THE ROLE OF THE FORENSIC ACCOUNTANT IN A MEDICARE FRAUD IDENTITY THEFT CASE

Maria Sanchez, Rider University

ABSTRACT

Identity theft is a rampant problem in the United States. It occurs when one's personal information is stolen for the purpose of impersonating that person, making unauthorized purchases, taking money from bank accounts, opening new lines of credit with the stolen information, or using that information for other financial gain. According to a recent survey by the Javelin Strategy and Research Center, at least one in ten people have been the victim of identity theft. Forensic accountants and fraud specialists can help to prevent, detect and prosecute identity theft. This study examines a case of identity theft involving Medicare fraud. The role that the forensic accountant may play in the prosecution is discussed. The forensic accountant is important in these types of cases because the financial trail must be traced and will lead back to the criminal. The forensic accountant also has the important job of preparing the evidence exhibits for the prosecutors to use in court.

JEL: M40, M49

KEYWORDS: forensic accounting, Medicare fraud, identity theft

INTRODUCTION

Identity theft is a huge problem in the United States. Some estimates indicate that one in ten people have been the victim of identity theft. It occurs when one's personal information such as social security number, drivers license number, etc. is stolen for the purpose of impersonating that person, making unauthorized purchases, taking money from bank accounts, opening new lines of credit with the stolen information, or using the information for other financial gain. According to the nonprofit organization Identity Theft Resource Center (www.idtheftcenter.org), identity theft can include check fraud, credit card fraud, financial identity theft, criminal identity theft, governmental identity theft, and identity fraud. According to the Department of Justice, identity theft often relates to cyber intrusions, health care fraud, mortgage fraud, and credit card fraud, but it can also be a significant element of violent crimes such as domestic abuse and even terrorism (U.S. Department of Justice, 2010). The Identity Theft and Assumption Deterrence Act of 1998 strengthened the criminal laws governing identity theft and makes identity theft a federal crime.

In 2010, identity theft was the number one complaint to the U.S. Federal Trade Commission (FTC, 2011). To understand how to prevent identity theft, it is important to understand how identity theft occurs. This study will take a detailed look at a case involving a massive alleged identity theft fraud involving the U.S. Medicare system, one of the largest Medicare frauds to date. The fraud was allegedly conducted by an Armenian-American crime ring who used stolen doctor and patient identities. The stolen identities were used to file reimbursement requests to Medicare for procedures that were not performed. From 2006-2010, the crime ring allegedly submitted over $100 million in fraudulent bills to Medicare based on the stolen identities, and received over $35 million in reimbursements (Rothfeld, 2010).

The remainder of the paper is organized as follows. I first define identity theft and present several examples of identity theft. Then, I review the prior literature and discuss common Medicare frauds. Then the case of the $35M Medicare fraud is detailed. The role of the forensic accountant is then described. Finally, I discuss the implications of the paper, with conclusions and suggestions for future research.

Identity Theft

There are many forms of identity theft. Identity theft is when one party steals another person's personal information for the purpose of impersonating that person and or using that information for personal gain. Common instances of identity theft are cases when one's credit card or checking information is stolen and used by another person. This is extremely common today and in fact, even the Chairman of the Board of Governors of the Federal Reserve System has fallen victim to this type of identity theft! In 2009, twenty one people were charged with participating in a wide ranging identity theft ring. The members of this ring stole victim's identity through several different methods, including stealing mail and pick-pocketing. One of the many victims of this crime ring was Fed Chairman Ben Bernanke and his wife. His wife's handbag which contained a family checkbook, credit cards and identification was stolen from a Starbucks in Washington, D.C. A week later, the criminals then tried to deposit one of the Bernanke's checks for $900 into a fraudulent account (Markon and Irwin, 2009). Prosecutors estimate that this identity theft ring netted more than $1.2 million before they were arrested.

In 2008, the Boston U.S. Attorney's office announced that eleven people were indicted for stealing more than 40 million credit card and debit card numbers. The perpetuators hacked into the wireless computer networks of several retailers, including Marshalls, T. J. Maxx, BJ's Wholesale Club, OfficeMax, Barnes & Noble and Sports Authority to steal credit and debit card numbers, passwords and account information. Some of the credit and debit card numbers were sold on the internet. The others were used by the hackers to withdraw tens of thousands of dollars from ATMs. The U.S. Justice Department and the Secret Service conducted an undercover operation to bust this fraud ring for three years, leading to the indictment in 2008 (Verini, 2010).

