Cutting through the Numbers: How Data Mining Was Used to Uncover Multiple Frauds at a Hospital System Medical Center

Dr. Bryan Cataldi
Bryan Callahan
Dr. James F. Sander
Dr. Anne S. Kelly*

Introduction

"You literally could not walk into this place without tripping over fraud."

How, then, could traditional audit procedures miss what the lead fraud investigator, Brent Carter, described in the quote above as so glaring?

The story begins in mid-2012. The new Business Manager of the Sugardale Medical Center (Center), Jacob Welsh, uncovered some unusual credit card activity specifically related to the prior year. His concerns culminated in a formal request to the hospital for their internal audit staff to further investigate the credit card abnormalities in an attempt to quantify the nature and extent of the financial impact. The internal auditors discovered overpayments of roughly $50,000 associated with the credit cards as well as payroll bonuses that should not have been paid. In order to assist with the investigation, the Center’s board of directors authorized the engagement of forensic accountants from an external CPA firm to perform a fraud examination. The hospital system had in place a $500,000 fraud insurance policy. The CPA firm was told to investigate potential frauds but to stop investigating if or when their forensic team discovered issues that exceeded that amount. The board authorized the firm to extend procedures back to 2010, which provided a window for investigation of the previous two years. Additional procedures could be authorized based on the initial findings.

It was late in 2012 when Brent Carter, head of the CPA firm’s forensic accounting team, had completed his forensic investigation, submitted the final report, and had time to reflect back on this challenging assignment, “You literally could not walk into this place without tripping over fraud. It was that evident, but only if you knew where and how to look. There was collusion between two long-time employees—sure they had segregation of duties, but this is where segregation of duties shows its weaknesses. As soon as people collude—poof—those protections are gone. While we used other procedures, we relied on data mining and data analytics as a particularly useful forensic accounting procedure for this situation because it can uncover financial connections that perpetrators frequently do not even realize they need to hide.”

Mr. Carter concluded, “Sometimes the large dollar-amount frauds are not particularly interesting because they are composed of only one scheme, and that one scheme simply gets repeated so many times that the amount gets to be large. Although the medical center case was not one of the largest in amount, I found it fascinating because there were so many multiple, smaller schemes to uncover.”

Company Background

Eleanor Ingalls landed the job of a lifetime in June 2002, as the Executive Director (ED) of the Sugardale Medical Center. She had built an impressive resume of relevant experience including supervising the billing and collection functions at a large regional hospital and managing the office for five orthopedic surgeons. This new job brought an opportunity to gain additional managerial experience, which also allowed for significant decision-making discretion. Eleanor’s first task was to hire her second in command, a Business Manager, who would be responsible for the day-to-day operations of the Center.

*The authors are, respectively, Assistant Professor at Butler University, Director of BKD, LLP, Associate Professor at Butler University, and Associate Professor at Butler University.
Mark Nyland applied for the Business Manager (Manager) position after working for a small Certified Public Accounting (CPA) firm in the healthcare industry. He was anxious to leave the daily grind of public accounting with its multiple deadlines throughout the year. Mark and Eleanor hit it off immediately and soon after his interview, Mark accepted the position with the Center. His hiring marked the beginning of a mutually beneficial professional relationship that lasted from 2002 to 2012.

The Center was fifty percent owned by doctors and fifty percent owned by a very large hospital system. Generally, the hospital system had the central responsibility to house all back-office operational functions; however, the Center maintained its own financial reporting and accounting. This autonomy was a key component in allowing Eleanor and Mark to initially perpetrate the fraud as they fiercely protected their combined control. A large, well-respected CPA firm conducted certain agreed-upon procedures related to the Center’s financial statements but it was not engaged to perform a full independent audit in compliance with generally accepted auditing standards. Furthermore, a board of directors provided oversight to the ED. Half of the board of directors was made up of executives from the hospital and the other half were surgeons who were elected to represent the fifty percent ownership of the doctors. Although the Center earned significant revenue, it was a small portion of the hospital system’s overall operations.

