Journal of Modern Accounting and Auditing, December 2018, Vol. 14, No. 12, 671-679
doi: 10.17265/1548-6583/2018.12.003

American Senior Communities: Healthcare Fraud Detection

Devon Baranek
Rider University, Lawrenceville, NJ, USA

Healthcare fraud is an increasingly large problem in the United States for patients, taxpayers, and the government, with the National Healthcare Anti-Fraud Association (NHCAA) estimating the costs to be more than tens of billions each year (NHCAA, 2018). To address this issue, government agencies and insurers can utilize data analytics to detect and prevent healthcare fraud. The American Senior Communities (ASC) case is a recent example of a complex healthcare fraud scheme committed by several high ranking officers involving kickbacks, fictitious vendors, and money laundering through shell companies. The indictment details how $16 million was stolen is particularly given the population cared for by ASC—the elderly, individuals with disabilities, low income adults, pregnant women and children. This case demonstrates several ways healthcare fraud can be perpetrated, highlights the role of the auditor, and introduces students to the importance of employing data analytics to prevent and detect fraud.

Keywords: fraud detection, auditing, healthcare fraud, data analytics

Introduction

Healthcare fraud is a serious problem in the United States, affecting patients and consumers, as well as the overall economy. During fiscal year 2016, the Federal Government won over $2.5 billion in healthcare fraud judgments and settlements, more than the gross domestic product of many countries during that same time, like Chile, Finland, or Greece (DOJ, 2017). These frauds drive up the costs for everyone in the healthcare system, and hurt the long-term solvency of programs like Medicare and Medicaid, which serve millions of Americans.

To combat this increasingly large problem, the Healthcare Fraud Prevention and Enforcement Action Team (HEAT), a collaboration between the Department of Health and Human Services and the Department of Justice, was created in 2009. HEAT is made up of top-level law enforcement agents, auditors, and attorneys aimed at preventing and prosecuting health care fraud (DOJ, 2017). The Medicare Fraud Strike Force, a multi-agency team of investigators who combat Medicare Fraud through data analysis and community policing, is part of the HEAT.

A recent example of Medicare Fraud is provided below. This study takes a detailed look at how the fraud was perpetrated, and considers how data analytics may be employed to prevent or detect this type of healthcare fraud in the future.

In 2015, the former CEO of American Senior Communities (ASC) and three others were indicted in a $16 million fraud and kickback scheme, following a year-long investigation involving the FBI, IRS, and several other federal agencies. Court documents allege the men received kickbacks from vendors servicing ASC-managed nursing homes, and falsified or inflated millions of dollars in invoices, which they then funneled

Devon Baranek, Ph.D., CPA, Assistant Professor of Accounting, Rider University, Lawrenceville, NJ, USA.

through shell companies. The case is especially disturbing because of whom the fraudsters preyed upon: the elderly, those with disabilities, low-income adults, pregnant women, and children. According to the prosecuting attorney,

> These men are alleged to have stolen from the most vulnerable in our society...they took advantage of a system entrusted with the care of this state's elderly, sick and mentally challenged allowing them to live a lifestyle of gratuitous luxury, fraught with unbridled greed. (DOJ, 2016)

In total, five defendants have pleaded guilty and been sentenced in association with this case, with sentencing ranging from 12 months of monitoring to 9.5 years in prison (DOJ, 2018; IBJ, 2018). The following paragraphs describe the fraud from information obtained from the indictments, court records, and local press.

ASC Background

American Senior Communities is a private nursing home management company located in Indiana. It is one of the largest in the state, with more than 70 nursing homes and senior care facilities. Managing these facilities requires the use of many different third-party vendors to supply goods or services, such as food preparation, patient therapies, landscaping, electronics, furniture, etc. Federal health care programs, chiefly Medicare and Medicaid, provided the majority of funds used by ASC to manage its nursing homes and senior care facilities.

In 2015, the Chief Executive Officer (CEO) of ASC was James Burkhart and the Chief Operating Officer (COO) was Daniel Benson. Neither were owners of ASC, but both were well compensated, with salaries of at least $1.5 million per year. As CEO and COO, each was authorized to negotiate and execute contracts, write checks, and make payments on behalf of ASC.

The Alleged Fraud Scheme

The indictment details a series of complicated billings and agreements ranging from 2009-2015 involving inflating costs to ASC and marking up invoices for goods and services provided, stealing discounts and rebates, and paying kickbacks. Burkhart and Benson, as well as two others not employed by ASC, used multiple shell companies to exploit ASC's numerous vendor relationships in order to divert, conceal, and launder millions of dollars for their personal benefit.

