The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches

April 2010

The consequences of medical identity theft to consumers can be severe. According to a national Ponemon Institute survey on Medical Identity Theft, 55% percent of respondents had to make out-of-pocket payments to a health plan provider or insurer to restore coverage and 48% lost their healthcare coverage.

An estimated 1.4M Americans were victims of medical identity theft in 2009.[1] While this number is only 5% of all reported identity theft incidents, medical identity theft is expected to increase dramatically as new federal regulations defined in the Health Information Technology for Economic and Clinical Health (HITECH) Act provide incentives for healthcare providers to quickly move medical records online.

Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous.

As a matter of fact, more than 50% of fraud victims didn't discover that they were a victim until at least a year after the incident(s) occurred.[2] Conversely, this percentage of victims indicates there is a significant population of consumers who are victims… and are still not aware of it!

This nascent form of identity theft can no longer be ignored. A breach of personal health information (PHI) can have a significant negative impact on clients, customers and on the ongoing health of a business.

Impact to the Consumer:

Unfortunately, by the time medical identity theft is discovered, the damage has been done. Forty percent of consumers say that they found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that thieves incurred in their name. As a result, the consequences of medical identity theft are frequently severe, stressful and expensive to resolve.

According to a 2010 Ponemon survey, the average cost incurred in trying to resolve a medical identity theft incident is more than $20,000.[3] Additionally, 55% of survey respondents had to make out-of-pocket payments to the health plan provider or insurer to restore coverage and 32% experienced an increase in their health

1 National Survey on Medical Identity Theft Prepared by Larry Ponemon, February 22, 2010.

2 The Ponemon Institute in February 2010.

3 National Survey on Medical Identity Theft. Prepared by Larry Ponemon, February 22, 2010.

insurance premiums. The effort to resolve the crime and restore an identity can also be extensive. Seventy four percent of those surveyed consumers say that the effort to resolve the crime and restore their identity was significant or very significant. In addition to the cost, consumers say the most immediate impact included mental anguish or embarrassment.[3]

Business Impact:

The effects of a breach of PHI can be devastating to a business, organization or institution both financially and to their coveted customer relationships. According to Ponemon Institute research, the average expense incurred for a company to address a medical data breach is $211 per record. Additionally, the research indicates that those companies that do not closely follow the new regulatory requirements established through the HITECH Act can incur damages and fines of up to $1.5M.

Damages go beyond the associated costs and potential fines in managing a data breach. The negative impact also manifests itself in losses to consumer trust, confidence and loyalty. As a matter of fact, over 70% of respondents surveyed trust healthcare providers such as hospitals, clinics and physicians to protect their PHI.[4]

Should this trust be broken the impact on a healthcare provider's bottom line could be severe. Fifty five percent of consumers responding to a Ponemon study strongly agree that the medical identity theft caused them to lose trust and confidence in health care organizations. Another 2009 study indicated that of those who were severely injured by a data breach, such as a breach of PHI, over 50% of them switched their business to a competitor.

Conclusion:

Even the most resource-rich healthcare providers experience data breaches. Healthcare organizations are faced with the challenge of how to protect the healthcare data that they handle and be within the compliance standards defined by the HITECH Act and HIPAA. Given the breadth and depth of the potential damages and consequences, the need for education, preparedness, and programs to address data breaches is clear.

To learn more about data breach resolution, visit www.experian.com/databreach, or contact Experian® at databreachinfo@experian.com or 1 866 751 1323.

4 Ponemon Institute, "Electronic Health Information at Risk." October 15, 2009.

5 Americans' Opinions about Healthcare Privacy, Ponemon Institute, January 31, 2010.

6 "Using Triage to Ease the Pain of Customers At Risk," 2009 Javelin Strategy and Research.