While controls did exist, including extensive segregation of duties between the ED and the Manager, the two together had full control over and access to the accounting records—processing billings, vendor payments, patient write-offs, payroll, etc. Furthermore, these two individuals fought to keep it that way in the face of changes within the organization. During the 2010–2011 timeframe, the hospital system made a decision that they had the resources to manage all of the back office processes for their joint ventures. Therefore, the hospital system proposed to take full control over all accounting and transaction processing functions to allow the Center to focus on surgeries. Every medical center/hospital joint venture agreed to accept the new arrangement—except this particular center. Eleanor appealed as high as the President of the hospital system to retain her authority over the Center’s accounting and transaction processing and keep that responsibility within the Center itself. Her argument was that their particular center was a smoothly operating and well-run machine that had experienced significant growth and earned substantial profits for its size. The hospital system eventually agreed to allow the Center to retain control over the back-office operations, which subsequently proved to be a huge mistake.

Timeline
Eleanor and Mark managed the Center from 2002 until the beginning of 2012. Throughout this time, Eleanor believed she was gaining significant recognition within the hospital system for her efforts managing the Sugardale Medical Center and the significant profits it generated. In 2011, she applied for a Vice President position within the hospital system. Given the Center’s very good financial performance, Eleanor was confident she would be hired for the position; she had successfully navigated through several elimination rounds during the hiring process and became one of the final two candidates for the job. Nonetheless, she was ultimately passed over for the position. Eleanor remained with the Center until January 2012 when she resigned. Upon Eleanor’s resignation, Mark also resigned; however, he remained briefly to train the new Business Manager, Jacob Welsh. Jacob assumed Mark’s responsibilities in March 2012.

Schemes Utilized to Misappropriate Assets

Credit Card Usage
The credit card fraud discovered by the new Manager, Jacob, triggered the fraud examination. Direct credit card purchases by Eleanor and Mark on the corporate credit cards amounted to $65,000 for personal groceries, gasoline, and travel expenses. Mark was so brash that he even used the Center’s credit card to pay for his family’s trips to his daughter’s athletic competitions.

Data Mining Discovery
The forensic accountant team, led by Brent Carter, performed a “weekend and holiday analysis” to search for potential abuses of corporate credit cards. It is recognized that legitimate expenses can occur outside of the normal five-day workweek; however, any use outside these days is flagged for further scrutiny. In this case, there was an extensive amount of weekend and holiday activity on the credit card statements. These particular transactions were analyzed to determine possible legitimate business purposes. They were also matched to known behaviors of the Manager. For example, the investigators were told through interviews with other employees that Mark’s daughter competed in athletic events across the country. They matched the dates and locales of these athletic competitions with the weekend credit card
transactions and found charges involving out-of-town restaurants and hotels in Mark’s name or in the names of his family members. They also searched for and found charges to the Center’s credit card for related airline tickets.

**Automated Clearing House (ACH) Payments**

Besides the direct credit card purchases, it was determined that an additional $54,000 was embezzled through a scheme devised by the ED. While several credit cards were in the Center’s name, the forensic accountants determined that all of the Center’s cards were from Wells Fargo Bank. A review of the Center’s ACH payments revealed that the balances on credit cards from other financial institutions were being paid via automated payments. Admission-seeking interviews with Eleanor confirmed that various payments were being made by the Center for unauthorized credit card accounts—and for significant dollar amounts. The ED admitted that she had linked her husband’s personal credit card to the Center’s accounts. She explained that she debited a variety of general ledger accounts for small uneven amounts, thereby spreading the fraud throughout the entire accounting system.

**Data Mining Discovery**

The forensic accountants performed an effective procedure to detect these improper ACH payments. A query was executed on all payments for the purpose of identifying any payment in which the payee name included any portion of the major credit card names (i.e., MasterCard, Visa, MC, Citi, Chase, etc.) other than Wells Fargo. These payments were flagged because only Wells Fargo cards were authorized for corporate use. Further investigation of these payments revealed non-medical center credit cards had automated payments tied to them. Admission-seeking interviews confirmed that these payments were tied to personal credit cards of the ED and her husband.

**Extra Manual Checks**

Eleanor abused the bonus system to ensure that her staff saw no need to question any unusual relationships or transactions. She paid illegitimate bonuses to favored employees: Mark and herself. The fraudulent activity was perpetrated by compensating personnel directly through accounts payable by using fictitious vendors. The ED’s responsibilities included the ability to add vendors to the accounting system. This capability allowed her to set up employees as vendors so as to permit cash disbursements made directly through accounts payable to employees. Eleanor inserted names and addresses of the employees in the vendor master file; she then wrote small bonus checks to the employees in the form of direct payments to these fictitious vendors. These small bonuses to employees were in addition to their legitimate payroll checks.