An interesting and somewhat unique case of identity theft involved a conman faking his way into Harvard University. In May, 2010, a student at Harvard, Adam Wheeler, was charged with a string of cons including using a fake identity to gain admission to Harvard. He allegedly faked his College Board admissions exam scores, doctored his letters of recommendation, and forged transcripts from MIT and Phillips Academy. He was charged with using the work of other scholars to obtain thousands of dollars in scholarships and grants (Jan and Valencia, 2010). Wheeler pled guilty in 2011.

A type of identity theft that is becoming more common involves the U.S. Medicare system. The U.S. Medicare system was established by the Social Security Act of 1965, which was signed into law by President Lyndon B. Johnson. The purpose of Medicare is to provide health insurance benefits to senior citizens or those who are disabled. Under Part B of the Medicare Program, qualified individuals are provided with supplementary insurance benefits. Under this program, health care providers submit claims and Medicare pays a large percentage of the cost of the medical services provided to beneficiaries. The claims submitted by health care providers are often paid by Medicare quickly, often without verification that the services were actually provided. This has led to widespread abuse and fraud in the Medicare system. For example, in February 2011, a health care crime sweep charged 114 defendants with Medicare fraud involving attempts to defraud the U.S. government of more than $240 million (Schoofs et al., 2011). One of the defendants in this case recently pleaded guilty to five counts of health care fraud (U. S. Department of Justice Press Release, 2011). The Medicare Fraud Strike Force was founded in 2007 and since then has charged more than 1,000 defendants who have collectively falsely billed Medicare for more than $3.2 billion.

LITERATURE REVIEW

Although Medicare fraud is a massive problem in the United States, there has been relatively little academic research on this type of fraud. Some research has documented that ending fraud in Medicare and Medicaid is a very difficult, if not impossible, process and that safeguards in the system are not

adequate to protect the program (Welch, 2006). The Wall Street Journal recently reported that the New York state agency in charge of recovering money stolen from the state's $52 billion Medicaid program returned more money in fraud cases to Medicaid providers than it brought back to the state (Gershman, 2011). This indicates a very serious problem in resources available to combat this type of fraud.

Research in health care fraud detection has noted that current antifraud systems are not adequate and that a more wide array of statistical methods are needed and are currently being developed to assist with fraud detection (Li et al., 2008). This research notes that advantages of improved statistical methods would include automatic learning of fraud patterns from data, specification of fraud likelihood for each case so that suspicious cases can be prioritized, and identification of new types of fraud.

Other research has proposed models to identify fraud, waste and abuse in Medicare (Musal, 2010). These models could be used to flag health care providers. Edwards (2011) examines the use of stratified sampling and ratio estimation in Medicare and Medicaid benefit integrity investigations.

Prior research has examined the risks of medical identity theft associated with the use of Electronic Medical Records (Harrison and Ramanujan, 2011). The prevalence of medical identity theft has also been examined (e.g., Dreiling, 2007), showing that organized crime is often involved.

Some research has detailed ways to avoid identity theft (Procaccino et al., 2010). Medical identity theft is often difficult to detect, and can cost the U.S. government at least hundreds of millions of dollars each year in fake billings (Katz, 2007). Medical identity theft can be used to file false Medicare claims. The thieves can either file the false claims or sell the stolen identities to others who will file false claims. This can be extremely dangerous if someone's health record is altered and as a result, they receive incorrect treatment (Katz, 2007). One study showed that increased antifraud enforcement efforts may lead to lower Medicare billings without detriment to patients (Becker et al., 2005). Krause (2006) looks at the failure of the system to adequately compensate victims of health care fraud and recommends a patient centered model for fraud recovery.

Studies have examined the expansions of State Offices of Medicaid Inspector Generals and implications for Medicaid fraud enforcement (e.g., Wenik, 2010). Other studies have examined efforts to detect and prevent Medicaid program fraud and abuse (Fusto, 2008), including the creation of the Medicaid Integrity Program (MIP). The purpose of the MIP is to identify, recover, and prevent overpayments resulting from fraud, waste, and abuse in Medicaid. Data mining and information sharing among agencies is recommended.

A recent report by the GAO notes five key areas in reducing fraud, waste and abuse in the Medicare system: strengthening provider enrollment process and standards, improving pre-payment review of claims, focusing post-payment review of claims on most vulnerable areas, improving oversight of contractors, and developing a robust process for addressing identified vulnerabilities (King, 2010). This report estimates Medicare fraud, waste and abuse to total $24.1 billion for 2009. However, it is impossible to get a precise estimate of the dollar amount of fraud, because some fraud likely goes undetected.