As employees of ASC, Burkhart and Benson were prohibited from owning or holding a significant interest in any supplier, customer, or competitor of ASC. They abused their positions as CEO and COO by exploiting the need for numerous products and services in the 70 nursing home and facilities they managed. According to the indictment, Burkhart and Benson cut side deals to overcharge for products and services, and funneled the overcharged amounts into shell companies they owned. In other cases, vendors paid kickbacks to the defendants in exchange for lucrative ASC contracts. When vendors questioned the overcharges or kickbacks, Benson and Burkhart would terminate negotiations. The fraud was widespread and no area was off-limits. Some of the more egregious parts of the scheme included:

Medical and safety equipment. Burkhart, Benson, and a third defendant installed upgraded nurse call monitoring systems throughout all ASC-managed facilities. They chose a vendor who agreed to inflate ASC invoices by 35% and pay the overcharges back to a shell company owned by the defendants. This same vendor was used to provide other safety equipment, including fire alarms and electrical generators, all of which were overcharged by 35%.

Medical supplies. At the defendants' instruction, a medical supply company inflated invoices by 40% and submitted the inflated invoices to ASC. The defendants also used a shell company to steal discounts and rebates they had negotiated on behalf of ASC for medical supplies.

Flags. Another shell company created by Burkhart purchased flags from a local supplier, including American flags, state of Indiana flags, and ASC-branded flags. These same flags were marked them up 150%, and resold to ASC. Burkhart personally approved these invoices and replaced the flags several times per year.

Uniforms, door wraps, t-shirts. Between 2013 and 2015, Burkhart, Benson, and a third defendant used a shell company to conceal overcharges to ASC for a variety of ASC-related products. These products included ASC-branded discharge packages, embroidered uniforms, seasonal door wraps, luggage, and t-shirts for an Alzheimer's Memory Walk. The prices for these items were marked up as much as 200%.

Landscaping and outdoor maintenance. Between 2009 and 2014, Burkhart and the owner of a landscaping company falsified and inflated invoices to pay kickbacks to numerous parties as well as fund personal travel and political contributions. Invoices were fraudulently inflated by as much as 45%, and the overages were paid to shell companies owned by Burkhart and others. During this period, an additional $1.5 million in ASC funds was paid for fictitious "consulting" services that never occurred.

Furniture. Burkhart, Benson, and a third defendant concealed overcharges for interior design and furniture services through a shell furniture company. Invoices were inflated by 20-25% and a portion of overcharges was paid back to the furniture company.

Pharmacy. The defendants allegedly used shell companies and fake contracts to conceal $5.5 million in kickback payments disguised as "marketing fees" in return for contracting with various pharmacies to provide pharmacy services throughout the ASC-managed facilities.

Hospice. No areas were off limits for the defendants, not even end of life care for dying patients. Between 2013 and 2015, Burkhart, Benson, and a third defendant set up shell companies and solicited kickbacks for referring patients to a "preferred provider" for hospice care.

Other shell companies and sham contracts were used to conceal kickbacks involving food services, office and industrial supplies, speech therapists, patient lifts, home health services, wound care products, and miscellaneous medical supply providers engaged by ASC. In total, more than 20 shell companies were used to conceal payments of over $16 million.

Aftermath

Eventually, a tip from a concerned citizen with knowledge of the fraud helped investigators crack the case. The president and COO of a local vendor called the FBI in June 2015 after being approached to join the fraud scheme by one of the defendants (IBJ, 2018). In September 2015 federal agents raided Burkhart's home and the headquarters of ASC. Burkhart and Benson were fired and another executive (Chief Financial Officer) also resigned. ASC has since hired a new leadership team and implemented more robust safeguards.

The defendants face multiple federal felony charges including mail fraud, wire fraud, health care fraud, and money laundering. Three of the defendants are also charged with conspiracy to circumvent the Anti-Kickback Statute. If convicted, the fraud and conspiracy counts carry 20 year prison sentences, the money laundering carries 10 years, and the violations of the Anti-kickback Statute carry five years.

Case Questions

1. Briefly describing the alleged fraud, how were the defendants able to steal from ASC and who was involved?

2. Describe how the fraud triangle may have come into play here. What were some of opportunities, incentives/pressures, and attitudes/rationalizations that led to the alleged fraud scheme?

