**Physician Targeted Scams**

The Board has sent several email warnings about scams targeting physicians and other medical professionals. The scams keep on coming, so this is another.

We know that some of you are reading and heeding the notices, because several licensees have quickly contacted us to let us know that they’ve been targeted. Thank you to those alert physicians who have helped us get the word out!

Most recently, on a May morning we heard from three different licensees. That scam presented as a caller posing as a Board of Medical Practice Investigator. Other scams have featured criminals posing as DEA or FBI agents. Sometimes they may be by telephone, but scammers may also use email or texts. Just this week the DEA contacted medical boards asking for assistance spreading the word about a con using a letter sent by email on June 23, 2025, purporting to be from the DEA and addressed to “Dear Registrant.”

The bottom line is that we all need to be cautious as we deal with the many emails, texts, and calls we receive each day. Sadly, it seems that physicians and other health care professionals are often targeted – you are busy, your rights to practice and to prescribe are important to you, and you have resources. You are also accustomed to having to quickly respond to many pressing issues over the course of the average day. And it might be more than just a thief who’s trying to trick you into paying a bogus fee. It could be a criminal trying to get you to click on the wrong link as part of an effort to plant ransomware on your hospital’s EMR system.

**How do you protect yourself**?

For one, remember that these scams are often designed to take advantage of a person's fear of getting in trouble with a regulatory or law enforcement agency and to prompt action before you can think about the situation or seek advice. It is possible that any medical professional could receive a legitimate call from a regulatory body or law enforcement agency, so you can’t ignore communications just because of the risk of scams. However, you can avoid being a victim if you remember one important lesson:

* **The Board (and other government agencies) will never contact you by telephone, text, or email to demand that you immediately pay money, or provide account information or protected personal information.**

Do we sometimes send letters to licensees about an administrative financial penalty, or to ask them to provide us information? Yes, we do, but it will never be a demand to **act immediately**. No legitimate regulator or law enforcement agent will force you to respond immediately and without the opportunity to confirm their identity.

Many of these contacts are by telephone. If a call seems suspicious, we recommend the following:

* Ask the caller to provide you with their name and the telephone number of the Board office (or other agency) so that you can call back. Sometimes that is enough to make them give up and they will just hang up.
* If they give you a number, **do not call back the number that you are given**. If you want to check with the Board, get the number from a reliable source. Our main office line is 802-657-4220. And remember that you cannot rely on caller ID to confirm that a call is coming from our office – scammers are able trick caller ID into showing a legitimate number.

Most of these scams begin with telephone calls, but there may also be text messages, emails, and faxes. **Don’t reply to a text or use a link in an email**. Also, don’t be fooled by official-looking documents. Some victims receive information allegedly detailing aspects of an investigation that feature letterhead, seals, stamps, and water marks of government agencies, as well as publicly available information such as the victims' National Provider Identifier numbers, license numbers, and business address. Your best protection is always to contact the agency that is purported to have sent the communication.

**Reporting**

Reporting a suspicious incident to us will allow us to put out an alert to Vermont licensees.

Other reporting options include:

* The local FBI Field Office. Licensees in Vermont should call the FBI Field Office in Albany, NY at (518) 465-7551. For other states check online at: https://www.fbi.gov/contact-us/field-offices.
* For online scams, you can report to the FBI’s Internet Crime Complaint Center at <https://www.ic3.gov/>.
* The Federal Trade Commission’s ReportFraud site at: <https://reportfraud.ftc.gov/>. The reports to the FTC are made available to law enforcement agencies.

The proliferation of fraud schemes is frustrating and annoying. As with other threats to your health, safety, and privacy, the challenge is to remain vigilant and make it a habit to always follow safe practices.