HINSHAW

Alerts

Physicians Beware: Identity Theft Is On The Rise

June 4, 2014
Health Law Alert

The California Medical Association (CMA) has issued an alert to physicians, warning them that they are at risk of being the subject of a tax scam. The CMA has received reports from physicians that fraudulent federal income tax returns have been filed using physician names, addresses and social security numbers. In many cases, the fraudulent tax return includes the name of an unknown person listed as the physician's spouse. Generally, this other name is a prior patient of the physician.

A physician who is a subject of the scam may learn of the scam in various ways. They may receive a 5071C letter from the IRS alerting them of possible fraud. In other instances, they may receive a rejection notification when attempting to electronically file their taxes because someone has used their social security number to file a false return.

These scams are not limited to California. Medical associations in a number of states, including Arizona, Connecticut, Indiana, Maine, Massachusetts, Michigan, North Carolina and Vermont, have found that their members are reporting more cases of fraud than in the past. In some instances, the fraudster files the false return to claim a large refund. In other instances, the information is used to open financial accounts and obtain loans, or to obtain employment. The IRS and Secret Service are conducting an investigation into the source and extent of the tax fraud scam. Although tax fraud scams have long existed, this appears to be more targeted than in the past.

When physicians learn that their identity has been or may have been compromised, we advise that they immediately take the following actions:

Internal Revenue Service (IRS). Contact the IRS through its identity theft website or by phone and advise IRS staff that the return is false and that the physician did not file the return. Physicians who receive an IRS 5071C letter should also notify their tax preparer, because they may not be able to electronically file their returns this year. If they file a paper return, they should attach an IRS 14039 Identity Theft Affidavit describing what happened along with copies of any IRS notices concerning the scam. Physicians who did not receive an IRS 5071C letter, but believe that their personal information may have been used fraudulently, should call the IRS Identity Protection Specialized Unit. Additional information is available on the IRS website.

Attorneys

Michael A. Dowell

Office of the State Attorney General. Physicians should also make a written complaint to their State Attorney General's office. In California, the Attorney General's website has a form called "Application for Registration as Identity Theft Victim" which can be completed on line or printed and mailed and faxed to the AG's office in Sacramento. In Illinois, the Attorney General has a toll free hotline "Identity Theft Hotline" at**:** 1-866-999-5630 **or** 1-877-844-5461 (TTY) which offers one on one assistance. In addition, the Illinois Attorney General's website includes an Identity Theft Complaint form. Physicians can fill out this form on line or can print out and complete the form and mail or fax it to the Attorney General. Additionally, both the California and Illinois Attorney General websites have a great deal of helpful information.

Federal Trade Commission (FTC). File a report of the theft with the FTC, either online via the FTC's website or by calling the FTC. If reporting on online, print a copy of the report. This report, along with a police report, constitutes an Identity Theft Report, which the physicians will need for the IRS and may need for financial institutions as well. The FTC also provides helpful information (including sample letters) on its website.

Police Report. File a report with the local police in the jurisdiction where the physician resides. File the report in person and bring all available documentation, including copies of all state and federal complaints filed as well as personal identification, such as a driver's license. Be sure to obtain the police report number and/or a copy of the police report.

Social Security Administration. Call the Social Security Administration's fraud hotline at 800-269-0271 to report fraudulent use of Social Security Numbers. Request a copy of the Personal Earning and Benefits Estimate Statement from the Social Security Administration at 800-772-1213, and check the report for accuracy.

Credit Reports and Bank Accounts. Take steps to protect various financial accounts, such as filing a fraud alert with one of the three credit reporting agencies (Equifax, Experian or TransUnion) and obtaining credit reports. If you notify one of these three companies, they are required to notify the other two companies. The initial fraud alert is good for 90 days. Contact each of the three credit reporting companies and order a free copy of the credit report. Ask each company to show only the last four digits of the physician's Social Security Number on the credit report. Other steps include placing a credit freeze on any existing credit cards, and changing banking and checking accounts. If specific accounts have been tampered with, contact each credit card company, bank or other financial institution, speak with someone in the fraud department to report the fraud, and follow up in writing with a letter sent by certified mail with return receipt requested.

Additional Information. Physicians may also consult the U.S. Department of Justice (DOJ) website for additional information, including checklists about identity theft and fraud.

Tracking of Procedures and Documenting Your Steps

Addressing identity theft requires a systematic approach. Physicians should: maintain a timeline, keeping track of important dates, including when they sent items, whether they received a response, dates for follow-up and any reporting deadlines; keep written documentation of all calls, including phone numbers and the names of individuals with whom they spoke; send documents by certified mail, return receipt requested; and keep copies of all documents.

Hinshaw & Culbertson is experienced in assisting clients concerning identity theft issues and we are happy to assist you in notifying the agencies and filing the reports described above. Should you need assistance or need further information on these issues, please contact Michael A. Dowell (mdowell@hinshawlaw.com), the health care partners in our Los Angeles office at 310-909-8000, or your regular Hinshaw attorney.

This alert has been prepared by Hinshaw & Culbertson LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship.