Steps physicians should take if in danger of identity theft

Identity theft has become increasingly common as the prevalence of Internet and other non-face-to-face transactions have proliferated. This resource offers steps physicians should consider taking if they learn that their credit card, checkbook, Social Security number (SSN) or other confidential information that could enable impersonation has been lost or stolen. **These steps are in addition to the obvious steps of canceling, closing or otherwise dealing with the compromised credit card(s) or bank account(s).** Unfortunately, physicians faced with potential identity theft must be vigilant concerning both their personal finances and ways someone may impersonate them as a physician.

Your financial welfare

With respect to your financial welfare, you can find extensive information at **www.ftc.gov/idtheft**, the Federal Trade Commission's (FTC) identity theft Web site. In brief, the FTC suggests individuals take the following steps when personal information has been compromised:

1. Place a fraud alert on your credit report.

If the stolen information includes your Social Security number (SSN), call the toll-free fraud number of any one of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. This alert can help stop someone from opening new credit accounts in your name.

- **Equifax:** 1 (800) 525-6285; **www.equifax.com**; P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1 (888) EXPERIAN (397-3742); **www.experian.com**; P.O. Box 2002, Allen, TX 75013-2002
- **TransUnion:** 1 (800) 680-7289; **www.transunion.com**; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

An **initial fraud alert** stays on your credit report for 90 days. When you place this alert on your credit report with a nationwide consumer reporting company, you will receive information about ordering one free credit report from each of the companies. It's prudent to wait about a month after your information was stolen before you order the report. This allows time for suspicious activity to show up on the reports. Once you receive your reports, review them for suspicious activity, such as inquiries from companies you haven't contacted, accounts you didn't open and charges on your accounts that you can't explain. Verify that the information included on the report—SSN, address(es), name or initials and employers—is correct. If needed, you may also file an **extended fraud alert**, which stays on your credit report for seven years.

2. Be watchful for the signs of identity theft.

Monitor your bank and credit card statements, mail, e-mail, phone calls and other communications for suspicious activities, such as:

- accounts you didn't open
- charges on accounts that you can't explain

- fraudulent or inaccurate information on credit reports
- failure to receive bills or other mail

  Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his or her tracks.
- receipt of credit cards for which you did not apply
- credit denials
- offers of less favorable credit terms
- calls or letters from debt collectors or businesses about merchandise or services you didn't purchase

3. Consider signing up for a credit monitoring service.

If you are offered free credit monitoring by a company that has experienced a security breach, you should consider accepting this offer. Credit monitoring from a reputable company can help you quickly detect any misuse of your information.

4. File an identity theft report if your information is misused.

File a report about your identity theft with the police, and file a complaint with the FTC. Visit **www.ftc.gov/idtheft** to file your complaint and access "Take Charge: Fighting Back Against Identity Theft" for detailed information on other steps you can take in the wake of identity theft.

Your professional identity

With respect to a physician's professional identity, there are also several steps you should consider to protect against someone filing fraudulent claims or writing improper prescriptions in your name:

1. Medicare enrollment

The Centers for Medicare and Medicaid Services (CMS) strongly recommends that physicians confirm there have not been any improper alterations to their enrollment information and that they update their enrollment information at **https://pecos.cms.hhs.gov**, the Provider Enrollment, Chain and Ownership System (PECOS) Web site.

Another way to help avert identity theft is through the use of electronic funds transfer (EFT). All physicians new to Medicare or re-enrolling are required to receive their reimbursement through EFT. EFT payments require a bank account for funds to be electronically deposited to. Generally establishing this account entails completing paperwork that is controlled by the physician or physician's practice, the authentic owner of the account. Using EFT is a deterrent for an identity thief to establish a different bank account the thief controls, as can easily happen when paper remittance payments are intercepted. Any time you reduce the number of paper checks coming through the mail, you reduce the likelihood of those being intercepted and used inappropriately.

2. Medicaid enrollment

You should also consider contacting your state Medicaid fraud unit to report potential identity theft so your state Medicaid program can flag efforts to open new offices or payment addresses in your name.

3. NPI enrollment

Similarly, you may wish to confirm the accuracy and currency of the information associated with your National Provider Identifier (NPI). Visit **https://nppes.cms.hhs.gov** to confirm that your NPI has not been improperly altered.

Note: The Freedom of Information Act requires CMS to make publicly available the content contained in the "Other Provider Identification Numbers," "License Number" and "Employer Identification Number (EIN)" fields. **Do not** report your SSN or the SSNs of other health care providers in these fields. If you need assistance in deleting inappropriately reported SSNs, contact the NPI enumerator at (800) 465-3203.

Remember that the law requires you to keep the following NPI information current by updating changes within 30 days: full name; mailing address, including zip code and associated telephone number; location address, including zip code and associated telephone number; date and place of birth; gender; medical license number(s) and issuing state(s); the name, title and phone number of the person authorized to change the physician's data; and the name, telephone number and e-mail (if available) of the person to be contacted if there are questions about the initial application or any changes to the data.

Finally, if your identity is stolen, you should notify the National Plan and Provider Enumerator System (NPPES) immediately. Although your NPI is intended to be permanent, the NPPES is authorized to deactivate NPIs and issue new ones in the case of identity theft and other limited circumstances.

4. Vigilance

You should instruct your staff to monitor strange activity, such as:

- calls from physicians, pharmacies or other health care providers that involve unknown patients, unlikely prescriptions or other orders
- suspicious health insurer remittances
- communications for patients that you have not seen

The AMA advocates that upon the identification of a security breach involving physicians' social security numbers or other confidential data, health insurers should:

- immediately notify physicians of the security breach
- offer free credit monitoring and adequate identity theft insurance, from more than one company, for at least five years
- publicly report confirmed cases of identify theft linked to the security breach
- provide legal protection and indemnification to physicians for any losses that result from the security breach

The AMA also advocates that the personal information of physicians and other health care practitioners be stored electronically only in encrypted form to reduce the likelihood for future breach and loss of data.

Be sure to notify the American Medical Association (AMA) and your state medical association or national specialty society regarding any potential security breach of your personal data so these organizations can advocate on your behalf and the behalf of other physicians who may have been affected by the security breach.

Questions or concerns about practice management issues?

AMA members and their practice staff may e-mail the AMA Practice Management Center at **practicemanagementcenter@ama-assn.org** for assistance.

For additional information and resources, there are three easy ways to contact the AMA Practice Management Center:

- Call (800) 262-3211 and ask for the AMA Practice Management Center.
- Fax information to (312) 464-5541.
- Visit **www.ama-assn.org/go/pmc** to access the AMA Practice Management Center Web site.

The Practice Management Center is a resource of the AMA Private Sector Advocacy unit.