LAW ALERT

September 7, 2021

By: Andrew T. Garbarino, Esq.

RMF
RuskinMoscouFaltischek P.C.
Smart Counsel. Straight Talk.

An Old Voice Phishing Scam Has Been Retrofitted to Target Physicians

New York physicians are now receiving calls from individuals identifying themselves as investigators from the "New York Medical Board" in a retread of a classic identity theft scam.

For years, "voice phishers" have engaged in cold calls while masquerading as law enforcement officers. These callers typically tell people that their fingerprints or DNA have been found at a crime scene – usually on the "Texas-Mexico border" – or that a package with drugs, money or both has been intercepted *en route* to the person called. In order to avoid arrest as a suspect, the imposter will demand confirmation of their identity, including social security numbers and other personal information.

These scammers bank on creating enough stress and worry that their call will shock someone into "cooperating" by providing the information demanded. Once obtained, the identity thief can use that information to open credit cards, loans, utilities accounts or even obtain government identification like a driver's license.

The scam targeting doctors is similar in that the "investigator" claims that the doctor's medical license is being suspended due to involvement in "opioid trafficking on the Texas-Mexico border". The call comes from the 518 area code and looks like an Albany-based government phone number.

The fake investigator will then email or fax a letter on what appears to be state-agency letterhead to the physician that accurately includes the physician's name, professional license number and home or office address. There are some oddities within the letter that signal its faked origin, but at first glance, it can appear pretty real.

After the physician has had an opportunity to review the letter, the investigator will explain that he will be conferencing in an "FBI agent" to ask her a few questions. The agent will then proceed with the confirmatory questions described above, while including medical-industry related information.

This scam should serve as a reminder of two things:

First, identity thieves and cybercriminals operate on volume. The great majority of physicians targeted would likely have either seen through this or immediately contacted an attorney for help. But these scam artists bank on hitting the less than 10% who, for whatever reason, may be overcome by fear and indulge the imposters.

Second, physicians are particularly attractive to identity thieves because, in addition to obtaining personal data that may be exploited for financial gain, a physician's identity may be used in an attempt to obtain access to prescription medications, medical services and DME. The additional information that may be stolen from a doctor is worth exponentially more to an identity thief.

No one should ever give out personal information to a caller unless that caller can be definitively identified. Moreover, whenever a physician receives contact from legitimate law enforcement, the best course is to seek immediate counsel.

For more information, please contact:

Andrew T. Garbarino, Esq.
(516) 663-6632
agarbarino@rmfpc.com