FOX BUSINESS
THE POWER TO PROSPER

August 13, 2014

How to Spot and Prevent Medical Identity Theft

By: Cathleen McCarthy

While credit card breaches at retailers are grabbing headlines, identity thieves are quietly homing in on an even more lucrative area: health insurance and medical records.

More than 1.8 million people in the U.S. were victims of medical identity theft in 2013, according to a survey by the Ponemon Institute released in September. That's a 19 percent increase over the previous year. "Medical identity theft is the fastest growing component of ID theft," says Drew Smith, founder and CEO of InfoArmor, a provider of business-to-business identity theft solutions.

The latest case involves the alleged theft by Chinese hackers of 4.5 million medical records from Community Health Systems, a company that runs 206 hospitals in 29 states. Thieves stole records including names, addresses, birth dates, telephone numbers and Social Security numbers.

Like any type of identity theft, medical ID theft can damage your credit and cost you hours of hassles trying to clear it up. But it could also endanger your life if incorrect information appears on your medical records.

Why the bull's-eye? Health information is easier to hack than credit. In April, the FBI issued a private industry notification warning to health care providers that their data networks are not as robust as those in the financial and retail sectors, and "the possibility of increased cyberintrusions is likely."

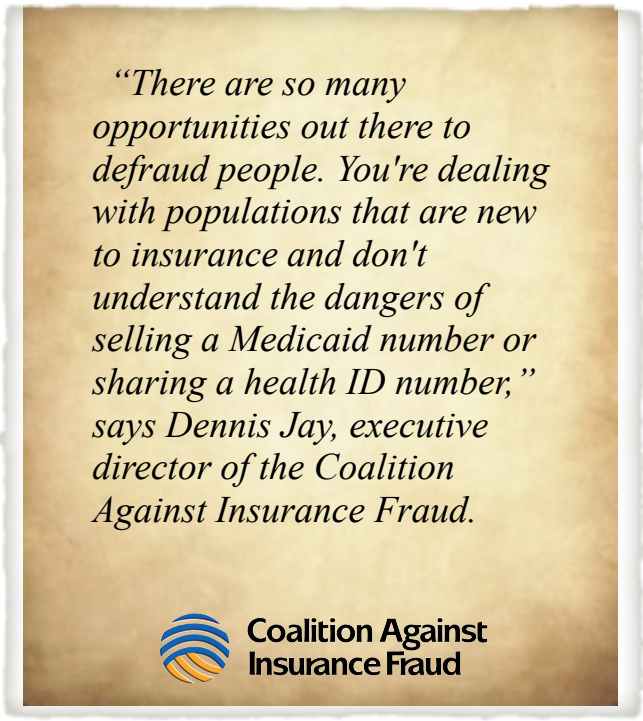
Safeguards are in the works, but the move to electronic records and the health exchanges set up under the Affordable Care Act, otherwise known as Obamacare, have opened new opportunities for fraud, both online and off.

Experts say Americans can expect to see medical fraud heat up again in the months before open enrollment for 2015 government-subsidized insurance begins in November 2014.

Your medical ID: black market gold

Why would hackers bother with health insurance when they could get a direct line to your pocketbook via credit cards or financial accounts? "It's very lucrative," says Ann Patterson, senior vice president and program director at the Medical Identity Fraud Alliance. "Stolen protected health information can be monetized for a much greater value than traditional financial account information."

A complete medical identity -- including name, address, phone number, Social Security number, medical insurance information and access to medical records -- is worth about $50 on the black market, says Michael Bruemmer, vice president of Experian's Data Breach Resolution group. "Without medical or insurance information, that drops to about $10 for someone's stolen information."



New fraud opportunities courtesy of Obamacare

Obamacare and the expansion of Medicaid have opened up a whole new stream of opportunities for fraudsters, experts say. In June, a backpack was discovered on a street in Hartford, Connecticut, near the Access Health CT exchange. Inside were four notepads containing the Social Security numbers of 151 people enrolled in Connecticut's Obamacare exchange.

"There are so many opportunities out there to defraud people," says Dennis Jay, executive director of the Coalition Against Insurance Fraud. "You're dealing with populations that are new to insurance and don't understand the dangers of selling a Medicaid number or sharing a health ID number."

Just before the rollout of Obamacare, roving gangs began knocking on doors in lower-income neighborhoods, requesting health information they said was needed to expedite the new health plans. "People gave it out," Jay says.

View the entire article. View other articles quoting the Coalition Against Insurance Fraud.