going back to the beginning of the conversation, I think one of the things that the general public doesn't realize is that about $3.6 trillion is spent on healthcare in the United States, that's based off of 2018, 2019 statistics.

They're usually a little bit behind. We could probably estimate anywhere from 3.6 to $4 trillion spent on health care here in the country. That's why it's such a lucrative area for fraudsters to really target from a financial standpoint because approximately, the federal government and law enforcement agencies along with the Department of Justice estimate up to about 10% of that cost is potentially or fraudulent, which is around $300 billion. If you consider that, it's a significant amount of money out there of losses for these programs, and for private health insurers. Approximately, 2.5 to 3 million of the people impacted by that kind of fraud are from medical identity theft.

Sarah: Wow. You talked a little bit before about how one of the things that makes this so insidious is also the fact that it can grow in the shadows, and you might be a victim of medical identity theft for years without knowing until you go in for treatment, or something happens. Or you might find out, you said from the explanation of benefits or being contacted by a debt collector. Is there any way that people can be more proactive to try? I know that for regular identity theft, there are some **[inaudible 00:12:54]** through your bank or through credit reporting that you can check your credit report. You can use different consumer services to maybe you put a credit freeze. Is there any way that consumers can stay one step ahead, potentially, of medical identity theft?

Scott: Absolutely. There's a lot of things similar to regular identity theft like protecting your personal information, your name, social security number, date of birth, those types of things. Then to take it a little step further, when you're talking about medical identity theft, is you need to make sure that you protect your health insurance enrollment forms when you're enrolling annually when you're making your adjustments to maybe your health insurance, or if you're in Medicare or Medicaid. You protect all of your personal information because those documents have a lot of personal information that can be used to commit fraud in your name when you're unknowing about it.

The health insurance cards that you might have issued, especially, from a private insurance company, that it's not from a federal fund but also your Medicare cards, for those that are in those programs or Medicaid cards. You need to protect those just like you would a credit card or your driver's license. Your prescriptions and prescription bottles that you have, you destroy those in the same fashion as that you would if you were shredding important documents that may have sensitive information on it along with billing statements from your doctors or your medical providers. Those are some things that you really want to make sure that you protect while you're doing that.

Then you've mentioned and I've spoken about the explanation of benefits statement from your health insurance company or from Medicare or Medicaid. When you get those you really want to make sure that you are protecting those as well because it has a lot of identifiers on those documents that can be utilized for that. Then you might check your credit report and look to see if regularly. That's always a

suggestion from traditional identity theft, looking for things for credit cards that may have been opened in your name.

You might see things out there as well, from a medical standpoint of you might have some debt collection from a hospital or from another healthcare provider for services that it never had rendered to you, and you had no idea were out there because somebody had used your information to get those services. Those are just some common things, and just the general, you should never ever give your information out to just anyone. It should be your healthcare provider that you know. Or if you're in a hospital setting, obviously, you're going to be there for that. You would expect that you're going to share that information so that they can get paid for the services but you need to make sure you know who you're giving that information to before you give it out.

Sarah: That makes sense. I feel like that's just good practice for literally everything now that we've been in the information age for quite some time. It really, in every aspect of life, it feels like information and data really is the most valuable currency. It's so important to make sure that you have control over who you're sharing that with, and that you have a good handle on who has access to it, too. It seems like medical data is just as important as you might consider llike you had mentioned, social security number is linked to both. Also making sure that that Medicare, Medicaid number for your account and that type of stuff that you have a lock on it, basically. What are some of the potential impacts of medical identity theft on patients?

Scott: Other than the financial impact, I think that the only other thing from my perspective that I think is really serious is really from a physical aspect of the medical insurance fraud as a result of patient misidentification could lead to serious repercussions in some senses. If someone else is getting services with your information all along, and then you go to get the services, there could be a lot of inaccuracies in your health data and it potentially could be life-threatening. If the person that has stolen your data was actually getting services and maybe they had conditions that you don't have or vice versa, you could end up getting diagnosed wrong. There could be delays in treatment, inappropriate care.

Then you also run the risk of having the data of an imposter being merged with your real-world data and then it becomes a mess for your electronic health records.

The ramifications will continue to grow but overall, the physical threat is you have a potential problem that you could be given the wrong type of prescription or drugs if you had a drug allergy. It could be potentially life-threatening. I think that's probably the most important thing before the financial part is that it could be something that could grow and turn into a catastrophic nightmare if it's not something you pay attention and make sure that you're not a victim of.

Sarah: Obviously, having your identity stolen and losing money and having to fight to try and get any of that back if you can is terrible, but that is no comparison to losing your life or getting permanently maimed or losing a loved one or having them suffer like you said, life-threatening consequences. Or even just ongoing quality of life consequences because of wrong data, puts it all in perspective and also I think underscores how important this issue is to combat. I am encouraged to hear that there's continued pushes for more regulation on these types of things and crackdowns and all of that and that it's being taken as seriously as it should be, it seems. If someone thinks that they're a victim of medical identity theft, what options do they have for recourse? Is there a certain body that they should report it to? Is there anything that they can do in addition to reporting it, to try and mitigate any negative effects from it?

Scott: Certainly, from a Medicare or Medicaid standpoint, as well as private health insurance, there's several agencies that combat this. The one that we primarily work quite a bit with is the Department of Health and Human Services Office of Inspector General. They have a fraud hotline, you can get that information on their website, oig.hhs.gov fraud hotline and you could make reports that way, and then those complaints go and they're triaged. Then, of course, they're investigated by the Office of Inspector General and then various contractors that they have working under that guise.