3. What could ASC have done differently to potentially prevent or limit the fraudulent activity? Describe how data analytics may have been utilized to identify issues specifically relating to vendors and invoicing.

4. How were the defendants able to circumvent the internal controls in place at ASC and conceal the fraud? The alleged scheme lasted almost six years: Were there any red flags? Consider what types of data metrics and monitoring could have aided the governance and management practices of ASC.

5. Due to the nature of the alleged fraud, ASC has additional controls in place for third party vendors providing goods or services. What are some examples of these controls?

6. Since 2009, the Healthcare Fraud Prevention and Enforcement Action Team (HEAT) has been using Fraud Prevention Systems (FPS) to identify abnormal or suspicious billing patterns. According to the U.S. Department of Health and Human Services Office Inspector General (HHSOIG), savings associated with this type of prevention and detection since 2011 were $820 million. What is FPS? Could a similar tool have been useful in the current case?

7. What happened to the senior leadership team at ASC? How has the fraud impacted their corporate governance structure? Do they have a CCO, and if so what is his/her role?

8. It appears that numerous vendors associated with ASC (as well as vendors that failed to win contracts) knew of the fraud and either helped perpetuate it or failed to notify any regulatory agencies. What options were available to these vendors who knew something was amiss and wanted to do something about it?

Teaching Notes

Overview and Learning Objectives

The primary objective of the case is to introduce students to the concept of using data analytics in the prevention and detection of health care fraud. A secondary objective of the case is to reinforce the topic of the fraud triangle. This case is appropriate for use in an auditing course as well as fraud or forensic accounting courses.

The case demonstrates to students how health care fraud may be perpetrated and introduces introductory techniques for its prevention and detection. The role of the auditor and the increasing use of data analytics are examined. Today's accounting graduates will be expected to be familiar with data analytics.

Implementation Guidance

This case has been used in an upper-level undergraduate auditing course. It is also appropriate for a fraud/forensics course and could also be used at the graduate level. The case is an extension of what can be found in a traditional textbook. In the auditing class, it was assigned as agroup project. It could also be assigned as an individual project. The case outlines a real world case of health care fraud committed at a large scale. If used in an auditing class, the case can be assigned after a discussion of the use on data analytics. We typically provide one 90-minute class period for students to read the case and complete the case questions. On the due date (the following class), we spend the about one hour discussing the case solutions. The cases take

approximately 15-20 minutes each to grade. Instructors can emphasize the demand for fraud control professionals, which should be good news for accounting professionals.

Evidence Regarding Case Efficacy

We have had positive student feedback on the case. Students find it surprising that there is such a problem with health care fraud in this country and even more shocking to learn that it is impossible to know exactly how big the problem is, since it is impossible to know how much fraud has gone undetected.

To help determine efficacy of the case, we administered a survey to an upper level auditing class. An Appendix to this section (Appendix: Evidence of Case Effectiveness) includes the survey questions and results. The survey was completed anonymously to ensure unbiased feedback. A majority of the students have indicated that they "agree" or "strongly agree" with the following statements:

- My understanding of data analytics increased as a result of this case.
- My understanding of the fraud triangle increased as a result of this case.
- My understanding of the role data analytics in healthcare fraud deterrence and detection increased as a result of this case.
- Through this case, my understanding of evaluating risks in the healthcare industry increased.
- I understand the role of data analytics better after completing this case.
- I found this case interesting.

Case Solutions

1. Briefly describing the alleged fraud, how were the defendants able to steal from ASC and who was involved?

The defendants created numerous shell companies, which were responsible for providing a wide range of products/services to ASC. These companies overbilled and falsified prices that were paid for with money from Medicare and Medicaid. In addition to receiving kickbacks, the defendants turned down or severed relationships with vendors that were not willing to participate in the scheme. Over $16 million was distributed in fraudulent kickbacks and overcharges.

2. Describe how the fraud triangle may have come into play here. What were some of opportunities, incentives/pressures, and attitudes/rationalizations that led to the alleged fraud scheme?

Opportunities: weak controls at ASC; inconsistent polices for third party vendors—no background checks, lack of monitoring, no price comparisons, etc. Additionally, the defendants took advantage of the scale of ASC (more than 70 nursing homes and thousands of patients), which required the use of many third party vendors.

Incentives/Pressures: Live/maintain extravagant lifestyles—FBI identified bank accounts, vacations, and excessive spending traceable to the alleged fraud.

Attitudes/Rationalization: The parties involved may have felt that they weren't stealing from the patients; they were stealing funds from the state and federal government. They may have felt that it was a victimless crime or that because they were still providing services to ASC, it wasn't stealing—it was overcharging or charging a little "extra".