Medicare fraud is a huge and growing problem. Some common Medicare frauds include the following: 1) paying kickbacks to patients and have patient say they receive services they do not need or do not get, 2) pay doctors to sign off on care that is not given, prescribe tests that are not necessary, or order medical equipment that patients do not need, 3) ambulance or medical transport companies recruit patients and bribe them to have transportation costs covered by Medicaid, 4) have doctors break down what should be a single charge into many separate charges to increase total reimbursement (Schoofs et al., 2011). One of the reasons that Medicare fraud is so widespread is that the system automatically pays the vast majority of bills it receives from companies that possess federally issued supplier numbers (Johnson, 2008). Below is

a description on one of the largest alleged Medicare frauds in history, involving several different types of fraud including identity theft.

THE CASE OF THE $35 MILLION MEDICARE FRAUD

In October 2010, the U.S. Attorney's office announced the unsealing of charges against 44 alleged members and associates of an Armenian-American organized crime enterprise. The accused were charged with operating at least 118 medical clinics located in 25 states, submitting over $100 million in fraudulent claims to Medicare and with operating a multimillion dollar scheme to defraud automobile insurance companies. In a press release, Manhattan U.S. Attorney said, "…this group of international gangsters allegedly ran a verifiable fraud franchise" (FBI Press Release, 2010). The charges include racketeering conspiracy and conspiracy to commit health care fraud, bank fraud, fraud in connection with identity theft, credit card fraud, money laundering, and immigration fraud, mail fraud, wire fraud, money laundering, and aggravated identity theft.

The case has not yet gone to trial. Below is a description of the alleged frauds. The information below was obtained from the indictments. It is important to note that the information in the following six paragraphs is a description of the charges, which are merely allegation. Those charged are presumed innocent unless proven guilty in a court of law.

According to the indictment, members of the organized crime enterprise are charged with operating an elaborate nationwide scheme in which Medicare was billed for over $100 million in fraudulent claims. It is alleged that dozens of "phantom clinics" – phony health care providers that existed only on paper – were created by stealing the identity of doctors. Identifying information such as the doctor's social security number, medical license number and date of birth were stolen. Then with that stolen information, the enterprise would incorporate a health care clinic without the knowledge of the doctor. An application would then be filed with Medicare, often using the address of an empty storefront or UPS Store. Bank accounts for the phony clinic were opened. Identities of legitimate Medicare recipients were stolen and used by the defendants to defraud Medicare. Bills were submitted to Medicare for services that were said to be provided (by a doctor whose identity was stolen) to patients (whose identities were stolen). No services were actually provided.

Medicare is set up to pay claims quickly. As such, many times Medicare paid large amounts of claims into the accounts created for the phony clinics. The money was then quickly transferred into other accounts, to untraceable locations, or withdrawn. In some cases, it is alleged that tens of thousands of dollars were hand carried to Armenia. The phony clinics would shut down after a few months each but the money was long gone by the time the clinic was detected. The indictment notes at least 118 phony clinics and at least $35.7 million in fraudulent Medicare payouts.

The fraud was detected because of the suspicious manner in which Medicare was billed, such as an ear, nose and throat doctor billing for pregnancy ultrasounds. Other suspicious billings included: an obstetrician billing for allergy skin tests, a dermatologist billing for heart tests, an ophthalmologist billing for tests of the bladder, a psychiatrist billing for MRIs of upper extremities, dermatologists billing for sleep studies, etc.

According to the indictment, members of the organized crime enterprise are also charged with operating a ten year, multimillion-dollar fraud scheme to defraud the no-fault insurance system in the New York area by submitting claims for treatments and medical equipment that were medically unnecessary or never even provided. The scheme involved both actual accident victims as well as the staging of accidents to recruit patients. In some cases, hospital employees were paid to provide the enterprise with confidential personal identifying information about actual accident victims so that the enterprise could recruit them to participate in the fraud.

Once victims were identified or created, the enterprise would use corrupt doctors who agreed to subject the patients to unnecessary medical exams and treatments in order to increase fraudulent billings for the scheme. Corrupt doctors were also paid to create medical professional corporations under which the fraudulent billings could be submitted.

Corrupt lawyers were also used in the scheme to help manipulate billings in order to attract less scrutiny from the insurance carriers. Lawyers were also used to coach the claimants on how to maximize the insurance claims. One attorney is charged with allowing fraud proceeds to be laundered through his escrow account.