Also, from a state standpoint, individual states have a senior Medicare patrol, and these senior Medicare patrols, they assist lots of people that are in the senior communities with doing things like not just reading your explanation of benefits and helping you understand your medical documents and things. They also help you to identify maybe when you've been taken advantage of in a certain way, or you potentially could be a victim of medical identity theft. They help you to try to deal with some of those things before your life becomes disrupted. The Federal Trade Commission also is a entity that you can contact their consumer advice division under the Federal Trade Commission. They have a pretty robust program to combat medical identity fraud, as well as identity theft as well.

Sarah: That's really good to know, and really important information I feel like to share with anyone and everyone basically. Going back a little bit earlier to talk about the schemes themselves, I'm just curious that for the past two years, we've been in a huge global pandemic. I know that we've seen lots of stories actually come out about maybe COVID testing sites that weren't regulated properly, or they were fly by night operations, people selling bogus cures, and targeting vulnerable people with those.

I guess this is a two-part question. First part, do you think that we will see an explosion of medical identity theft as a result of all of this increased focus on healthcare that everyone has needed to access? Also, the second part of that is, do you foresee any further upcoming trends in that arena of how COVID might have affected medical identity theft?

Scott: Absolutely. I think that the pandemic as it's related to the coronavirus or COVID 19 has been probably one of the worst catastrophes at least in my career of creating more healthcare fraud and that relates to medical identity theft as well. Traditionally, in the past, when they've had some-- what the government refers to, or the Department of Health and Human Services refers to as catastrophe, it's usually things like a hurricane or storms or things which we're all familiar with all over the country if you go back to like Katrina or hurricane Ike, or even hurricane Sandy on the East Coast, there was always an impact from that.

It was just usually geographic and it was based on the demographics of just a small impacted area of the country. The pandemic has impacted the entire country. I think probably within the next year to two years, you're going to see really the overall impact of the fraud that's coming out of it because we really haven't been able to identify how bad the exposure's been. As it relates to medical identity fraud, there already have been,--they've already identified, as you mentioned earlier, they have the fraud takedowns and there is a healthcare fraud strikeforce that is in place.

It's made up of multiple agencies, the FBI, the Office of Inspector General under the Health and Human Services, the Department of Justice, Medicaid fraud control units and state's drug enforcement agency, and various other law enforcement agencies that are all put together looking at that. Some of the things that they've already identified is false advertisements for COVID 19 testing and treatments. A lot of this is through social media. Also, false testing sites that really they're offering to do the testing, but really what they end up being is they're scammers that are selling fake and unauthorized tests.

They're also using those as a setup to get your information, to obtain your insurance information, or for Medicare and Medicaid recipients and beneficiaries, get at those identification as well so they can bill for other services. Some of the schemes that have been coming out of it from those federal programs, you're looking for things where they go for a COVID 19 test then you see thousands of dollars of other testing that is not even really related to COVID 19, like genetic testing, drug testing for like opioid usage, which you wouldn't think would be common for somebody that say is a Medicare beneficiary. You look at the schemes or the exposure.

It's just interesting that everyone goes in for a COVID 19 test to see if they've contracted the virus and then they're getting multiple other services that just, for example, we might talk to the beneficiaries or interview the patients that were billed for it. They thought they were just getting a test for the coronavirus. They had no idea they were being tested for other services or had no idea that there had been other services billed. They weren't aware of that. You're going to see probably a wave as it's starting to unfold as we start to get back to some normalcy I think. You're also going to see some things where people are going to hold onto this information.

Like I said, they get it and they sit on it for a little while, you think that you're fine t1en the next thing you know, that information's been sold to fraudsters, and then you might be impacted years down the road, and you had no idea that your information was compromised. We're going to have to monitor that and there's going to have to be some efforts to look for those types of activities.

Sarah: It's bleak to think about, but it seems inevitable that we're going to be feeling the impacts of medical identity, and healthcare fraud in general that arose, and new types of schemes that weren't something that were possible before the pandemic with large-scale testing, like you mentioned, and then running a bunch of other tests. We're going to just keep seeing the effects of that, unfortunately, for years and years to come. One last question. That's if there's a fraud examiner who's working on a case, they might not be a healthcare fraud examiner or specialized in that area. They're working on investigating another type of fraud case and they start to see evidence that suggests that medical identity theft is involved in that case. Do you have any advice for them of what next steps to take or who to-- I know that you mentioned different the Department of Health and Human Services, OIG, or state agencies, but when they're in the course of the investigation, do you have any advice for resources for them to turn to?

Scott: I think my number one advice would be going back to I would report it immediately if they suspect it or see signs that it potentially, that's what it could be to Health and Human Services Office of Inspector General, or even their local law enforcement because they'll all lead back to the Health and Human Services tips line or hotlines. Even if you're sure about it, it's good to report that. Have a discussion or a dialogue with the experts related to the health and the healthcare fraud industry because more than likely, it potentially could be something, or it could be something new that hasn't been recovered or hasn't been identified yet.

Sarah: Well, thank you so much, Scott, for joining us today.

Scott: Thank you for having me today.

Sarah: Thank you for listening. You can find this podcast in all ACFE *Fraud Talk* episodes on iTunes, Spotify, or wherever you get your podcast. I'm Sarah Thompson signing off.

[00:30:41] [END OF AUDIO]