The Philadelphia Inquirer

September 2, 2013

Beware of health-insurance scams under ACA

By: Robert Calandra, For The Inquirer

Confused is the word many Americans are using to describe the Affordable Care Act.

An August survey from the Kaiser Family Foundation found that 51 percent of Americans who responded still don't understand how the law will affect them. Confusion is highest among Hispanics (64 percent), the uninsured (62 percent), and young adults (62 percent). And that makes them fertile ground for fraud and scams.

"Confusion is a crook's best friend," said James Quiggle, communications director at the **Coalition Against Insurance Fraud** in Washington.

In ACA fraud, the key objective is your medical record.

"In the scammers' world, medical records are called 'fulls,' " said Sid Kirchheimer, author of Scam-Proof Your Life (Sterling, 2006) and AARP's Scam Report. "They are the holy grail of scamming because they have all the information that a scammer needs. They can really clean up."

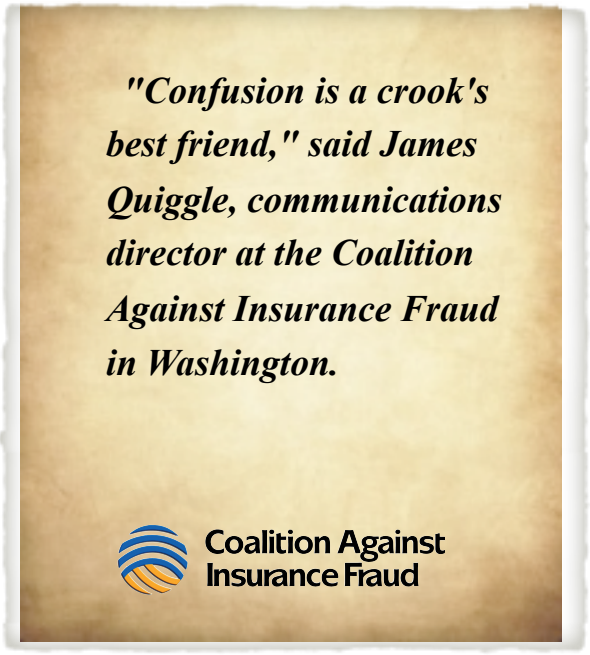
That's because medical records contain your financial and insurance information. So an enterprising fraudster with a "full" can drain your bank account and run up credit cards while filling fraudulent prescriptions and getting a facelift. That's why "fulls" sell for $50 and Social Security numbers go for a dollar or two on scammers' websites (yes, they have websites) and the black market, Kirchheimer said.

With the act about to expand coverage to millions, the two biggest scams now circulating, he said, are people selling fake insurance and posing as a government employee.

The fake-insurance deception is usually done on the phone. The thief calls to sell you health insurance on the online marketplace at a discount. All he needs is your bank account number to set up direct withdrawal. Of course, you can't buy any insurance on the marketplace until it opens Oct. 1.

But it sounds legitimate because agents and brokers are allowed to assist people in enrolling for coverage. Legitimate agents or brokers will identify themselves and acknowledge any link to an insurer. Agents and brokers don't have to show clients the full range of insurance available, but they must tell people about the online exchange.

Crooks are making calls and even going door to door, posing as government employees for agencies such as the Department of Health and Human Services and Medicare. The marks - that would be you - are told they are among an initial group of Americans selected to receive the new ACA insurance card. To get it, all you must do is provide your Social Security and bank account numbers. The caller may also ask for a Medicare number, which is the same as your Social Security number.



The ACA does not require an identification card.

"We are going to warn people," said Laura Line, corporate assistant director for health care at RHD, a Philadelphia nonprofit that works with many uninsured clients. "You don't take cold calls and give people your personal information. That is not how we operate."

Online, scammers are setting another kind of trap: look-alike websites. Thieves are buying similar-sounding domain names and designing sites that look official. They often contain links that, if clicked on, install malware on your computer, giving scammers access to your information.

The federal government has only one official health-care website: healthcare.gov.

"Sometimes scammers use dot org, dot com, or dot net," Kirchheimer said. "Those are the telltale signs of a scam. If it's a state agency, it will have a dot gov URL."

But not always. In Pennsylvania, where the federal government is running the exchange, the official health-care website is a dot com.

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