ROLE OF THE FORENSIC ACCOUNTANT

Due in part to the sheer magnitude of the dollar amounts involved, it is likely that the prosecution is using a forensic accountant to calculate damages. For the Medicare fraud, a team of forensic accountants could possibly perform Computer Assisted Audit Techniques (CAATs) to search the Medicare databases for: suspicious billings such as the one noted above where an ear, nose and throat doctor billed for pregnancy ultrasounds, reimbursements made to P.O. boxes or UPS Stores or similar, dates on which one doctor performed many more procedures than would be possible to perform in one day, reimbursements made for treatments performed on a date subsequent to the Medicare recipient's death, requests for reimbursements for procedures performed after the doctor's death, etc. If either the physician or patient were not alive at the time of the service, this is obviously something that would warrant further investigation. These types of CAATs, along with other procedures, may help uncover the extent of the fraud.

Once the extent of the fraud has been determined, the forensic accountants would need to prepare the case for court. In the role of an expert witness at a trial, the forensic accountant has the difficult job of presenting often complex financial information in a way that is easily understandable to the judge and/or jury. Numerous charts and exhibits will likely be prepared for this case. Volumes of complex data will likely need to boiled down into understandable chunks of testimony.

A forensic accountant may also be used to track the funds that were deposited into the bank accounts of the phony clinics. The indictment alleges that the funds were sometimes transferred from one bank to the next before being withdrawn. The prosecutors will likely want to be able to "follow the money."

For the automobile insurance fraud, a team of forensic accountants may be used to calculate the amount of fraudulent billings. Then, the laundering of the proceeds would be of interest. Exhibits would likely be prepared for the courtroom including charts with dollar amounts and graphs, as well as timetables and charts showing the flow of the money.

CONCLUSION

The goal of this paper was to highlight the problem of identity theft and Medicare fraud, and to explain the role of the forensic accountant in the detection and prosecution of such frauds. One case of a large scale Medicare fraud was detailed. Identity theft, especially in the area of Medicare fraud, is a serious problem. Government is taking some steps to combat this type of fraud. For instance, in March 2011, Attorney General Eric Holder and Department of Health and Human Services Secretary Kathleen Sebelius participate in a regional health care fraud prevention summit. These summits are part of the Obama Administration's efforts to root out fraud, waste and corruption in the U.S. health care system (U.S. Department of Health and Human Services, 2011). The Department of Justice and the Department of Health and Human Services are working together through the Health Care Fraud Prevention and Enforcement Action Team (HEAT). As one part of HEAT's efforts, Medicare Fraud Strike Force operations have expanded from South Florida and Los Angeles to a total of nine health care fraud hot

spots including Houston, T.X.; Detroit, M.I.; Brooklyn, N.Y.; Baton Rouge, L.A..; Tampa, F.L.; Chicago, I.L.; and Dallas, T.X. (U.S. Department of Health and Human Services, 2011). However, government should take further steps to prevent, identify and combat this type of fraud. Forensic accountants can be of assistance in designing auditing tools to detect such fraud and also in prosecuting cases relating to this type of fraud.

Individuals bear some of the responsibility for preventing and detecting fraud as well. Some steps that individuals can take to prevent Medicare fraud are: Keeping your personal information such as social security number and Medicare number safe and secure. This information should only be given to doctors or other providers who are approved by Medicare, your State Health Insurance Assistance Program, or Social Security. Individuals can help spot fraud and abuse by looking out for the following: suppliers who offer you free equipment, suppliers who want you to use their doctors, anyone you don't know asking for your Medicare or Social Security Number, calls from companies you did not give your phone number to, and charges for products or services you did not get on your Medicare Summary Notice (Medicare, 2009). Anyone suspecting Medicare fraud can call the Inspector General's Hotline at 1-800-HHS-TIPS.

This paper is limited in that only one large case of Medicare identity fraud was examined in detail. There is a need for much more academic research in the area of identity theft and fraud. Some suggestions for future research include examining how to make government programs such as Medicare more resistant to fraud, how to train governmental employees on fraud prevention and detection, and analyzing whether more harsh penalties may deter potential fraudsters.

REFERENCES

Becker, David, Daniel Kessler and Mark McClellan (2005) "Detecting Medicare Abuse," *Journal of Health Economics*, vol. 24, p. 189-210.

Dreiling, Geri L. (2007) "Medical ID Theft," *ABA Journal*, vol. 64, p. 36.

Edwards, Don (2011) "On stratified sampling and ratio estimation in Medicare and Medicaid benefit integrity investigations," *Health Services & Outcomes Research Methodology*, vol. 11 (1/2), p. 79-94.

FBI Press Release (2010) "Manhattan U.S. Attorney Charges 44 Members and Associates of an Armenian-American Organized Crime Enterprise with $100 Million Medicare Fraud," October 13.