While the ED was the major recipient, these bonuses allowed her to create allies of the employees. She essentially bought their complicity by paying them small bonuses outside of their normal compensation as recognition “for their hard work.” The forensic investigation revealed that employees overlooked irregularities and failed to act on suspicions of her behavior even in the face of a variety of red flags. A total of forty-nine checks were written amounting to $21,000 over the course of the two-year period as determined by the forensic accountants. Eleanor would write the checks manually and charge the bonuses to a variety of general ledger accounts for very small amounts.

**Data Mining Discovery**

The forensic accountants used an employee–vendor matching technique to detect the fictitious vendor fraud. This approach cross-references all of the attributes (name, address, phone, tax ID, etc.) in the employee master file with the vendor master file to see if there are any exact or close matches. Direct matches produce a potential red flag that must be investigated. The system is “smart” enough to produce more than just direct matches. If any part of the employee name (including abbreviations, initials, and anagrams), or if any portion of the employee address matches the vendor file, this match generates a red flag exception as well.

**Over-the-Counter Withdrawals**

Another fraud committed by the ED and the Manager entailed cash withdrawals made in person from the Center’s operating bank accounts. Usually this activity would occur on Fridays (consequently, the forensic accountants speculated this activity provided weekend spending money). Eleanor or Mark would prepare general journal entries for very small amounts, with the debits to a wide variety of expense accounts. Overall, the ED and the Manager withdrew $4,000 and $3,800, respectively, in amounts ranging from $200 to $1,100 each.

**Data Mining Discovery**

938
Withdrawals of cash by both the ED and Manager were always in round numbers. A standard procedure in data mining is to run a query of all round-number cash disbursement transactions with their related general journal entries. Generally, most invoices and payments are not in round-number amounts. In this case, expense accounts were debited for various uneven amounts but the credits to cash were in round numbers. The peculiar nature of round-number credits to cash raised the initial concern and prompted further investigation. Admission-seeking interviews revealed that Eleanor and Mark were, in fact, withdrawing money from accounts for personal use.

Gross-up of Paid-Time-Off (PTO)

The Center’s policy of permitting employees to cash out excess PTO facilitated fraudulent payments. The Manager would manually override the payroll system to indicate employees worked when in fact they had taken days off or he would simply replace an employee’s PTO balance with a higher, erroneous amount. Using this scheme, the Manager embezzled over $41,000 during the two-year period analyzed while other employees benefitted by roughly $39,000. The ED was involved in this scheme to the extent that she approved all timesheets for her staff. Furthermore, she advised the Manager to gross up her own PTO and subsequently cash it out as a bonus.

Data Mining Discovery

A simple examination of vacation account balances over time discovered unusual fluctuations in the account balances. Forensic accountants observed that during a given two-week timeframe, individual employee PTO balances might increase by more than forty hours (which could not happen legitimately) and then subsequently drop forty hours in the next pay period when the employee cashed out the fictitious PTO balance.

Scrip Program

The final fraudulent approach involved a scrip program, which is a typical fundraising mechanism for schools. In a scrip program, a parent buys from the school a gift card that is from a store at which the parent normally shops. The school obtains the gift card from an intermediary at a discount ranging from two percent to thirteen percent. The school keeps the difference and local businesses generate goodwill in the community by helping the school system raise money. In some cases, the donor also receives a three percent reduction in tuition. For example, an individual can purchase from the school a $1,000 gift card to Home Depot and then use the card at Home Depot to receive a $1,000 worth of merchandise as well as receive a thirty dollar reduction in tuition dollars.

Most people donate small amounts; however, Eleanor wrote manual checks to the scrip program from the Center’s bank account in amounts of $800 to $1,200. The vast majority of the gift cards she received were in large denominations for her personal use. She also acquired smaller denomination cards that she would hand out to selected employees as a reward for their work. These actions fostered goodwill among the employees and furthered their admiration for and complicity with the ED. Eleanor wrote checks directly to the school; however, she hid these payments by creating invoices and recording the amounts in the major vendor accounts of the Center, knowing the amounts were small in comparison to the total amount billed to the vendors. Eleanor wrote forty-seven checks totaling about $39,000.

