Episode 9 – Licensee Scams

Intro music: 0:00

Podcast Introduction: 0:10

Hello, and thanks for joining me. I'm Jean Fisher Brinkley, Communications Director for the North Carolina Medical Board, and this is MedBoard Matters.

I don't know about you, but it seems that every time my phone buzzes, it's someone trying to scam me. Maybe my amazon order is on hold until I update my credit card information. Or my Netflix account has been hacked and that means no more Schitt's Creek until I create a new password.

It's getting so bad the next time my sister texts I'm going to ask her what the password is.

In all seriousness, scams are everywhere. On this episode of MedBoard Matters we are going to talk about a specific type scam that targets our licensees.

The North Carolina Medical Board has been hearing from physicians and PAs about this scam for at least the last two or three years. Every time we think that it has surely run its course, there's another round of activity. The latest prompted the Office of North Carolina Attorney General Josh Stein to issue a consumer alert in March to warn licensed medical professionals about this con.

The medical board has posted alerts on its website. We've run articles in our newsletter. And we have warned licensees about scams on social media. Now we are dedicating an episode of our podcast to the topic of scams.

Interview with Pat: 1:30

JFB: I've asked our Chief Investigative Officer, Pat Berckmiller, to offer licensees some guidance on how to recognize scammers and how to avoid falling victim to them. Before coming to the North Carolina Medical Board, Pat retired from the Federal Bureau of Investigation as a Special Agent after nearly 30 years of service. He has also worked with Blue Cross Blue Shield as an Investigator. Pat, welcome so you are a retired FBI agent who, if I recall correctly, has experience catching bad guys who run these types of scams. Could you talk a little bit about your background in this area?

PB: Hi Jean, thanks for having me and yes, over my law enforcement career with the FBI, I worked many years on cyber related crimes involving mostly business email compromises and other sophisticated fraud related scams where the losses amounted in the millions of dollars. These scams often would involve the acquisition of funds through various means through like things like payroll, wire transfers and even executive level schemes.

JFB: OK, well it is nice to have an in house expert. I think most of us would like to believe that we can instantly recognize a scammer, but in the heat of the moment when someone's got you on the phone and they're telling you there's some sort of urgent problem that you need to deal with right away, it's not so easy. So, I wondered if you could talk about some of the red flags that might be present that could alert someone that they're dealing with a scammer.

PB: Sure, so when it comes to scams involving our licensees, they'll often receive like a phone call many times that their practice, or when they're already busy seeing patients, or in the midst of their work and the caller will create a scenario where two things are going to occur. The first thing is going to be a sense of urgency. And the second thing is going to be an action that they need them to take in the urgent situation that they have created. These are the two biggest red flags that we see and when the story is presented quickly, the goal is to make them act so fast that even a highly intelligent person presented with these facts can be taken advantage of in that exact moment. The fabricated scenarios will involve usually pieces of information about the licensee, which are often obtained from social media or other public sources to make them even more believable. It may include things like information about your practice, such as names of your staff members, your national provider identifier, or your NPI number. And always remember that scammers are known to call businesses after hours to listen to your recorded out of office messages on your phone extensions to gain additional information.

JFB: Wow, that's fascinating. I had no idea it was that sophisticated. So, what should a physician or PA do if he's on the phone with someone who claims to be with the medical board? Because that's the scam that we've been hearing about most recently. Is someone calls up and says they're an investigator with the medical board or with law enforcement, but they reference some problem with their medical license. Often, it's suspended, and they need to pay a fee to reinstate it. So, what should they do?

PB: I would say that one of the first things that you want to do is buy yourself some time. So again, there's a sense of urgency that is going to be created in that initial call to you. Buy yourself time by delaying a response by saying, “I need to check up on this, hold on, I'll get back with you. Can you give me your callback number? You know, make an excuse that you're in the midst of seeing somebody you know you have another meeting that you have to go to the. Get a callback number. We don't want you to call the number actually back, but just obtain the number. Again, that gives you the time to think about the scenario and to not move forward with them.

JFB: OK, now should the licensee call the medical board?

PB: Yes

JFB: Just say, “hey, I just got a call from someone who says they work for you.” Is that a good thing to do?

PB: Yes. So, the best thing to do would be to call our main number and at any time we can verify not only the authenticity of the name of the investigator that you've had contact with, or a staff member, but we could verify the purpose. And again, looking up on the website publicly, you can check your own license as well as we can provide that information to you as well.

JFB: Now, sometimes scammers will threaten that the FBI or the DEA is on its way to the medical practice to arrest the physician, or PA or shut down their practice or do something awful to try to scare the licensee into paying them. What should a licensee do if this happens?

PB: So, we have heard of one of these types of scenarios being presented to our doctors and PA's and this is an immediate red flag. Remember, the ultimate goal of all of these scams is to obtain money. And no legitimate law enforcement agency will ever demand any payment in a criminal investigation. That's

just not how it works. I would say call their bluff. Tell them to stop by the office, but do not give in to any demand for payment or provide any personal information in the course of that conversation.

