Senior Identity Theft: A Problem In This Day And Age

by Robin Slade of FraudAvengers

The May 7th Federal Trade Commission (FTC) Senior Identity Theft: A Problem in This Day and Age panelists related that seniors are often preferred targets, especially for medical identity theft. Fraudsters, who may include unscrupulous relatives and/or caregivers, view these individuals as more trusting, less financially sophisticated and less likely to report the crime because they fear family members may think they cannot maintain their independence.[1] Panel members discussed the many still unanswered questions regarding how to prevent tax and government benefits fraud, medical identity theft, and identity theft in long-term care, and how to reach older consumers.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Individuals are the only ones with the detailed knowledge of their medical care or financial expenditures who can raise the alarm when they do fall victim, it is essential for consumers to learn the true impact of these crimes and how to protect themselves as best they can and raise the alarm when it is needed.

In addition, system practices continue to make personally identifiable information (PII) available in ways advantageous to criminals. For example:

-

Social Security Numbers are used on Medicare insurance cards.

-

HIPAA rules intended to protect patient privacy also prevent victims from gaining access to their records to correct them.

-

Healthcare providers have been implicated in the vast majority of crimes and may choose not to help the victims at all.[2]

-

94% of US healthcare organizations studied have had critical PII data breaches and 45% of these organizations showed five or more breaches during the study period.[3]

-

Three out of five providers studied, including major hospitals and healthcare providers, do not have the policies and procedures in place to safeguard health records.[4]

-

More than six in ten healthcare organizations studied say they do not have enough resources to ensure data security.[5]

We know that medical identity theft and fraud cost the healthcare industry $41 billion in 2012and cost taxpayers and consumers in higher premiums and healthcare costs and has life-altering consequences for patients and their families, so the attitude that resources cannot be dedicated to data security indicates a lack of understanding regarding the true value of the PII.

In financial identity theft, the financial institution may make the individual financially whole again â€“ not so for medical identity theft victims. We are seeing some success in which insurance companies are some of the most proactive players, as are federal government investigation units and law enforcement. And Medicare has assisted patients by simplifying EOBs and providing some consumer education. The public/private consortium, the Medical Identity Fraud Alliance, is leading the current opportunity to include all ecosystem stakeholders in developing cost effective technologies, policies, and best practices that we need to lessen patient exposure to fraud and theft.

_____

[1] National Crime Prevention Council, 2012.

[2] The majority of medical identity theft occurs with provider and sometimes patient complicity, though in some cases provider licenses are stolen or data breaches provide the information needed to commit these crimes. World Privacy Forum, 2013.

[3] Ponemon, Third Annual Benchmark Study on Patient Privacy & Data Security, 2012.
[4] Ibid.
[5] Ibid.

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow ACCESS