December 7, 2015

Medical ID theft going mobile?

Scammers looking to hack mobile phones for patient medical info.

By: James Quiggle, Coalition Against Insurance Fraud

Mobile phones may be the newest emerging battleground in combating widespread heisting of people's medical identities. Two recent reports provide telling evidence.

More than 25 million people will have their medical and/or personal info stolen from their health providers between now and 2019, says a new report by Accenture. That's one of every 13 patients.

Mobile transactions form the newest arena for ID theft in general, adds a report by IDology. The report focuses on broader ID theft, with some healthcare organizations taking part. Still, it's a warning of emerging vulnerability for healthcare providers – and their patients.

Some 8 percent of polled organizations report rising mobile scamming this year, up from 3 percent last year. Spoofing, account takeovers and device cloning are favored tactics.

"Fraudsters have become quite skilled at exploiting the many nuances that accompany mobile devices — from the millions of change events to the increasing ability of fraudsters to attack mobile technology with methods similar to what we found in these survey results — porting, spoofing, cloning and more," IDology says.

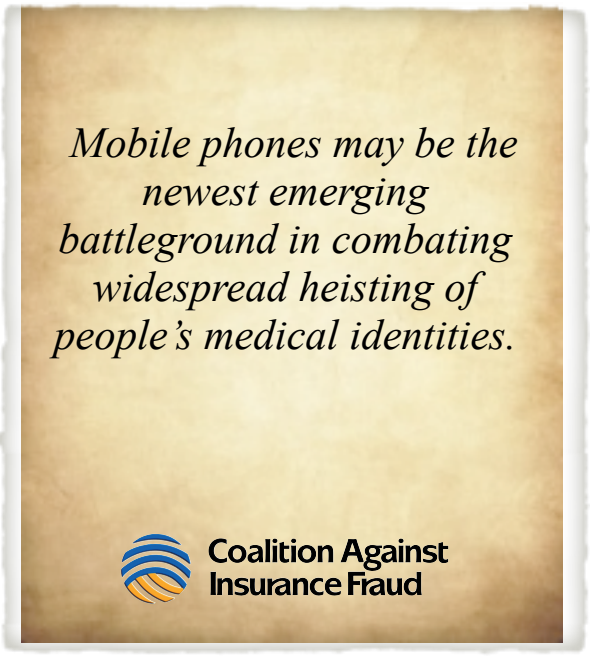
More organizations plan to invest in mobile-based transactions, yet nearly half say they lack resources to properly manage mobile security, IDology says.

"Mobile fraud has become increasingly top of mind for businesses as the use of smart devices gains in popularity and usage. With the convenience of smart devices being able to access a consumer's personal accounts across multiple industries, security is becoming more and more of a priority for organizations of all sizes," IDology says.

It takes only a small leap to see how mobile hacking and security will increasingly become next big fraud problem for the healthcare industry and their patients.

Mobile transactions are rapidly becoming prime portals for healthcare transactions. Just Google "health care mobile devices." You get 46 million hits.

HHS also is warning healthcare organizations about mobile security. We're looking at a double security problem. The vast digital highway of healthcare records and record sharing, combined with a growing migration of everyday transactions to mobile devices.



With the healthcare sector accounting for nearly 43 percent of data breaches — the highest percent — the U.S. healthcare sector remains the largest target for sophisticated hackers. The 80 million records stolen in the famous Anthem breach drives that point home poignantly.

Health records are far more valuable to black marketeers than standard credit card info. Each record can easily command up to $50 in sale value compared to $1 or so for credit-card info. Why? Health claims can steal many thousands of dollars before they're discovered and shut down. Credit card scams often are discovered and stopped in real time.

Nearly 2/3 of consumer victims each pays an average of $13,500 out of pocket to clear up the mess, says an earlier report by Ponemon Institute. That also can siphon hundreds of hours. Nearly half of frustrated patients will find another healthcare provider if they learn their personal records were hacked. The cumulative cost to breached providers will reach $305 billion by 2019, Accenture adds in its analysis.

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