Bankrate.com

September 18, 2013

Beware of identity theft tied to Obamacare

By: Chris Kissell, Bankrate.com

In October, millions of Americans are expected to begin shopping for health plans on Obamacare's federal and state-based health insurance exchanges.

But this new opportunity to purchase coverage also may open a door for identity theft.

Some criminals already have set up phony websites intended to lure unsuspecting applicants into giving up vital personal information. Others may try to infiltrate the ranks of health reform "navigators," paid helpers who will guide consumers through the health insurance purchase process.

In all cases, a scammer's goal is to obtain your Social Security number, medical information, bank account identifiers and credit card information, says James Quiggle, spokesman for the **Coalition Against Insurance Fraud** in Washington, D.C.

"The first months of health reform's launch will be prime time for scammers," he says. "Just one consumer's info could be a gold mine for identity thieves."

Thieves smell an opening

Quiggle says identity thieves likely will try to exploit weaknesses in security and fraud measures at both the federal and state levels.

Right now, officials charged with setting up health exchanges are "running a nonstop wind sprint" to put highly complex operations into place by Oct. 1, Quiggle says. The federal government is running the show for 34 states, while the other 16 plus the District of Columbia will operate their own exchanges.

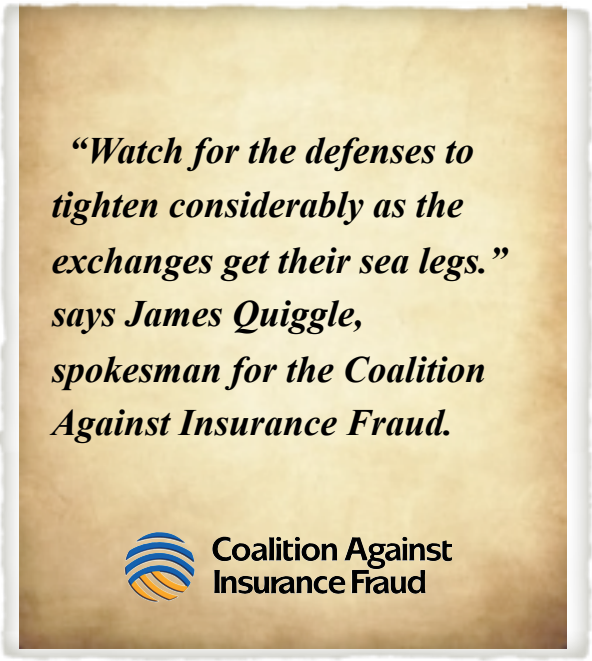
"Some exchanges may be focused more on getting a robust operation going before they make anti-fraud defenses their top priority," he says.

Recent federal budget and staff cuts are compounding the problem, he says. According to news reports, the cuts are forcing the federal government to scale back its investigations of health care fraud and abuse. The potential pitfalls for consumers shopping for health care coverage worry Eva Casey Velasquez, president and CEO of the Identity Theft Resource Center in San Diego.

Bogus websites sprout up

"Our biggest concern is the scammy websites," Velasquez says.

For years, criminals have used fake websites to dupe people into wiring money or applying for loans, she says. Now, crooks are establishing bogus health insurance exchange sites to lure consumers into giving up personal information.



"This is just one more tool that they can use," Velasquez says.

Consumers may be especially vulnerable to such scams because starting next year they will be required by law to have health insurance, making them more likely to click on a questionable link, she says.

For criminals, "the return on investment is going to be high, because again, people are being compelled to do this," she says.

Quiggle says several official-looking fake exchange websites already have been shut down.

Fraudsters play 'navigators'

Another aspect of Obamacare -- its deployment of health navigators -- also could open the door to identity theft. These experts, being hired nationwide, will help health insurance shoppers determine if they are eligible for federal subsidies, and guide them through the process of purchasing a plan.

Some criminals likely will pose as navigators to prey on people looking for help, Quiggle says. He suspects these scammers will be very polished and will carry forged credentials that look authentic.

Other crooks may try to become officially certified as actual navigators so they can fleece consumers, he says. Quiggle worries that officials charged with hiring an army of navigators in a short time will not be able to properly vet