3. What could ASC have done differently to potentially prevent or limit the fraudulent activity? Describe how data analytics may have been utilized to identify issues specifically relating to vendors and invoicing.

- Searching for duplicate invoice/vendor numbers

- Calculation of ratios for key numerical fields, such as unit prices
- Compare vendor pricing to similar products from other vendors
- Data analysis techniques like Benford's Law, with investigation of unusual digit patterns
- Examining invoice data for outliers or gaps in sequential data
- Check vendor approval and/or invoice approval processes—check for an appropriate segregation of duties in the ordering/approval/receiving/payment processes

4. How were the defendants able to circumvent the internal controls in place at ASC and conceal the fraud? The alleged scheme lasted almost six years: Were there any red flags?

Because the defendants included high-level managers of ASC (the CEO and COO), they were able to collude and avoid detection by circumventing the existing internal controls in place. They concealed their ownership interests in the shell companies, and further mislead ASC employees by creating corporate email addresses with fake names and using those in correspondences about orders.

Red flags that may have indicated something were amiss:

- Extravagant spending by the defendants—private plans, golf trips, Rolex watches, vacation homes, political contributions, etc.
- Excessive purchases for ASC—for example, new American flags, State of Indiana flags, and ASC-branded flags were purchased multiple times per year
- Vendors expressing concern about overcharging and then paying the overcharge to a shell company
- Negotiating a discount on medical supplies while choosing to pay the full, non-discounted prices
- Ganote documented much of the fraudulent scheme in binders, records, and handwritten notes and ledgers

5. Due to the nature of the alleged fraud, ASC has additional controls in place for third party vendors providing goods or services. What are some examples of these controls?

- ASC Compliance Hotline and website, managed by a third party vendor, where reports can be filed anonymously. Incident reports can be submitted or interested parties can follow-up on a previous incident report.
- Published Standards of Conduct for ASC's Purchasing Services Group as well as ASC's vendors. Includes standards to provide guidance, as well as policies that have been established to ensure adherence to the Standards of Conduct.
- Published Elder Justice Act—detailing vendors' responsibility to report reasonable suspicion of a crime against a resident of a healthcare facility. Also provides information for filing a complaint regarding retaliation via phone or email.
- Commitment to Corporate Social Responsibility—purchasing goods and services from a diverse pool of suppliers. All vendors are encourages to provide quotes via email and all vendors who meet the capabilities and qualifications will be considered.

6. Since 2009, the Healthcare Fraud Prevention and Enforcement Action Team (HEAT) has been using Fraud Prevention Systems (FPS) to identify abnormal or suspicious billing patterns. According to HHSOIG, savings associated with this type of prevention and detection since 2011 were $820 million. What is FPS? Could a similar tool have been useful in the current case?

Similar to the fraud detection technology used by credit card companies, Fraud Prevention Systems (FPS) apply predictive analytics to claims before making payments in order to identify abnormal or suspicious billing patterns.

ACS could have used this type of analysis on vendor invoicing and for other third party providers of goods and services. In a 2017 report, the GAO reported that FPS can speed up certain investigation processes, like identifying and triaging suspect providers. This type of system could have been useful to ASC in identifying leads for fraud investigations by comparing billing or pricing patterns against expectations or models of fraudulent behavior. Vendors with suspect billing patterns (or ASC purchases of suspect patterns) could have been flagged or investigated further.

7. What happened to the senior leadership team at ASC? How has the fraud impacted their corporate governance structure? Do they have a CCO, and if so what is his/her role?

CEO Burkhart and COO Benson were fired and an interim CEO and COO served until Donna Kelsey (CEO) and David Stordy (COO) were hired. ASC filed a civil lawsuit against Burkhart and Benson and is seeking to recover losses and damages ASC claims it sustained through their actions. Additionally, the CFO resigned.

After the fraud, ASC hired a Chief Compliance Officer (Kim Martin). A CCO is typically responsible for overseeing and managing regulatory compliance issues and may also be tasked with designing and implementing internal controls, policies, and procedures to ensure compliance with all applicable laws and regulations.

8. It appears that numerous vendors associated with ASC (as well as vendors that failed to win contracts) knew of the fraud and either helped perpetuate it or failed to notify any regulatory agencies. What options were available to these vendors who knew something was amiss and wanted to do something about it?