Federal Trade Commission (FTC) (2011) "Consumer Sentinel Network Data Book for January – December 2010," March.

Fusto, John (2008) "MIP on the radar: the new drive to end Medicaid fraud," *Healthcare Financial Management*, vol. 62(6), p. 76-80.

Gershman, Jacob (2011) "Medicaid Unit Falls Short," *The Wall Street Journal*, Jan 27, p. A23.

Harrison, P. J. and Sam Ramanujan (2011) "Electronic Medical Records: Great Idea Or Great Threat To Privacy?," *The Review of Business Information Systems*, vol. 15 (1), p. 1-7.

Jan, T. and M. J. Valencia (2010) "This can't be our Adam Wheeler' ; Friends, teachers struggle to see the quiet striver they knew in student charged with duping Harvard," *The Boston Globe*, May 30, p. B1.

Johnson, Carrie (2008) "Medical Fraud a Growing Problem; Medicare Pays Most Claims Without Review" *The Washington Post*, June 13, A1.

Katz, Ian (2007) "South Floridians Victimized by Medical Identity Theft: Theft of Records is Rising Because it is Hard to Detect," *Tribune Business News*, July 2, p. 1.

Krause, Joan H. (2006) "A Patient Centered Approach to Health Care Fraud Recovery," Journal of Criminal Law and Criminology, vol. 96(2), p. 579-619.

King, Kathleen M. (2010) "Medicare Fraud, Waste and Abuse: Challenges and Strategies for Preventing Improper Payments," *GAO Reports*, June 15.

Li, Jing, Kuei-Ying Huang, Jionghua Jin and Jianjun Shi (2008) "A Survey on Statistical Methods for Health Care Fraud Reduction," *Health Care Management Science*, vol. 11, p. 275-287.

Markon, J and N. Irwin (2009) "ID Theft Ring Ensnares Even the Fed Chairman," *The Washington Post*, August 28, p. A22.

Medicare: Centers for Medicare and Medicaid Services (2009) "You Can Help Protect Yourself and Medicare from Fraud Committed by Dishonest Suppliers" CMS Product No. 11442.

Musal, Rasim M. (2010) "Two Models to Investigate Medicare Fraud within Unsupervised Databases," *Expert Systems with Applications*, vol. 37 (2), p. 8628-8633.

Procaccino, J. Drew, Maria H. Sanchez and Sherry Fang Li (2010) "Identity Theft: Protect Yourself and Your Clients," *The Tennessee CPA Journal*, vol. 55(3), p. 10-12.

Rothfeld, M. (2010) "Medicare Scheme Neted $25 Million, Officials Say," *The Wall Street Journal*, October 14, p. A3.

Schoofs, Mark, Maurice Tamman and Brent Kendall (2011) "Medicare Fraud Crackdown Corrals 114," *The Wall Street Journal*, February 18, p. A3.

U.S. Attorney's Office, District of Arizona (2010) "Hacker Indicted in Massive Tax, Mail and Wire Fraud Scheme," *Press Release*, April 8.

U.S. Department of Health and Human Services (2011) "Departments of Justice and Health and Human Services team up in Detroit to crack down on health care fraud; Attorney General Holder and Secretary Sebelius host fifth regional health care fraud prevention summit in Michigan," *News Release*, March 15.

U.S. Department of Justice (2010) "The Department of Justice's Efforts to Combat Identity Theft," *Audit Report*, March.

U.S. Department of Justice (2011) "Brooklyn Physical Therapist Pleads Guilty to Fraud Scheme Involving False Billings to Medicare" *Press Release,* May 13.

Verini, J. (2010) "The Hacker Who Went into the Cold," *The New York Times*, November 14, p. 44.

Welch, James M. (2006) "Mission Impossible: Stopping Medicaid Fraud," *Journal of Health Care Compliance*, vol. 8, p. 57-58.

Wenik, Jack (2010) "State Offices of Medicaid Inspector Generals: Implications for Medicaid Fraud Enforcement," *Journal of Health Care Compliance*, vol. 12(4), p. 5-10.

ACKNOWLEDGMENTS

The author gratefully acknowledges the support of the Rider University Summer Research Fellowship.

BIOGRAPHY

Maria H. Sanchez is a Professor of Accounting at Rider University. She received her Ph.D. in Accounting and her MBA from Drexel University and her Bachelor of Science in Accountancy from Villanova University. Her research primarily focuses on decision making and decision maker behavior in accounting and auditing contexts. She can be contacted at Rider University, 2083 Lawrenceville Rd., Lawrenceville, NJ 08648, US. Email: msanchez@rider.edu