Data Mining Discovery

The forensic accountants conducted a data analytics procedure known as frequency analysis. Interviews with employees uncovered the fact that the larger vendors billed the Center once each month with the typical average amount at well over $10,000. Frequency testing for invoices that occurred more than once a month produced potential discrepancies, which were investigated. A second test could have uncovered this scheme by flagging amounts that deviated from the average invoice total by a statistically significant value and then reviewing the supporting evidence.

Red Flags Missed

"Fraud schemes are very clear in hindsight. Many times those who may have caught the fraud earlier or prevented it entirely are blinded by trust, apathy, or hectic schedules. Trusting people is normal, especially those we work with for a long time; however, trust is also the best tool for the fraudster. Establishing routine monitoring activities is the key to not letting the fraudster or potential fraudster get too far before being stopped," per Brent Carter of the fraud investigation team. "These factors open the door for fraud, and were certainly a key component in how the frauds were perpetrated and carried out for so long."
Interaction of multiple elements made this case particularly interesting, and allowed these schemes to be carried out successfully for a comparatively long period of time. Given that the medical center was both financially successful and yet was a small portion of the overall operations of the hospital system, the entity was able to “fly under the radar” of hospital oversight. In addition, the shared responsibilities by the ED and Manager gave them access to every aspect of the accounting system. This combination created one of the three crucial factors in the Fraud Triangle, opportunity to perpetrate fraud. Ultimately, the collusion between Eleanor and Mark circumvented critical internal controls furthering that opportunity.

The ED and Manager were cunning in how they implemented schemes in ways that minimized the risk of detection. They rarely, if ever, charged the general ledger accounts for round numbers or large amounts. As the ED, Eleanor also effectively manipulated key employees by creating a culture of complacency as a benevolent dictator. Employees loved and respected her. Consequently, they were either blinded to the realities of suspicious behaviors in the first place or they outright looked the other way in the face of evidence contradicting their perceptions. For example, the accounts payable clerk mentioned in one interview that she found it odd that the ED frequently paid with gift cards, but she failed to mention the practice to anyone in upper management. The two perpetrators were handing out bonuses and providing employees with a variety of perks—why would the gift recipients want to ask questions?

The Center was good at what it did, and the ED and Manager managed it seemingly very well. As long as the business continued its successes and remained a small portion of the larger hospital pie, no one felt the need to challenge local policies and decisions. One major red flag occurred when the hospital sought to take the back-office accounting from the medical center as it had done successfully with other similar operations. This move met staunch resistance from Eleanor and Mark. The hospital system relented, and no one ever pursued the underlying reasons why the opposition existed in the first place. Again, the Center was making money and the path of least resistance was to let them continue to do what they seemed to be doing well—“if it ain’t broke, don’t fix it.”

In summary, over $300,000 in assets was misappropriated by the ED and Manager over the two years covered by the fraud examination. During admission-seeking interviews, the forensic accountants learned that the fraud had been perpetrated for more than 10 years for an estimated total in excess of $1,000,000.

Final Thoughts

Brent Carter was thinking about the various tasks his forensic accounting team would do for this new assignment. Based upon his past forensic accounting experiences, he directed his team to apply the data mining discovery procedures as discussed in this case. Also, he developed the following discussion questions for his team to consider.

Discussion Questions

1. Contrast three types of engagements: an agreed-upon procedures engagement, an independent audit of the financial statements, and a forensic accounting examination. How does the investigator’s role and responsibilities for detecting fraud differ?

2. How does data mining differ from traditional audit procedures? Are traditional audit procedures using sampling likely to be replaced by data mining techniques using data analytics in the future with advances in information technology?

3. The Fraud Triangle includes three main risk factors that converge to facilitate fraud. Identify and describe these factors. Which factors are evident in the case? Provide specific examples.

4. Describe specific internal controls that could have deterred or detected the fraud of misappropriation of assets described in the case. What could hospital system management have done to reduce the related control risk?

5. How did the ED and Manager create a culture of complicity within the organization that allowed them to perpetrate the frauds? How did the nature of the frauds allow them to go undetected for so long?