Journal of Consumer Education, 29, (75-79), 2012

http://www. cefe/illinois.edu/JCE/archives/vol29.html

Medical Identity Theft

Whitney Walters
School of Family and Consumer Sciences, Eastern Illinois University

Axton E. Betz
Eastern Illinois University

The purpose of this position paper is to provide information on medical identity theft. Secondary purposes of this paper are to describe signs of victimization, consequences of victimization, and how to recover from medical identity theft. An additional secondary purpose is to describe how individuals can protect themselves from becoming victims of medical identity theft. More robust public policy need to be developed. And, more educators in the fields of consumer education, business and finance along with those from economics and family services need to develop detailed lessons and programs on medical identity theft and its effects on the individual, families and communities as a whole.

Journal of Consumer Education (2012) **29**, (75-79).
http://www.cefe.illinois.edu/JCE/archives/vol 29.html
Published online September 2013

Keywords: identity theft, prevention, consumer education
JEL: G01, G28

INTRODUCTION AND OVERVIEW

Identity theft occurs when personal information is stolen and used for another's financial or other personal gain (Cullen, 2007; Sullivan, 2004). Nine million new cases of identity theft are reported each year (Federal Trade Commission, n.d.). Many cases of identity theft involve obtaining loans in a victim's name; these cases are considered cases of financial identity theft (Schmidt & McCoy, 2005).

When consumers think of identity theft, their first thought is typically of financial identity theft. However, a 2006 report by the Federal Trade Commission (as cited in Sullivan, 2009) stated that medical identity theft accounted for at least 250,000 of the reported cases of identity theft between the years of 2001-2006. Although financial identity theft and medical identity theft are related in that they both involve one stealing another's personal information for means of financial or other personal gain, medical identity theft differs from financial identity theft in that medical identity theft is limited to the healthcare field (Sullivan, 2009). Thieves will use another individual's personal and health information to obtain prescription medication, personal medical treatment and even surgery. They may also use the information to send in false billing statements to the victim's health insurance provider in an effort to make a financial profit (Federal Trade Commission, 2010).

The purpose of this position paper is to provide information on medical identity theft. Secondary purposes of this paper are to describe signs of victimization, consequences of victimization, and how to recover from medical identity theft. An

additional secondary purpose is to describe how individuals can protect themselves from becoming victims of medical identity theft.

SIGNS AND CONSEQUENCES OF VICTIMIZATION

One indicator of being a victim of medical identity theft is receiving medical billing statements or debt collection notices for treatment or services that were never personally received. Another indication that one may be a victim of medical identity theft is being denied health insurance or plan benefits due to false medical statements claiming reports of a health condition that the victim was never diagnosed with (Federal Trade Commission, 2010).

A significant problem with medical identity theft is that a victim may never know their information has been stolen and used for this crime. This creates the problem of misdiagnosis. If a victim is unaware that someone has been using their information to be treated for conditions that the victim does not have or to obtain medical prescriptions that the victim does not need, this can lead to inappropriate medical diagnoses, and injuries or even death (Federal Trade Commission, 2010).

Furthermore, a possible consequence of medical identity theft that many do not realize is employers may disregard potential employees who show a record of severe health complications that could cause risk or financial cost to the company. Because many employers do not explain their exact reasons for denying employment, one may never know that this was due to an inaccurate medical history. Also, an erroneous medical record could cause public officials or those running for office to have embarrassing, public issues. For instance, if someone were to test positive for HIV or AIDS or other STIs but had done so using a public official's name and private insurance information; this could cause for a media scandal during candidacy (Schmidt & McCoy, 2005).

The emotional consequences that a victim of medical identity theft may suffer from may be same as those of any other identity theft crime. Emotional reactions to identity theft include anger, fear, loss, and anxiety (Betz, 2012; Cullen, 2007; Identity Theft Resource Center, 2007). It has been reported that some victims of identity theft have even committed suicide (Sullivan, 2004). Victims often experience physical consequences as well, including heart palpitations, hyperventilation, dizziness, sweating, high blood pressure and muscle aches, and sexual dysfunction (Identity Theft Resource Center, 2009).

RECOVERING FROM MEDICAL IDENTITY THEFT

There are things that one can do to recover upon discovering that they have become a victim of medical identity theft. The first thing a victim should do is file a report with the Federal Trade Commission (Federal Trade Commission, 2010). This can be done online at https://www.ftccomplaintassistant.gov or by calling them at 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261. The next thing a victim of medical identity theft should do is to file a police report with the local police department. An important step to always remember when filing reports is to always make and secure copies of the information. Also, one needs to keep a log of all conversations they had about the crime and record all

dates and times that the conversations took place. One should send copies of the police report to all health care providers and insurance companies.

An additional step a victim can take in recovery is to place a fraud alert on their credit report (Federal Trade Commission, 2010). This action can help prevent any future financial accounts associated with the medical identity theft from being reported on the victim's credit report. Contact only needs to be made to one of the three credit reporting agencies (Equifax, Experian, & TransUnion). The one contacted is required by law to notify the other two credit bureaus so that all three reports will have a fraud alert placed on them.

One final step toward recovery that victims of identity theft can make is by filing a "security freeze" or "credit freeze" on their credit reports (Federal Trade Commission, 2010). This essentially freezes ones credit and blocks access to potential creditors; it serves as a warning. In some states anyone can put a freeze on their account but in other states, it is a service provided only to those who are identity theft victims. Before applying for credit after the freeze is in place one must first call and lift the freeze. This can be time-consuming and in some instances can cost money.

PREVENTING MEDICAL IDENTITY THEFT

There are many methods of prevention. Some of the basic methods of preventing oneself from becoming a victim of any type of identity theft include shredding any documents that contain personal information that are no longer needed. Be sure to shred any documents that have any financial, medical, or includes insurance or other benefit information. Keep any and all personal documents containing such information stored securely, such as in a lockbox. Personal computers need to be protected with secure passwords. Also, personal computers need to be protected with anti-virus software in an effort to prevent hackers from gaining personal information (Cullen, 2007). It is extremely important to protect one's Social Security number (SSN) and limit who receives this information. If one does decide to share their SSN, they must first ask why the company needs the information and how that company plans to secure their information and ask about any privacy policies that may help protect them. Lastly, one of the most proficient protection methods against identity theft is simple self-education. Self-education on company privacy laws, current identity theft trends and prevention methods are key (Cullen, 2007).

There are two agencies that primarily provide security for consumers' medical information. One of those agencies is the United States Department of Health and Human Services (DHS). The other agency is that of the Federal Trade Commission. DHS oversees the Health Insurance Portability and Accountability Act (HIPAA). This act's primary purpose was to allow employees to keep their health insurance while changing employers. However, a side benefit of the act was that the Administrative Simplification section of the act directed the Secretary of Health and Human Services to "establish security specifications for the electronic exchange of medical information " (Sullivan, 2009; p. 657). This section also established penalties for wrongful disclosure of such information.

CONCLUSION

With every protective measure enacted regarding medical identity theft, there are still discrepancies and loopholes. These are the very discrepancies and loopholes identity thieves prey on and victims suffer as a result. With regard to medical identity theft, more attention needs to be devoted to consumer education and more robust public policy need to be developed. Too many consumers are oblivious to the fact that medical identity theft is even possible; let alone how to protect themselves from becoming a victim. More educators in the fields of consumer education, business and finance along with those from economics and family services need to develop detailed lessons and programs on medical identity theft and its effects on the individual, families and communities as a whole. Most consumer education course texts do not discuss medical identity theft. If we are not educating the younger generations about this issue, consumers will continue to be vulnerable to this crime.

More needs to be done with regard to public policy to protect individuals from becoming victims of medical identity theft. Along with laws that protect victims more policies need to be developed that help victims gain access to their insurance and medical records more easily and command health providers and companies to work with the individuals on correcting the matters and preventing them from happening again.

References

Betz, A.E. (2012). *The experiences of adult/child identity theft victims.* (Unpublished doctoral dissertation). Iowa State University, Ames.

Cullen, T. (2007). *The Wall Street Journal complete identity theft guidebook.* New York: Three Rivers Press.

Federal Trade Commission (n.d.). *About identity theft.* Retrieved October 21, 2007, from http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

Federal Trade Commission. (2010). *Medical identity theft.* Retrieved January 23, 2011, from: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.shtm

Identity Theft Resource Center. (2007). *Identity theft: The aftermath 2006.* Retrieved November 28, 2007, from http://www.idtheftcenter.org/artman2/uploads/1/The_Aftermath_2006_2.pdf

Identity Theft Resource Center. (2009, December 4). *ITRC fact sheet 108 - overcoming the emotional impact.* Retrieved May 30, 2010, from http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_108_Overcoming_The_Emotional_Impact.shtml

Schmidt, S. & McCoy, M. (2005). *Who is you? The coming epic of identity theft.* Urbandale, IA: The Consortium.

Sullivan, B. (2004). *Your evil twin: Behind the identity theft epidemic.* Hoboken, N.J.: John Wiley & Sons.

Sullivan, K.M. (2009). But doctor I still have both feet! Remedial problems faced by victims of medical identity theft. *American Journal of Law and Medicine, (35),* 647-681.