JFB: OK, it occurs to me that one of the things that allow scammers to use a, you know, medical b oard investigation to manipulate our licensees, is the fact that most physicians and PA's don't really know how a real medical board investigation works. So, if you know how the actual investigative process works, you should know in theory that the circumstances the scammers are describing just aren't possible. I wondered if you could talk with me about the investigative process and the laws and the rules that govern it so that people might be better able to spot red flags.

PB: Sure. It's really important to understand that the medical board actually follows the law, and we have specific rules that govern how we conduct our investigations. For example, we're required by law to notify all of our licensees who are under investigation. This happens really at the very beginning, and we do it in writing, so you will actually receive a document from us, or an investigator will present that document to you. It actually details the complaint that has been made against the licensee and you are never going to get a call or a letter from us that says your license has been suspended. This will not never be the first time that you're going to be hearing from us. You're going to be hearing about the complaint at the very onset of when the complaint was made, and additionally, our investigators would never ask you for money or to pay any fine to keep your license from being suspended.

JFB: OK, I think that's really important because that key process if someone contacts the licensee, I just want to repeat it, if someone contacts a physician or a PA and says your license has been suspended, you should be very suspicious, because as you just said, that is not how the medical board process works. It is never going to be the case that your license has been suspended without you knowing that you're under investigation and without you having the chance to defend yourself or respond to whatever inquiry may be underway. So, let's see, we have mentioned that licensees who are approached by one of the licensing board scammers, that they should report it to the medical board. I just want to say for clarity's sake that NCMB obviously does not have criminal powers and we can't open an investigation. So why do we ask that licensees notify the board?

PB: That's a great question. We do want to hear about the scams because it keeps us informed of how their changing. These scams will always be altered to fit the particular audience. And if we're aware of a change in how a scam is being implemented, these are the kinds of things that we can push out to our licensees to let them be aware of a new trend that we're seeing. And again, we'll always identify the legitimacy and the identity of any call made by our staff.

JFB: Right. Now, we've been talking about phone scams in particular, but the medical board has seen scammers use other approaches too. So, what are some other examples for our licensees to be on the lookout for?

PB: There are a lot of scams out there if your cell phone number has been obtained, which is actually not very difficult in today's day and age. And we've seen a lot of attempts via text messages for people to click on links. Remember that any phone number can be spoofed, and we know that these scammers now are using the North Carolina Medical Board's name and telephone number, which is going to display on your caller ID, again, add that sense of legitimacy to this. Oftentimes it will include a board

investigator's name and or phone number in the body of the text message, but not necessarily involving the link. The scammer may have you on the phone, it creates that that sense of urgency to get you to click on that link. The link is essentially going to be malware which will contain a keystroke logger which will capture everything that you type, and they're seeking that one thing, which is your username and passwords to your accounts. Just remember that even one letter difference in an email address that you were expecting to receive, such as having to "Vs" next two a "W", when you look at it very closely, can make it look like you're receiving something from a legitimate email address, but once this information is obtained, the scammer will no longer be contacting you because the keystroke logger is already installed.

JFB: OK, so they've got what they wanted.

PB: Exactly. So, I have really 2 tips here and one is to never recycle your password amongst your accounts. And always use multi factor authentication with any account that offers it and before clicking on a link in a text message, always verify with the actual sender.

JFB: OK, now one that I have seen involves a letter you know that is either mailed or faxed to the licensee's is medical practice usually. Often that will be an official looking letter head, you know that says North Carolina Medical Board. Can you say anything about that approach and what they may be asked to do?

PB: Sure, and keep in mind that our seal and our logo, of the North Carolina Medical Board are widely available on the Internet. So, keep in mind that these can always be recreated in any type of false documentation. So, I go back to if you are suspicious of a letter that you receive in the mail, always verify directly with us by calling our phone number, not the phone number that is listed on that letter, because that obviously will not go back to us.

JFB: Right, right and I guess I'll probably say this multiple times during this episode, but again, you know the Medical Board's website is www.ncmedboard.org, not.com, so make sure you go to the correct web website and get phone numbers and information from that website rather than anything that is sent to you. If you go looking for it, that's one thing. It's probably legitimate. If somebody offers it to you freely, you need to ask questions about is this real? Well thank you so much Pat for that information. You really do have to be so careful these days. I really appreciate you being here. Is there anything else that you'd like to add that I haven't asked about that you think would help our listeners?

PB: I would just say that…I'd like to reiterate the best protection that we have against the majority of all these scams is to spread the word. Tell others not only in your professional group of colleagues, but your friends and family members as well. These people prey on citizens outside of the medical profession as well.

JFB: OK wonderful. Well thank you again.

PB: Thank you.

Red flags practice: 13:21

JFB: Now, we are going to practice spotting some of the red flags Pat talked about. How? Well, I just so happen to have a recording of a scam telephone call. I want to stop here and give a huge thank you to Carren Mackiewicz for making this recording. Carren is Legal Operations Manager for the North Carolina Medical Board and she was at work when her phone rang. Carren noticed that the caller ID on her office phone indicated it was the NC Medical Board calling. Since she was at the office of the North Carolina Medical Board at the time she knew that an internal call wouldn't show up on the Caller ID that way. Suspecting that it might be a scam call, she used the voice recording app on her smartphone to capture her conversation. We're going to play clips from that recording, and I'll point out the red flags along the way.