Numerous vendors are identified in the case as having been rejected as a third party vendor for ASC because they refused to overbill and pay kickbacks to the defendants. These vendors could have reported the suspected fraud by doing any of the following:

- Call Medicare Fraud tip line (1-800-Medicare)
- Email the department of Heath and Human Services
- Report it online to the Office Inspector General
- Mail a report to the Office Inspector General
- Call the Office Inspector General

According the Assistant U.S. Attorney, a member of the public came forward and spoke with the Department of Justice. The person was employed by one of the companies that were turned away by the defendants for refusing to participate in the kickback scheme. This launched a joint investigation between the FBI, IRS, and Department of Heath and Human Services, Office Inspector General.

References

American Senior Communities. (2017). Retrieved October 21, 2017 from http://www.ascseniorcare.com/

Centers for Medicare & Medicaid Services Official Blog. (2016). *Encouraging innovation to fight medicaid fraud.* Retrieved October 25, 2017 from https://blog.cms.gov/2012/05/25/encouraging-innovation-to-fight-medicaid-fraud/

GAO. (2017). *CMS fraud prevention systems uses claims analysis to address fraud*. Retrieved November 6, 2017 from https://www.gao.gov/assets/690/686849.pdf

Indiana Business Journal (IBJ). (2016). *Defendant in American Senior Communities probe agrees to plead guilty*. Retrieved October 25, 2017 from https://www.ibj.com/articles/61697-defendant-in-american-senior-communities-probe-agrees-to-plead-guilty

Indiana Business Journal (IBJ). (2018). *Vendor's honesty helped unravel $19M American Senior Communities fraud*. Retrieved July 20, 2018 from https://www.ibj.com/articles/69742-vendors-honesty-helped-unravel-19m-american-senior-communities-fraud

National Healthcare Anti-Fraud Association (NHCAA). (2018). *The challenge of healthcare fraud.* Retrieved from https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx

Trading Economies. (2017). *GPD*. Retrieved November 6, 2017 from https://tradingeconomics.com/country-list/gdp

United States Department of Justice (DOJ). (2016). *Former American Senior Communities Executives Indicted*. Retrieved October 22, 2017 from https://www.justice.gov/usao-sdin/pr/former-american-senior-communities-executives-indicted

United States Department of Justice (DOJ). (2017). *Fact sheet: The heath care fraud abuse and control program protects consumers and taxpayers by combating health care fraud*. Retrieved October 22, 2017 from https://www.justice.gov/opa/pr/fact-sheet-health-care-fraud-and-abuse-control-program-protects-conusmers-and-taxpayers#_ftn1

United States Department of Justice (DOJ). (2018). *Former health care chief executive sentenced to 9.5 years in federal prison*. Retrieved November 22, 2018 from https://www.justice.gov/usao-sdin/pr/former-health-care-chief-executive-sentenced-95-years-federal-prison

USA Today. (2016). *Health care execs accused in multi-million dollar scheme*. Retrieved October 22, 2017 from https://www.usatoday.com/story/news/nation-now/2016/10/12/indiana-nursing-home-fraud-accusations/91948536/

WTHR News. (2016). *Charges announced against Former American Senior Communities Execs for Medicare Fraud*. Retrieved October 22, 2017 from https://www.wthr.com/article/former-american-senior-communities-ceo-other-former-company-officials-arrested-wednesday

Appendix: Evidence of Case Effectiveness

	Survey question	Response*	1	2	3	4	5
1.	My understanding of data analytics increased as a result of this case.	Response Frequency	-	-	6	17	10
		% Frequency			18%	52%	30%
2.	My understanding of the fraud triangle increased as a result of this case.	Response Frequency	1	2	4	9	18
		% Frequency	3%	6%	12%	26%	53%
3.	My understanding of the role data analytics in healthcare fraud deterrence and detection increased as a result of this case.	Response Frequency	1	-	5	11	16
		% Frequency	3%		15%	33%	49%
4.	Through this case, my understanding of evaluating risks in the healthcare industry increased.	Response Frequency	-	-	1	15	15
		% Frequency			3%	48%	48%
5.	I understand the role of data analytics better after completing this case.	Response Frequency	-	1	7	11	14
		% Frequency		3%	21%	33%	42%
6.	I found this case interesting.	Response Frequency	2	-	3	6	21
		% Frequency	6%		9%	19%	65%

Notes. *Students were required to respond to a questionnaire designed using the following scale: 1 = Strongly Disagree; 2 = Disagree; 3 = Neutral; 4 = Agree; 5 = Strongly Agree.