CM: Hello, this is Carren.

Scammer: Yea, hi Carren…a very good afternoon. This is Justin Scott from state medical board and I'm looking for Dr. [Bleep].

CM: Um, can I ask what this is regarding?

Scammer: Yea, it regards about her state practice license number.

CM: OK, what medical board are you calling with?

Scammer: State medical board from North Carolina.

JFB: OK, first red flag. The caller gets the name of the agency he is supposedly calling from wrong. First, he says he is calling from the state medical board. When Carren asks him to repeat his affiliation he says, "state medical board of North Carolina". The correct name of the agency is the North Carolina Medical Board. Let's hear a little more.

CM: OK, so you work for the medical board in North Carolina?

Scammer: Mmm-yea, I am an officer of state medical board. My badge ID is KA-9089.

CM: You're an officer with the state medical board in North Carolina?

Scammer: Yea…you're right…yea.

Carren: And what's your telephone number?

Scammer: You can see on my caller ID.

JFB: There's the second red flag. When Carren asks the caller to confirm where he is calling from, he directs her to look at her caller ID. That's a clue that this scammer is using what's known as spoofing technology to make it appear that he is calling from the North Carolina Medical Board. Of course, Carren already knows that he's not calling from the medical board, but she keeps him talking.

CM: And what do you do for the North Carolina Medical Board?

Scammer: I am an officer of state medical board.

CM: And what do you do for them? What do you do as an officer for the North Carolina Medical Board?

Scammer: I's investigate…

CM: What do you investigate?

Scammer: Listen to me…I ahmmm Chief Investigating Officer of state medical board, ok?

CM: You're the Chief Investigating Officer for the North Carolina Medical Board?

Scammer: Ya…you're right…ya.

CM: OK…um, their website doesn't have you as the Chief Investigating Officer of the North Carolina Medical Board.

JFB: There's actually no red flag in this clip. I just want to highlight that Carren references the North Carolina Medical Board website. This is one way to challenge the information a scammer provides to you. Of course, some organizations don't list the names of their employees on their website, so in most cases you'd probably want to call the organization directly. Make sure you don't call any number the scammer gives you because it's going to connect you with another scammer – look up the number on your own. So, Carren and the scammer go back and forth a bit and the scammer's starting to get frustrated that she won't let him talk to the doctor he's trying to con.

Scammer: Yah, so can you please transfer my call to Dr. [Bleep]?

CM: Um, no I can't transfer you until you tell me what you need to talk to her about.

Scammer: See….miss..ok, you don't want to transfer my call? Ok…can you lend me your fax number so that can I…send a suspension letter to Dr. [Bleep]? Because you are wasting my time and Dr. [Bleep]'s time.

CM: Um…no sir.

JFB: See how the scammer shifts gears here? Carren won't transfer him so he falls back to plan B, which is to fax over a phony suspension letter. Again, never call a telephone number or visit a website provided to you on such a letter. Go to the medical board website on your own to find contact information and verify the identity of anyone who has called you.

Eventually, the scammer realizes he is not going to get what he wants, and he hangs up. Not today, scammer. And Carren, nicely handled.

Resources and wrap up: 18:08

Let's say you've already fallen victim to a scam. Hey, it happens to the best of us.

Depending on the situation, there may be several things you can do to protect yourself.

First, consider reporting it. Again, the North Carolina Medical Board does not have jurisdiction over scammers, but the state Attorney General does. You can report a scam to North Carolina Attorney

General Josh Stein's consumer hotline toll free within North Carolina at 1-877-5-NO-SCAM or (919) 716-6000.

Keep in mind that scams like the ones we have described on this podcast are notoriously hard to investigate because there is so little information to go on. Still, keeping law enforcement aware of the latest tricks and trends in scams helps raise awareness.

Next, if you have given a credit card number or other financial information to a scammer, you'll want to immediately notify the credit card issuer and report it as lost or stolen. In addition, you may wish to put a temporary credit freeze on yourself with the three credit bureaus to prevent scammers from opening new accounts in your name.

Be aware that you will be unable to obtain instant credit, obtain a loan or request a credit report until you notify the credit bureau to lift the freeze. Find information on how to request a credit freeze on our podcast show page on the medical board website, www.ncmedboard.org

If you believe that you may be a victim of identity theft and that someone is using your information to open new accounts or make purchases, visit www.identitytheft.gov to get help with a personal recovery plan.

One last thing, and it probably goes without saying, but stay vigilant. Once scammers have your contact information – your phone number, your fax number, your email address – they are going to keep using it. And they are going to sell the information to their scammer friends who are also going to come for you.

The next time someone contacts you with an urgent problem and pressures you to take immediate action, remember that scammers win when they convince you to act before you think. So slow down, remember the red flags and hang up the phone, or hit the delete button.

That brings us to the end of another episode of MedBoard Matters. I hope you found it helpful. As always, if you have questions or comments, you can send them to us at podcast@ncmedboard.org

Thank you for listening, and I hope you will join me again.