After publishing the *Stevenson University Forensics Journal* annually for five years, it was time to try out something new. The Journal is still full of interesting articles touching many disciplines within the vast field we call Forensic Studies, and the articles are still fully student researched and written. However, this year we doubled the word limit requirement for the submissions. As a result, authors were given room to explore their subject matters a bit deeper, offer more extensive analysis and offer the reader a more thorough perspective on the topics.

Also new this year is an “Ask the Experts” column. The column is a feature that will give the reader perspective on a topic related to Forensic Studies by asking an expert to address common questions in his or her field. The experts will rotate to address different areas of Forensic Studies each year. Readers are encouraged to submit questions via email to chjohnson@stevenson.edu. I look forward to your participation in this aspect of the Journal.

Once again, I offer my congratulations to the students from the Stevenson University Masters in Forensics program whose articles were selected for publication this year. Publication in the Journal is a highly competitive process and involves a tremendous commitment on the part of the author and editors. As always, the results are proof of the talent and dedication of our students.

Carolyn Hess Johnson, Esquire
Editor and Publisher
TABLE OF CONTENTS

1 INTRODUCTION
   CAROLYN JOHNSON

4 ASK THE FORENSIC EXPERT:
   MICHAEL ROBINSON

6 REGULATIONS FOR OFF-BALANCE-SHEET
   FINANCING PRODUCE RISKY FINANCIAL
   STATEMENTS
   CRYSTAL ABRAHAM

11 PROACTIVE DATA ANALYSIS TO PREVENT AND
   DETECT FRAUD IN SMALL BUSINESSES
   ROBERT E. BATES

19 TERRORISM IN CYBERSPACE:
   IS THE U.S. READY FOR A VIRTUAL 9/11?
   KERA N. VALENTI

25 SECURITY IN THE CLOUD
   JONATHAN MAY

30 AFFINITY FRAUD:
    IDENTIFICATION AND PROSECUTION
   CHRISTINE KREKE

36 RECENT TRENDS OF ENFORCEMENT AND
   COMPLIANCE WITH THE FOREIGN COR-
   RUPT PRACTICES ACT
   WILLIAM OLSEN

42 DISRUPTING TERRORIST FINANCING:
   INTERAGENCY COLLABORATION, DATA
   ANALYSIS, AND PREDICTIVE TOOLS
   ANDREA LYNCH PYON

52 ERADICATING ELDER FINANCIAL ABUSE
   CHERYL A. PANATTONI

57 DATA ANALYSIS AND RELIABILITY
   IN PREDICTING FRAUD
   JOSEPH T. HARRIS, CIA, CFE

65 MEDICAID AND MEDICARE FRAUD,
    WASTE AND ABUSE
   LINDSAY M. WHEATLEY
Ask the Forensic Expert: Michael Robinson

Michael Robinson is a computer forensic examiner and cyber threat analyst for a large international company. He has performed computer and cell phone exploitation and analysis for customers in both the U.S. Intelligence Community and the private sector. Michael has performed computer forensic examinations for the FBI’s Investigative Analysis Unit, where he assisted special agents with counter-intelligence and criminal cases. Michael is the former CIO of the U.S. Department of Defense’s Business Transformation Agency, where he oversaw all information technology and information assurance operations for the agency, including overseeing all incident response and forensic investigations.

Michael is the Program Coordinator and an Adjunct Professor for Stevenson University’s Master of Science in Cyber Forensics. At Stevenson, he was the recipient of the Rose Dawson Award in 2013. He teaches courses in mobile device forensics, intrusion analysis, and cyber warfare. Michael holds a Bachelor of Science in Chemical Engineering, a Master of Science in Information Assurance, a Master of Science in Forensic Studies (concentrating on computer forensics), and a graduate certificate in Applied Intelligence.

Michael has presented at numerous national and international conferences including DEF CON, the DoD Cyber Crime Conference, InfoSec World, and the BCISS Conference on Intelligence Analysis. He has authored over a dozen journal articles and a book on disaster recovery planning for nonprofit organizations.

Michael Robinson is a computer forensic examiner and cyber threat analyst for a large international company. He has performed computer and cell phone exploitation and analysis for customers in both the U.S. Intelligence Community and the private sector. Michael has performed computer forensic examinations for the FBI’s Investigative Analysis Unit, where he assisted special agents with counter-intelligence and criminal cases. Michael is the former CIO of the U.S. Department of Defense’s Business Transformation Agency, where he oversaw all information technology and information assurance operations for the agency, including overseeing all incident response and forensic investigations.

Michael is the Program Coordinator and an Adjunct Professor for Stevenson University’s Master of Science in Cyber Forensics. At Stevenson, he was the recipient of the Rose Dawson Award in 2013. He teaches courses in mobile device forensics, intrusion analysis, and cyber warfare. Michael holds a Bachelor of Science in Chemical Engineering, a Master of Science in Information Assurance, a Master of Science in Forensic Studies (concentrating on computer forensics), and a graduate certificate in Applied Intelligence.

Michael has presented at numerous national and international conferences including DEF CON, the DoD Cyber Crime Conference, InfoSec World, and the BCISS Conference on Intelligence Analysis. He has authored over a dozen journal articles and a book on disaster recovery planning for nonprofit organizations.

IS IT REALLY POSSIBLE FOR A COMPUTER FORENSIC EXAMINER TO RECOVER DELETED FILES?

It depends. When a user deletes a file, the pointers to the file are deleted and the file system is told that it can re-use the storage space, when it is needed. The file, itself, will still reside on the disk until it is overwritten. During a computer forensic examination, it is possible to recover the deleted file until the old content is overwritten. It is also likely that a portion of the file may be overwritten, rather than the entire file, which will result in a fragment of the original file being recovered.

WHAT IS TIMESTOMPING AND HOW EFFECTIVE IS IT?

When files are saved to digital media, such as a hard drive or USB flash drive, the file system stores data, which describes the file. This metadata includes filenames, timestamps, and other information. Timestomping is a form of obfuscation, where a person or piece of malicious software changes the timestamps associated with a file. Timestomping may give the appearance of a file being created earlier or later than what is displayed to the user. As a result, a file can be hidden and made to look like it was installed a long time ago, e.g., when the operating system was originally installed. On the surface, timestomping may look efficient, but most file systems store dozens of artifacts associated with each file, and when timestamps are analyzed across all of this metadata, timestomping typically stands out.

WHEN I NEED TO DISCARD MY CURRENT SMART PHONE FOR A NEW ONE, WHAT SHOULD I DO TO ENSURE THAT MY OLD DATA HAS BEEN DELETED?

When discarding a smartphone, one of the safest ways to ensure that old user data, such as text messages, call logs, or Internet history, is deleted is to complete a three-part process. This includes: 1. enabling encryption on the phone, 2. disabling cloud backups, and then 3. performing a factory reset of the phone. Resetting the smartphone will delete the encryption key and render the old user data unrecoverable. For older feature, i.e. dumb phones, the phone should be physically destroyed to ensure the chips holding data are non-useable. This may mean destroying more than just the screen and keyboard, which are often repairable.

HOW DIFFICULT IS IT TO DELETE MY INTERNET HISTORY ASSOCIATED WITH MY BROWSER?

By default, Internet browsers such as Google Chrome, Microsoft Internet Explorer, and Mozilla Firefox, cache user activity on the computer. This is done to make visiting websites more efficient. The browser will not need to re-download content, when a web page is visited subsequently. User’s can delete their browsers’ caches and cookies; however, until the files are overwritten with new data, the Internet history can be recovered. Additionally, most computers will also store fragments of data with Internet history in other operating system files, such as temp files and swap files, to improve system efficiency. Most computers are connected to Local Area Networks, which employ firewalls and other security devices. These network devices, which a user cannot access directly, will frequently record portions of Internet activity. This information is retained for a time period determined by the administrators.

COMPUTER FORENSICS OFTEN INVOLVES ANALYZING HARD DRIVES FROM COMPUTERS. WHAT OTHER DATA IS ANALYZED AND IS IT CONSIDERED FORENSICALLY SOUND?

Digital forensics, which is broader than computer forensics, frequently involves removing hard drives from computers and analyzing the contents stored on them. This is frequently referred to as “dead box” forensics. In addition to this type of analysis, forensic examiners will
capture and analyze the contents of RAM in a running computer to
gather running processes, passwords, and other volatile data, network
traffic captured by firewalls, routers, and intrusion detection systems,
mobile phones, and system backups. Provided the procedure to
capture and analyze this data is appropriately documented and meets
certain industry standards, these techniques are forensically sound.

WHAT IS THE DISTINCTION BETWEEN A
“SMART” PHONE AND A “DUMB” PHONE?

“Smart phone” is the term used for mobile phones which can do more
than just make phone calls and send text messages. They have more
memory, better screens, more robust processors, have the ability to
surf the web, download/run apps, and establish VPN connections.
They function like computers, which can make phone calls. Android
and Apple phones fall into this class.

Dumb phones can perform only basic functions, such as making calls
and sending text messages. A few of them have some built-in apps
such as alarm clocks and calculators. These phones are smaller, have
low-end processors, typically cannot surf the Internet, and do not
allow the user to download/run third-party apps. Example: the cheap
$10 phone you can buy at the grocery store.

The terms “smart phone” and “feature phone” are real terms and are
actually used in the industry. However, the industry has moved away
from using the term “dumb” phone and went to “feature” phone.

WILL HAVING A PASSWORD ON MY MOBILE PHONE
PROTECT IT FROM HAVING THE DATA ACCESSED?

Many people use passwords to lock the keyboard and screen on
dumb phones. Dumb phones allow a user to lock their phones
to avoid the so-called “butt dialing” or to prevent a stranger from
picking up the phone and scrolling through it. The passcode typically
does not lock the data port on the phone. Therefore, in many, but not
all situations, a mobile device forensic tool can be used to conduct
an acquisition of the locked phone, which will recover the user data
from the phone. On smart phones, the password may or may not
protect the phone and its data from being accessed. Popular mobile
device forensic tools have been configured to access many, but not
all locked phones. It will vary on a case-by-case basis. Locked iPhones
(4S and newer) and BlackBerries typically enable encryption to
prevent unauthorized access to the phone. For Android phones,
“USB debugging” should be disabled, when it is not in use to
ensure data is not accessed through the micro-USB port.
Regulations for Off-Balance-Sheet Financing Produce Risky Financial Statements
Crystal Abraham

Is it true that off-balance-sheet financing creates financial reporting discrepancies due to the failure of appropriate and comprehensive regulations? As permitted by the Financial Accounting Standards Board (FASB) and Securities and Exchange Commission (SEC), accounting methods are devised to allow corporations the financial power to eliminate debt from their balance sheets. Corporations engage in off-balance-sheet financing to hide their financial risk from creditors and investors. Off-balance-sheet financing does not appear as a liability on a corporation’s balance sheet. The opportunity to present a healthy balance sheet by lowering its debt-to-equity ratio allows a corporation greater access to credit at more favorable rates. This false depiction of a corporation’s financial position does not provide creditors or investors accurate information for sound financial decision-making. Off-balance-sheet financing provides the illusion that a corporation controls its liabilities when in fact it is burdened with more debt than it presents. Based on the flexibility in accounting regulations for off-balance-sheet financing, the corporation retains an advantage over the potential creditor or investor regarding the accuracy and true financial position presented.

Off-balance-sheet financing has been problematic since the 1920s. In the white paper, Make Markets Be Markets, Frank Partnoy and Lynn Turner explain that there is no transparency in off-balance-sheet financing, which makes it impossible for financial statement readers to assess a corporation’s true risk (Partnoy & Turner, 2010, p. 85). Transparency in a corporation’s balance sheet is vital to the financial statement reader, so there is a clear understanding of overall financial risk. Transparency entails disclosure of all assets and liabilities. However, disclosure may never materialize unless effective enforcement of current regulations occurs.

Financial reporting regulations are developed and written broadly to provide corporations flexibility in applying accounting practices suitable to their industry (Mulford & Comiskey, 2002, p. 25). Corporations may abuse this flexibility through creative accounting practices. These creative accounting practices allow corporations to exercise certain aspects of regulations in an aggressive manner, which alter the corporation’s financial results and financial position in order to create a potentially misleading impression of its business performance (Mulford & Comiskey, p. 26). As a result of flexible financial reporting regulations, corporations may engage in off-balance-sheet financing, which ultimately provides financial statement readers a false financial representation.

In the article, “Off-Balance-Sheet Financing: Holy Grail or Holey Pail?” Paul Bahnson and Paul Miller describe off-balance-sheet financing as “one dirty little secret of financial reporting” (Bahnson & Miller, 2010). Apparently, managers intentionally seek accounting methods that allow them to acquire large amounts of debt while keeping the same off the corporation’s balance sheet. Although off-balance-sheet financing techniques are in compliance with Generally Accepted Accounting Principles (GAAP), such accounting treatment is considered unreliable and deceitful. A manager is responsible for disclosing all financial transactions in a corporation’s financial statements for the purpose of informing readers of the corporation’s financial health. In essence, a manager who deliberately omits truthful and/or useful information from a corporation’s balance sheet in order to encourage users to make faulty decisions can be perceived as a fraudster. Fraudulent performance can create a corrupt environment in a corporation and adversely affect creditors and investors.

Regulations must affirm the integrity of financial reporting in order to assist creditors and investors with making sound financial decisions by restricting corporations from hiding liabilities thus presenting a false financial picture. As a duty to the investing community, regulations must be revised to prevent corporations from misleading financial statement users through deceitful reporting techniques.

Examples of off-balance-sheet financing include: equity method, lease accounting, pension accounting, and special-purpose entities (SPE). Equity investments may be reported as available-for-sale securities thus implying a ready source of gains regardless of actual value. The equity method is often preferred over consolidation to net out the subsidiary’s liabilities, so these liabilities are not part of the corporation’s debt. Corporations may report leases as operating leases to avoid a recording obligation under capital leases. Corporations are permitted to net pension assets against pension liabilities, which misleads financial statement readers to believe that the assets will be available to cover pension liabilities. A corporation can simply avoid recording the liabilities of an SPE by not reporting the entity on its balance sheet, therefore, improving its debt-to-equity position.

A corporation must account for its investments in equity securities based on ownership percentage and significant influence over the investee (company); wherein a corporation, which has a high ownership percentage and exercises significant influence over an investee, will encompass the power to participate in the operations and financial decisions of the investee. If a corporation owns less than 20% of a company’s total capital stock, and does not exercise significant influence, then it may record its equity investment as trading securities or available-for-sale securities. If a corporation owns between 20 to 50% of the total capital stock, and has significant influence, then it would apply the equity method. If a corporation owns more than 50% of the common stock, and controls the company’s operations, then it must apply the consolidation method (Kertz, 2003, pp. 54-55).

A corporation may record equity investments as trading securities or available-for-sale securities. Trading securities are those to be sold in the near future. Available-for-sale securities are neither held-to-maturity securities nor trading securities (Kertz, 2003, p. 54). The primary difference between trading securities and available-for-
The investee is classified as a subsidiary under the consolidation method. To avoid consolidation a corporation may prefer to apply the equity method instead of consolidating the subsidiary's financial results with its financial statements. To avoid consolidation a corporation will deliberately develop an affiliate with ownership slightly below 50% to avoid consolidation (Ketz, 2003, p. 64). Under the equity method, the investment account reflects a net amount consisting of the company's assets and liabilities. If the company's assets are greater than their liabilities, then essentially the company's liabilities will be hidden (Ketz, 2003, p. 70). Therefore, the corporation will not report the liabilities of the company on its balance sheet, and essentially lower its debt-to-equity ratio. Creditors and investors favor a lower debt-to-equity ratio because the corporation's ratio portrays a promising investment/return option with minimal risk. Although a corporation may have less than 50% ownership in a company, it can still have total control over the company's operations; and therefore, it must consolidate both operations in its financial statements (Ketz, 2003, p. 70).

An effective auditor must evaluate the corporation's procedures for identifying and properly accounting for investment transactions. It may be necessary to request the names of all joint ventures from appropriate management personnel, and determine if the corporation controls the operating, investing, and financing decisions of the company by examining executed copies of agreements, contracts, invoices, cash receipts, and bank statements. The auditor should obtain independent third party confirmations with banks, guarantors, agents, and attorneys, to discuss and verify the accuracy of significant information for a better understanding of each transaction. If the corporation has employed the equity method when accounting for any joint ventures, which it clearly controls, then the auditor must determine if the corporation was hiding the subsidiary's debt in order to keep it off the balance sheet instead of consolidating the operations. To determine the impact of utilizing each accounting method, the auditor will need to obtain financial statements for each company to consolidate the financial results of the operations. To determine whether there are any financial risks for the given period, the auditor can calculate the debt-to-equity ratio using the corporation's financial results under the equity and consolidation methods. The auditor may also perform a horizontal analysis of operating revenues, cost of goods sold, gross profit, and operating expenses to determine whether the implications of the differences suggest that the parent company is hiding debt with the equity method.

In, “How Leases Play a Shadowy Role in Accounting” a Wall Street Journal review of annual reports for companies in the Standard & Poor’s 500-stock index reveal a total of $482 billion in off-balance-sheet operating-lease commitments out of $6.25 trillion reported as debt (Weil, 2004). Accounting for leases represents an opportunity for corporations to mislead creditors and investors. The two types of leases are operating and capital. An operating lease represents a rental for a short period. In contrast, a capital lease ultimately represents a purchase through the method of financing over the life of the lease (Ketz, 2003, p. 73). Corporations may seek to structure their leases to appear as operating leases for the purpose of hiding debt; however, certain aspects of leases clearly distinguish the two types.

---

1The investee is classified as a subsidiary under the consolidation method.
Accordingly, a corporation may disguise a capital lease as an operating lease by arguing the following criteria stipulated by FASB Statement No. 13:

1. Passage of title to the lessee
2. Bargain purchase option
3. Lease term equals or is greater than 75% of the useful life of the asset
4. Present value of the minimum lease payments equals or is greater than 90% of the fair value of the property

If any one of these criteria is met, then the lease is treated as a capital lease. However, if all four criteria fail, then the lease is treated as an operating lease (Ketz, 2003, p. 89).

First, the passage of a title from the lessor to the lessee usually does not occur until the end when all lease obligations are complete; therefore, allowing a corporation to claim this criterion has not been met. Second, the option to purchase at a bargain price may not be established until the end of the lease, wherein this criterion may not suffice until that point. Third, the length of the lease’s term is a significant factor in determining whether the lease is categorized as an operating lease or a capital lease. If the lease represents 75% or more of the useful life of the asset, then it appears that the lessee has completed a purchase transaction. Again, this criterion may not be met until the length of the lease has reached 75% of the useful life of the asset. Last, the fourth criterion suggests that if the present value of the minimum lease payments is comparable to the total fair value of the asset, then the lessee has completed the purchase. Leases may be devised to reflect the present value of minimum lease payments just below the stated criterion for the purpose of disguising the lease as an operating lease (Ketz, 2003, p. 89). Therefore, a corporation may report a lease as an operating lease to avoid recording a capital lease obligation. Gerald Lander and Kathleen Auger in “The Need for Transparency in Financial Reporting” note that establishing precise guidelines in terms of percentages allow corporations to structure their lease agreements in order to achieve the greatest benefit (Lander & Auger, 2008, p. 33). A lease agreement may be structured to represent 74% of the asset’s useful life, yet the present value of the minimum lease payments reflects 89%, thus creating conditions favorable to an operating lease designation.

In *Hidden Financial Risk: Understanding Off-balance-sheet Accounting*, Edward Ketz argues that a lessee may claim ignorance to avoid reporting a capital lease. A lessee appears ignorant of the implicit rate of return used to calculate the present value of the minimum lease payments. This approach is unlikely as the information can be obtained from the lessor. However, if the implicit rate of return is a true unknown, the FASB permits the lessee to use the borrower’s incremental borrowing rate (a standard interest rate applied to payments for financing a purchase), which is usually higher than the implicit rate of return. Utilizing a higher rate to discount the minimum lease payments to present value will consequently lower the probability of payments totaling or exceeding 90% of the asset’s fair value (Ketz, 2003, p. 90). This provides the lessee flexibility in utilizing either the implicit rate of return or the borrower’s incremental borrowing rate to discount the minimum lease payments. Although the FASB requires the lessee to use the lower rate of the two if known, the lessee may actually employ creative accounting practices by selecting the higher rate to discount the minimum lease payments to reflect less than 90% of the asset’s fair value (Ketz, 2003, p. 90).

Another technique to avoid capitalizing a lease is not guaranteeing the residual value. Unguaranteed residual values do not require a payment from the lessee at the end of the lease term; therefore, the FASB specifies that unguaranteed residuals cannot be included in the minimum lease payments (Ketz, 2003, p. 91). Unguaranteed residual values can lower the total value of the minimum lease payments to equal less than 90%. A lessee may require unguaranteed residual values when structuring a lease agreement so as to lower the total value of the minimum lease and to report it as an operating lease. The connection between the two rate types (implicit rate of return and borrower’s incremental borrowing rate) and the unguaranteed residual value is that the lessee may abuse the flexibility provided in the FASB accounting regulations for off-balance-sheet financing. The flexibility of these particular regulations are problematic for creditors and investors as they do not provide the corporation’s accurate financial profile.

In comparison with unguaranteed residual values, contingent rental payments are also excluded from minimum lease payments. In exchange for a standard monthly lease payment, the lessee may require a lessee a lower monthly lease payment with a contingent percentage of sales each month to lower the total value of the minimum lease payments (Ketz, 2003, p. 91). Consequently, the lessee will avoid reporting the lease as a capital lease; since the total value of minimum lease payments only includes the lower monthly lease payments discounted to present value i.e. the total value equals less than 90%. All of these methods are in accordance with the FASB regulations for lease accounting. However, the methods result in customized lease agreements beneficial to only one party.

To detect hidden financial risks, an effective auditor must examine the corporation’s lease agreements in accordance with FASB Statement No. 13. The auditor must determine the following: identify type and accounting of leases (operating or capital); verify present value computations and determine appropriateness of the discount rate used; ensure lease agreements specify whether the residual values are guaranteed or unguaranteed; identify existence of contingent rental payments; and vouch the lease payments and expenses to the provisions of the lease agreements to obtain a better understanding of these transactions. In addition, the auditor can pursue independent
third party confirmations from each lessor to discuss and verify the accuracy of lease terms for a better understanding of the corporation's lease accounting practices. It is imperative to ascertain whether the lease amounts and footnote disclosures in the corporation's financial statements are accounted for in accordance with FASB Statement No. 13.

There are two types of pension plans offered by employers: the defined contribution plan and the defined benefit plan. A defined contribution plan allows an employer and an employee to contribute funds to the pension plan in which the funds are then used to make investments until the employee retires (Ketz, 2003, p. 106). In the defined contribution plan, the employee contributes funds to the plan, which the employer may match depending on the agreement between the employer and the employee. Conversely, in a defined benefit plan, an employer guarantees to pay the employee an agreed amount once the employee retires, wherein the employer is burdened with this long-term obligation (Ketz, 2003, p. 107). Based on the agreement between the employer and employee, the amount paid after retirement is determined at the employer's discretion.

In the book Hidden Financial Risk: Understanding Off-balance-sheet Accounting, Ketz warns “…we cannot believe the pension costs that most corporations report, for the FASB engages in some fairy-tale magic” (Ketz, 2003, p. 117). Corporations may exercise greater flexibility in accounting for a defined benefit plan than a defined contribution plan because they determine the funding amount, and measure the present value of the projected benefit obligation paid after retirement as well as the service costs for the annual impact on the pension commitments. In addition, the employer must calculate the interest cost and expected return on plan assets for the net pension cost (annual service cost plus interest cost minus expected return on plan assets), which is reported on the income statement. The net amount (previous balance minus net pension cost plus funding) is reported on the balance sheet as either an asset account, prepaid pension cost (if positive), or a liability account, accrued pension cost (if negative). The net amount should also equal the plan assets (previous balance plus the expected return on plan assets plus any additional funding) minus the projected benefit obligation (Ketz, 2003, pp. 107-113). Accordingly, corporations may employ creative accounting practices for a defined benefit plan by manipulating the net amount reported on their balance sheet as a prepaid pension cost or accrued pension cost and/or estimating a higher interest rate to calculate the projected benefit obligation and expected return on plan assets. This will lower the corporation's liabilities and hide its pension debts (Ketz, 2003, p. 118). A corporation is permitted to report a net amount on the balance sheet however the corporation's assets may exceed its liabilities, and a positive amount will result in an overfunded pension plan; wherein this amount is only an illusion, because the corporation is permitted to avoid reporting the liability on its balance sheet. Assets often exceed liabilities resulting in a positive net amount; however, financial statement readers should be able to identify the assets as well as the liabilities separately, in order to make sound financial decisions.

A study conducted by the SEC revealed “…defined-benefit pension plan obligations and assets reported by the population approximate $1.320 trillion and $1.119 trillion, respectively… pension plans for the population may be underfunded by approximately $201 billion on a net basis” (United States Securities and Exchange Commission [SEC], 2005, p. 55). The FASB permits corporations to net pension assets against pension liabilities; however, the netting of the pension assets against the pension liabilities can mislead financial statement readers to believe that the assets will be there to cover the pension liabilities. As noted by the SEC’s study on the United States population, pension assets and pension liabilities should be reported separately, so creditors and investors can determine the corporation's pension fund status. To obtain a true representation of the corporation's pension costs, a prudent creditor and investor must adjust the prepaid pension cost or accrued pension cost account on the balance sheet to separate the projected benefit obligations from the pension plan assets (Ketz, 2003, p. 123). In reviewing a corporation’s pension costs, financial statement readers use a corporation's balance sheet by allocating pension assets to the assets section and pension debts to the liabilities section. In addition, estimates of interest rates must be evaluated for reliability, since these factors of measurement can be easily manipulated.

Established in 1970, special-purpose entities (SPE) are another method for a corporation to hide debt, wherein a separate entity is created and operated for a specific purpose such as financing (Ketz, 2003, p. 126). SPEs have evolved over time and assumed different values within the business community. A corporation may create and structure a SPE to obtain credit at a cheaper price, decrease its income tax liability, or avoid consolidating its liabilities on the balance sheet (Ketz, 2003, pp. 127-128). Critics believe SPEs are a new mechanism to conquer deception in order to mislead creditors and investors, while advocates argue SPEs aid in hedging risk. Ketz states “…the government’s pension fund known as social security is a massive SPE that the federal government maintains for the express purpose of hiding the debts from its citizens” (Ketz, 2003, p. 128).

Consolidation is the key issue when accounting for SPEs. In comparison to accounting for equity investments, a corporation that controls another entity's operations must apply the consolidation method when accounting for an SPE. In recent times, concerns regarding SPE consolidation were elevated by investors, the SEC, and the President’s Working Group on Financial Markets. The FASB addressed these concerns in FASB Statement No. 167. The revised regulation requires a corporation to consolidate an SPE if it has the “ability to direct the activities of the entity that most significantly affect the entity's economic performance” i.e. a corporation must...
consolidate SPE in which it has a controlling interest (American Institute of Certified Public Accountants, 2009).

Off-balance-sheet financing does create financial reporting discrepancies due to existing loopholes in accounting regulations, which prevent creditors and investors from obtaining a corporation’s true financial profile. Corporations view off-balance-sheet financing as an accounting tool used to reflect a lower debt level and hedge risk. However, off-balance-sheet financing is perceived by creditors and investors as a practice and a detriment because it affects the financial reporting integrity. The FASB and SEC should disallow off-balance-sheet financing, and require corporations to accurately report all of debt on the balance sheet.

Off-balance-sheet financing is not a trick of the trade – it is fraud. Off-balance-sheet financing has existed for almost a century, thus transparency is hampered within the financial industry. Off-balance-sheet financing must be eliminated, and regulations revised to encourage integrity and allow sound financial decisions by financial statement readers.

REFERENCES


CRYSTAL ABRAHAM

Crystal Abraham is a Graduate Student at Stevenson University focusing on Accounting in the Forensic Studies master’s degree program. Ms. Abraham has 16 years of experience in the financial industry, and is currently employed as an Auditor by the Defense Contract Audit Agency. Ms. Abraham holds a Bachelor of Science in Accounting from the University of Baltimore.
Proactive Data Analysis to Prevent and Detect Fraud in Small Businesses

Robert E. Bates

Large public companies are accountable not only to shareholders but to lenders and government regulators. Leaders of large public companies have a fiduciary duty to protect the assets of the company from fraud. In the most recent Report to the Nation on Fraud, the Association of Certified Fraud Examiners (“ACFE”) found that “a typical organization loses 5% of revenues each year to fraud” (ACFE, 2014a, p. 4). A critical concept in preventing fraud is to build and maintain a strong internal control environment. One important control is proactive data analysis.

Proactive data analysis is accomplished with the use of sophisticated software applications that comb through massive volumes of data to determine weak spots in the control system. By analyzing data in this manner, large companies can prevent fraud from happening or detect an ongoing fraud scheme. The ACFE study revealed that “of the anti-fraud controls analyzed, proactive data monitoring and analysis appears to be the most effective at limiting the duration and cost of fraud schemes” (ACFE, 2014a, p. 38). By performing proactive data analysis, fraud schemes were detected sooner, limiting the total potential loss. Data analysis is not a new concept, but with the increasing number of electronic transactions due to advances in technology, analyzing large volumes of data has become more complex and costly to implement and manage.

Small businesses have a similar accountability to owners and shareholders but are not as highly regulated by the government since they are not public companies. The leaders of small businesses share the same fiduciary duty as large businesses: to protect company assets. Since the average company loses 5% of revenue to fraud, it stands to reason that preventing losses due to fraud could increase profitability by 5%. When viewed in this light, many small businesses should take a second look at implementing stronger fraud prevention controls.

In the ACFE’s Report to the Nation on Fraud, it was reported that small businesses tend to be victims of fraud more frequently than large businesses because small businesses have limited financial and human resources (ACFE, 2014, pp. 4, 32). In terms of fraud prevention and detection, having fewer resources overall translates into having fewer resources dedicated to strong internal controls. The Report also stated that small businesses (less than 100 employees) experience significantly larger losses percentage-wise than larger businesses (greater than 100 employees) (ACFE, 2014, p. 4).

Since small businesses do not have the resources to dedicate to fraud prevention and detection, they are not able to detect fraud schemes as quickly, prolonging the scheme and increasing the losses to the company.

When determining the type of human resources available in a company to prevent or detect fraud, any of the following employees could be beneficial: accountant, controller, accounting manager, fraud examiner, forensic accountant, financial analyst, fraud investigator, and CPA. For the purposes of this paper, they will be referred to inclusively as “fraud examiners.”

In light of this situation where small businesses experience a disproportionate share of fraud losses when compared to large companies, this paper will explore the proactive data analysis tools available and how they can be implemented as internal control, to prevent and detect fraud. The starting point is to understand what anti-fraud internal controls are available and effective.

ANTI-FRAUD INTERNAL CONTROLS

There are three types of controls that should be part of any internal control system: preventative controls, detective controls, and corrective controls (Wood, Brown, & Howe, 2014, p. 24). Preventive controls are put in place as a way to stop fraud from occurring. Segregation of duties and authorization are two examples that are the simplest to implement in a small business. Preventive controls are the gatekeepers of fraud. Detective controls are designed to identify a fraud that has already occurred, such as a supervisor performing a monthly bank reconciliation. If these controls are properly monitored, they can detect a fraud scheme in its early stages. Corrective controls are put in place once a detective control has been breached. A good corrective control might include additional training for employees on how to prevent and detect fraud. Sometimes it is not clear what type of control a procedure is. A preventative control that many confuse as a detective control is an external financial audit. In the past, a common misconception about external audits was that they should detect an existing fraud. However, most audit procedures are designed to determine if the financial statements are “free from material misstatements.” While an external audit may detect an ongoing fraud, it is actually preventative in nature, as it gives the perception of detection to an employee who might consider committing fraud.

Certain controls are anti-fraud by nature and can prevent and detect fraud, including conducting external audit of a financial statement, maintaining an internal audit department, having an independent audit committee, management review of financial statements, providing a hotline to company employees, implementing a company code of conduct and anti-fraud policy, and pro-active data monitoring (ACFE, 2014b, p. 31). While most of these controls are common for large companies, small businesses have difficulty implementing some of these controls because of their limited financial and human resources.

Hiring an external auditor to audit financial statements and maintaining an internal audit department are large costs for a small business to absorb. External audit fees have increased disproportionately since the implementation of the Sarbanes Oxley Act. The Act placed a higher level of accountability on external auditors by requiring them to perform an increased
level of internal control testing. More work causes fee increases. Preparing for an audit can also impact the human resources of a company because of the significant time commitment from a company's financial employees. To endure an external audit, a company needs to have strong financial controls in place prior to the audit. This requires years of implementation and training. Finally, an external audit is regularly a requirement for bank loans and regulatory agencies, such as the SEC. When a company does not need an external audit for these purposes, they may not want to allocate company resources to this control.

An internal audit department is also cost prohibitive for a small business because it comes with inherent base costs. Internal auditors should be independent from all other company functions since they will be auditing the work of other employees. To be effective, this department should have dedicated staff that does not perform other accounting functions. This requires that a company have a large enough workload to keep internal auditors busy on a full-time basis. Again, it is difficult for a small business to employ internal auditors solely because the costs are too high.

Small businesses need to focus on those controls that will provide the largest impact at the lowest cost. Examples of affordable fraud prevention controls are an anti-fraud policy, management review of financial statements, and data analysis.

An anti-fraud policy is a great way for a company to convey to its employees management's position on fraudulent behavior. An anti-fraud policy discusses the scope of the policy, the responsibilities of management in preventing and detecting fraud, what acts are considered fraud, investigative responsibilities, how an investigation would be conducted and reported, and protection to whistleblowers (ACFE, 2014b, p. 1). This is a relatively low cost control, but it can result in a big impact. Employees will know that management does not take fraud lightly, and this can enhance the perception of detection, which is an employee's belief that he or she will be caught. By specifying investigative responsibilities, it signals to employees that allegations of fraud will be investigated. Employees will also see that whistleblower protection is in place if they were to report suspicious behavior. This encourages employees to step forward when they see something that doesn't appear right. Overall, a fraud policy sets the "tone at the top," the perception that management values honesty and integrity. When management takes fraud seriously and emphasizes ethics and good business values, the culture of a company usually forms around their leadership principles.

Another cost effective anti-fraud control is management's review of financial statements. Top management understands the effort that is exerted and the rewards that should be derived. A regular review of company financial statements can corroborate this understanding. Management usually has a feel for where numbers should be: when actual numbers do not meet their expectations, they can allocate resources to find a resolution to variances.

When red flags arise, such as declining margins and lack of cash flow, further investigation may be warranted to determine if fraud is occurring. One of the strongest aspects of management's review of financial statements is the perception it gives to other employees. If employees know that a knowledgeable executive is reviewing the financial statements, it increases the perception that they might get caught, which can prevent fraud from occurring in the first place.

The ACFE’s Report to the Nation on Fraud found that only 15% of businesses under 100 employees performed proactive data analysis, while 41.9% of businesses over 100 employees did (ACFE, 2014a, p. 32). This is a sign that many small businesses could be doing a basic level of data analysis, but are not. The largest costs associated with data analysis are software costs and employee time to perform the analysis. With respect to employee resources, data analysis is a control that can be performed by a variety of employees, such as a financial analyst, an accountant, an external consultant, a controller, or even the CFO. The level of data analysis should be structured to fit within the cost structure of the company. While larger companies may be able to assign a full time analyst to handle these responsibilities, smaller companies may only be able to allocate a portion of their time to this task. For smaller businesses, they need to look for basic data analysis techniques that can be easily implemented.

**HISTORICAL DATA ANALYSIS TECHNIQUES**

The most basic data analysis techniques are taught in introductory accounting courses: vertical analysis, horizontal analysis, liquidity ratios, and profitability ratios (Mantone, 2013, p. 22). Large public companies are required to prepare these type of calculations for their filings with the Securities and Exchange Commission. For small businesses, these ratios and analyses can be calculated by using two of the basic financial statements found in any accounting software: the income statement and the balance sheet. By comparing the results of these calculations to prior periods or to industry peers, significant variances can point to areas where fraudulent transactions may have occurred. This type of data analysis can be performed in a tabular format and the results used to create visual aids. Charts and graphs are a great way for a fraud examiner to visualize variances and trends (Mantone, 2013, p. 29).

A vertical analysis views each item of the financial statement as a percentage of a base amount. For instance, a vertical analysis of the income statement would calculate the percentage of each item in relation to a base amount. Sales would be the highest percentage at 100%, and net income or loss would be the lowest percentage. Specific components of the analysis can then be compared to an analyst's projected outcome. Are margins in-line with management's projections? How do the company's margins compare to their competitors?
A horizontal analysis compares trends of data over time. It calculates the variance of a financial statement line item between two periods and then calculates a percentage increase or decrease. Again, these variances are measured against an analyst's expectations. For both the vertical and horizontal analysis, variances that are outside the expectation should be investigated. For example, a horizontal analysis comparing the income statement of the current year to the prior year would reveal if there were significant declines. Decreases from the prior period might appear reasonable because of declining economic conditions or a diminished demand for the company's products. But if the same decreases do not appear reasonable, it may mean that there is fraudulent activity and further investigation is required.

Liquidity ratios, which are fairly easy to calculate, are the working capital and current ratio. These ratios determine the ability of a company to meet its debt obligations. Working capital represents the excess of current assets over current liabilities. Low or negative working capital is a red flag to investors and creditors, signaling that the company may not be able to conduct basic operations in the future. These ratios are also used in debt covenants that a company may be required to meet in conjunction with a loan. A struggling company might be tempted to manipulate a covenant calculation in order to prevent a loan default (Mantone, 2013, p. 20).

The most common profitability ratio is the gross profit margin. This ratio is very important for manufacturing companies. Positive trends in the gross margin are a good indicator of the strength of a company. Negative trends in the gross profit margin may signal that cost of sales are increasing, which may mean that the company is paying more for inventory. These increased inventory costs may be the result of market trends, but they could also represent a kickback scheme by a company employee.

A more complex calculation used by fraud examiners is the Benish M Score Model. This calculation uses eight financial indices that may point to financial statement fraud. All of these indices can be calculated by using the balance sheet and income statement. The eight indices are the days’ sales in receivable index, gross margin index, asset quality index, sales growth index, depreciation index, selling, general and administrative expenses index, total accruals to total assets index, and leverage index. A normal result is -2.22. Variances from this base result may point to financial statement manipulation (Mantone, 2013, p. 119). Investigating the individual variances of each index, which have a benchmark of “1” or “0”, will point to the areas where fraud may have been committed. The Benish M Score is not too complex for a small business to calculate but would most likely require a seasoned internal financial professional or external fraud examiner to interpret the results.

Benford’s Law is a calculation commonly used by fraud examiners to detect fraud. This calculation does not require expensive data analysis tools and can be calculated using Microsoft Excel. Benford’s Law analyzes “the frequencies of digits in each position of the number for naturally occurring numbers” (Mantone, 2013, p. 239). In Benfords’ research, he tested over 20,000 different observations of numbers. For each of the numbers 0 to 9, Benford determined the probability of each of those numbers occurring in the first, second, third, or fourth numerical position. As an example, for the number 1,562, “1” is the first position, “5” is the second position, “6” is the third position, and “2” is the fourth position. According to Benfords’ findings, the number “1” has a 30% probability of occurring in the first digit (Mantone, p. 239). Since naturally occurring numbers can be predicted, unnaturally occurring numbers would fall outside of the probability results of Benford’s calculation. Unnatural numbers could be those created by a person committing fraud.

To perform a Benford’s Law calculation, a fraud examiner would obtain detailed transactions of a company and apply Benford’s Law to that data set. Any numbers that fall outside the range of the expectations of the calculation would be areas of further investigation. A good way to determine the outlier transactions is to create a graph or chart. Benford’s Law has been deemed successful in detecting past frauds and many of the popular data analysis applications include it as a standard calculation. Analyzing the results of Benford’s Law will require a fraud examiner that has a good understating of accounting. While Benford’s Law alone cannot prove that fraud exists, it is a strong indicator of financial transactions that have suspicious characteristics. Benford’s Law would not be costly or too time consuming for a small business to implement: several templates can be found with a simple internet search.

All of the above calculations can be performed with Microsoft Excel and Microsoft Access. These are off-the-shelf tools that a fraud examiner can use to perform analytical calculations. “The availability of computing power in Excel and Access and the relatively easy access to audit tools...known as CAAT, have accelerated the analytical review process. With access to the accounting server and related applications to the general ledger…CAATS are very powerful companions” (Wood, et al., 2014, p. 75).

Microsoft Excel has evolved into a powerful data analysis tool. Early fraud examiners might have been able to visually scan the general ledger looking for transactions that met a specific set of criteria, but today the volume of transactions make that a time consuming and inefficient process. Until the early 1990’s, not every business was conducted with the assistance of a computer. A computer might only have been used to perform specific complex calculations or tasks. The majority of business transactions were performed manually with paper documents. Many early users of Microsoft Excel used the program to calculate complex financial calculations, such as interest rate calculations, present value calculations, or internal rates of return on investments.
Financial institutions were early implementers of using computer systems on a transactional basis. Banks and credit card companies emerged as the first users of “data-driven” information security. Accordingly, they have been using fraud detection techniques for decades. The original fraud detection processes were costly to implement because they were custom built for each system (Jaeger, 2014).

Most small businesses now use Microsoft Excel to perform data analysis. Excel can pull data directly from outside data sources. This allows Excel to analyze transactions from a source that does not have analysis capability. Excel also has a strong search function. This advanced search capability allows a user to focus only on transactions that meet a specific criteria, such as potentially fraudulent transactions.

Analytics are what Microsoft Excel does best. Filters allow a user to show certain criteria in a list while hiding the rest of the data. Sorting allows a user to view data in a certain order, such as numerically from lowest to highest. This can be an easy way to isolate potentially fraudulent transactions by determining ranges of dollar amounts. A pivot table is a data visualization tool that combines both the filter and sort functions to specify the data that is extracted. Pivot tables allow a fraud examiner to easily analyze the same source of data in multiple ways. With a data source that has a large number of transactions, this can save the examiner significant time. These are all tools that can assist a fraud examiner detect fraud quickly and with a high degree of accuracy.

An example of how Excel might be used by a fraud examiner is a search for round dollar payments. In many embezzlements, the payment of the stolen funds occur in round dollar amounts (i.e. $1,000, $10,000, or $100,000). By using Excel, a fraud examiner can easily segregate transactions that meet this search criteria. Once the suspect transactions have been identified they can be investigated for elements of fraud.

Microsoft Excel does have limitations. Each worksheet is limited to 1,048,576 rows and 16,384 columns (Microsoft Corporation, n.d.). For small businesses, this may not be an issue, but for larger companies they would need a higher capacity data analysis tool. Another limitation of Microsoft Excel is that it isn’t always the easiest to use when encountering multiple data sources.

With the use of Microsoft Excel, all of the data analysis techniques discussed above can determine key areas to explore further. However, most will require a higher level of analysis to determine if fraud has been committed. This requires reviewing items on a transactional level.

BIG DATA

Large and small businesses now exist in an environment where transactions must be conducted electronically to accommodate the needs of their customers and to stay competitive. This has created a large volume of transactions called “Big Data.” “Big Data is a situation in which data sets have grown to such enormous sizes that conventional information technologies can no longer effectively handle either the size of the data set or the scale and growth of the data set. In other words, the data set has grown so large that it is difficult to manage and even harder to garner value out of it. The primary difficulties are the acquisition, storage, searching, sharing, analytics, and visualization of data” (Ohlhorst, 2012, p. 1). Fraud examiners experience all of these difficulties in their quest to prevent and detect fraud.

Ensuring that all sources of data are available is critical in determining if fraud has occurred. A fraud examiner must consider all the locations that data is stored. A company might have a server that is networked to individual computers in the corporate office. If the fraud examiner has access to the server, then the individual computers would be accessible as well. However, the company might have offsite locations with remote access to the server. This presents the challenge of accessing data on a computer that does not have a full-time connection. The best scenario would be where the company has those remote computers backed up to cloud-based storage on a regular basis.

Data can also be stored on mobile devices, such as smart phones and external hard drives. Business information that smart phones may contain are e-mails, text messages, phone records, documents, and social media activity. If it is a company device, then the company can have data backed up through the mobile service provider. If it is a “bring your own device” or personal phone that is used for business, it is more difficult to access company related data. Finally, most individual smart phones have personal passwords, so the company might only be able to access information that is backed up, such as emails.

Storage becomes an issue with the volume of transactions that Big Data produces. According to IBM, “every day we create 2.5 quintillion….bytes of data, so much that 90 percent of the data in the world today has been created in the last two years” (Ohlhorst, 2012, p. 2). At a small business, not only do they need to maintain financial records, but they need to keep copies of all e-mail activity and activity related to their websites and social media. These volumes of transactions require adequate storage to maintain daily access as well as storage reserved for a backup copy. As it relates to a fraud examiner, recent court cases have required that companies maintain and provide e-discovery in an electronic format (Ohlhorst, p. 3). This requires a redundancy in data storage.
As a result, cloud-based data storage is growing in popularity due to the ease of access and the affordability. For a small business, it might be more cost efficient to have a cloud solution in place that reduces the cost of IT personnel and server maintenance, repair and replacement. A common scenario would be for each individual employee to have a desktop or laptop computer that uses a cloud drive to store and share company files. Then, those individual computers are backed up to a cloud server on a regular basis, capturing any data that is not already saved to a cloud network drive.

Data may also be stored with outside sources such as banking and website transactions. For example, a company might have a web portal that stores individual sales transactions or customer information but may not import that detail into the accounting system. They may only import an entry of total sales for the day. So, if a fraud examiner were attempting to identify transactions by invoice amount, that data would need to be acquired from the outside source. A good solution for this would be to save copies of the detailed transactions to a .pdf file on a server where it becomes a searchable transaction.

Data may also be stored within a software application, requiring a user to first access that application and then either analyze data within that software or export it to an aggregating database. Once it has been extracted from the software application, it becomes a searchable transaction as well.

To share data, it must be aggregated and stored in a common location. The best solution for storing for a small business is to have all company data backed up and stored to a cloud server. This provides the greatest accessibility for company personnel and fraud examiners.

Once accessibility and storage have been addressed, a fraud examiner will need a way to organize and search through these volumes of data. This type of analytics requires a common tool to consolidate data from multiple sources.

NEW TECHNIQUES IN PROACTIVE DATA ANALYSIS

According to Joseph T. Wells, founder of the ACFE, “data analytics have never been more important or useful to a fraud examiner. There are more places for fraud to hide, and more opportunities for fraudsters to conceal it. Due to its size and complexity, Big Data requires the use of creative and well-planned analytics” (Spann, 2014, p. xi). This type of analytics is above the capabilities of most accounting software products. Since some of the data to analyze exists outside of the accounting system, a fraud examiner will require the help of software tools specifically designed for the prevention and detection of fraud. This level of data analysis requires a program that can analyze multiple sources of data and data types in order to search for patterns that point to suspicious activity.

Performing data analytics requires executing a plan. While each organization may have a specific technique or strategy that is customized to their business model, the plan should consider the following basic steps: 1) develop a plan to collect records, 2) gather data in standard formats, such as a spreadsheet file, a database file, or a .pdf file, 3) enter the data into a central database, 4) review the data for irregularities, 5) analyze the data, and 6) create a report to summarize conclusions (Spann, 2014, p. 27). Following these steps helps with the efficiency of the analysis. For example, specifying ahead of time the formats that the fraud examiner would like to receive will eliminate issues with entering the data into the database. Following these steps can also ensure that the integrity of the data is not compromised.

While there are many data analytic products on the market, most have a specific purpose and target user. Guidance Software’s Encase Forensic is designed for “practitioners who need to conduct…forensically-sound data collection and investigations” as well as “maintain the integrity of evidence in a format the courts have come to trust” (Guidance Software, n.d.). Encase’s target user is a fraud examiner that suspects fraud has been committed and is searching for evidence to use in a legal matter. Accordingly, this product is designed to ensure that digital devices and data are not changed during the investigation. It works well in a situation where data needs to be collected from multiple sources, such as a computer, a tablet, and a phone.

Another forensic software specifically designed for situations where fraud has occurred and evidence needs to be gathered is AccessData’s Forensic Toolkit. The Forensic Toolkit is “a court-cited digital investigations platform” that can “zero-in on the relevant evidence quickly” (Forensic Toolkit, 2014). This will have similar attributes to those of Encase. While both Encase and Forensic Toolkit are highly specialized products to gather evidence once fraud has been detected, they may not be the most practical data analysis tools to prevent fraud.

Caseware’s IDEA is less of an investigative tool and more of a data analysis product. IDEA works best when there are large data sets available, such as 200,000 to 1 million records (Spann, 2014, p. 77). While a small business may accumulate that volume of data in total, after filtering transactions to analyze, there may not be enough data to generate meaningful results.

For instance, IDEA works best on accounts receivable with greater than 300 balances, fixed assets with greater than 2,000 items, inventories with greater than 2,000 items, purchases, and credit card transactions greater than 1,000 per day (Spann, 2014, p. 77).
A small business would not usually have more than 2,000 fixed assets. Likewise, a company having more than 1,000 credit card transactions a day would probably not be considered a small business.

Caseware’s website details the types of files that can be imported such as “spreadsheet and database software, mid-range accounting programs, ERP systems, legacy mainframes, telecom switches, travel and expenses applications, flat and printed files such as a .pdf file, plain text (.txt), and print-report (.prn) files” (Caseware Analytics, n.d.). This enables a fraud examiner to investigate virtually all the data sources. Because most software programs can export data into these formats, acquiring the data and consolidating it with IDEA is fairly simple.

One benefit to an auditor or fraud examiner is that IDEA analyzes data with “read only access” (Caseware Analytics, n.d.). This is important because it preserves the original data source from manipulation by the analysis performed. This is a key factor when the results will be used for an audit or a legal matter.

Additionally, IDEA uses calculations that fraud examiners are familiar with, such as trend analysis and Benford’s Law (Spann, 2014, p. 83). Using familiar calculations saves time on learning new techniques and makes it easier to explain the results. Another benefit is extracting data over a certain threshold, such as a dollar amount, or the ten top or bottom transactions in an account (Spann, 2014, p. 83). These are common analysis points for auditors, so extracting data quickly makes data analysis more efficient.

IDEA is an appropriate product to import, consolidate, and analyze data for large companies. However, because of the minimum transaction sizes, it may not work optimal in a small business environment.

One of the most popular data analysis products is ACL Analytics. ACL Analytics has many similar characteristics of IDEA. ACL can accommodate data source types similar to that IDEA: spreadsheets, .pdf’s, etc. One difference is that the data import can be automated through ACL’s Audit Command Language (ACL, n.d.a.). This allows a user to automate the same tasks each month, so that time is spent analyzing data, not gathering and importing it.

ACL uses several methods to analyze data. First, ACL looks at the classification of data to develop patterns. It then uses stratification to filter out irregularities. It can identify duplicate transactions based on amounts or invoice numbers. Next, it performs gap testing to determine missing numbers in expected sequences. This would be useful in finding missing check numbers. Finally, ACL applies Benford’s Law to analyze the sequence of digits (Spann, 2014, p. 35).

An added ACL benefit to fraud examiners is the “ScriptHub”. The ScriptHub is a library of pre-written analytic tests (ACL, n.d.b). Situations may arise where a fraud examiner will want to perform a specific analysis of data but does not know how to perform the calculation. With the ScriptHub, the fraud examiner can search through ACL’s historical analysis library to find the right one. By having access to the ScriptHub, a fraud examiner can eliminate a learning curve in using the software.

Another ACL product is the free Microsoft Excel Add-In. When installed, the ACL Add-In appears at the top of Microsoft Excel as a tab in the ribbon. The tab is arranged as a series of groups that would simulate the workflow for an ACL analysis (ACL Add-In, n.d.a). By using this tool, a fraud examiner can analyze data in a familiar environment, Microsoft Excel, and access a higher level of analytical tools that have been developed by ACL.

The key to this tool is that all data must be converted into a Microsoft Excel format because the ACL Add-In will analyze data contained in the workbook. As long a data source can be converted to one of the Microsoft Excel readable formats, such as .csv, .txt, or .xml, then it can be converted into an Excel spreadsheet. Most software applications have the capability to export data in one of these formats. One limitation with using the ACL Add-In is that documents such as .pdf’s or application specific data may not be converted into a readable format by Excel. Another limitation is that the user might invest significant time getting data into the proper forma to be analyzed.

After a data source has been selected, the Add-In allows the data to be filtered, sorted, summarized, aged, and stratified. Filtering and sorting are standard Excel features that are automatically enabled by the Add-In. Summarizing is a feature that can be used without having to write formulas to aggregate totals. Stratifying data allows a user to divide the data by specific numeric interval, count the occurrences and apply as the percentages (ACL Add-In, n.d.a). Sampling enables a user to draw a random selection of data from the source (ACL, n.d.b).

While all the proactive data analytic tools discussed have many benefits that a small business can use, the fact that ACL has a free Add-In for Excel means that fraud examiners can implement a data analysis internal control solution at very low cost. The only costs that would be encountered would be the human resource cost. That would include employee time in designing the data analysis structure, in analyzing the data, and investigating the irregularities.

While the ACL Add-In may not have all of the functions that ACL Analytics has, it allows a small business to develop a proactive data solution early on in the company lifecycle. The company could then grow into a more robust analysis program once it has more financial and human resources to dedicate.
SUGGESTIONS AND CONCLUSION

Fraud prevention and detection are issues that both small and large businesses must address. When faced with a potential loss related to fraud of almost 5% of revenues, a company should implement internal controls to prevent those estimates from becoming a reality. Anti-fraud internal controls such as an audit, an internal audit department, a code of conduct, a fraud hotline, and proactive data analysis have been determined by the ACFE to reduce fraud. Specifically, proactive data analysis was found to be the most effective in preventing fraud for small businesses.

The most significant barriers to implementing proactive data analysis at a small business are the reduced financial and human resources available. However, there are cost effective ways to do it. To start, small businesses can perform both a horizontal and vertical analysis on their monthly financial statements and investigate irregularities. They can also calculate profitability and liquidity ratios. Finally, they can calculate a Benish M Score and utilize Benford’s Law.

The next step would be to consider using more advanced data analysis programs. Microsoft Excel has many features to perform data analysis, and it is probably already installed on many computers. Adding the ACL Add-In to Excel can add another layer of advanced analysis that will help make data analysis more effective and efficient.

When a small business reaches a level of profitability where they can incorporate a more advanced data analysis program, they can add a more robust tool such as IDEA or ACL Analytics. Improving controls by adding a specialized software program will require financial resources to acquire it and to train employees. It will also require the dedication of time from employees serving the role of fraud examiners.

Professional organizations such as the ACFE and AICPA have dedicated their time and efforts to ensuring that companies of all sizes are aware of the threats of fraud in the workplace. They have continued to educate the public on fraud prevention and detection. One suggestion to these professional organizations would be to work with accounting software developers and the current developers of proactive data analysis tools to incorporate data analysis reports into their standard products. If a small business had the ability to run an anti-fraud report as a part of their monthly management review of financial statements without having to program the report, it would save a significant amount of company resources. Another collaborative effort between accounting software developers and data analysis tool developers could be an Add-In or App, similar to the ACL Add-In. This may happen in the near future, as Intuit has created an open source database with their latest version of QuickBooks Online. The basis of the new QuickBooks Online product is that QuickBooks will remain the base accounting system, but a user would purchase apps that provide special functions, such as timekeeping and payroll.

What if a small business using QuickBooks Online could purchase an app that would allow them to run an anti-fraud report based on their company data at the push of a button?

Clearly there are resources for small businesses to implement proactive data analysis tools. With the significant advances in technology, new solutions may be on the horizon.

REFERENCES


**ROBERT E. BATES, CPA, CFE**

Mr. Bates is a Certified Public Accountant (CPA) and Certified Fraud Examiner (CFE) with 24 years of experience in accounting and finance. He has accumulated a breadth of experience leading and managing the fiscal and operational functions of companies whose industries include real estate and manufacturing. He has taught accounting theory and fraud examination to college students at Glendale Community College for the last 8 years and holds a Bachelor of Science Degree in Accounting from the University of Southern California.
Terrorism in Cyberspace: Is the U.S. Ready for a Virtual 9/11?
Kera N. Valenti

U.S. ON THE BRINK OF A NEW WAR

In the aftermath of the September 11, 2001 terrorist attacks, physical security measures aimed at protecting the nation’s critical infrastructure increased exponentially. The Department of Homeland Security emerged, the Transportation Security Administration appeared in airports, pilots were afforded the opportunity to carry loaded guns on their flights, barriers were erected around government compounds, and increased police presence became the norm. It took an event as devastating as September 11th to bring about the physical security adjustments necessary to protect against another physical attack. Over a decade later, with the country’s critical infrastructure running its operations in cyberspace, is the United States focusing enough attention on cybersecurity to prevent a virtual version of the 2001 terrorist attacks?

September 11th, in concert with other terrorist attacks on American soil, demonstrated that the physical threat against the United States is real and powerful. Thousands of lives have been sacrificed, the economy altered, and morale devastated all in the name of terrorism. The effects of these attacks are seen and shared in real time. They are shocking, overwhelming, and almost incomprehensible as they replay across televisions, smartphones and computer screens. The critical object lesson imparted is a visible testament of hatred toward this nation and its people.

Americans are now fully cognizant of the physical threat, but cyberspace threats remain an unknown and potentially equally devastating entity. Failure to implement effective cybersecurity measures before the first major cyber attack is a failure to protect. According to former Director of National Intelligence, Mike McConnell, the United States is the “most wired nation on Earth” (McConnell, 2010). Data networks crisscross the nation as American citizens rely on computers to accomplish day-to-day activities, and government and private industry conduct large-scale operations on computer networks. These systems are key to providing the basic services to which people have become accustomed.

WHY CYBER?

Cyberspace is such an important cultural and business asset today that the United States would be crippled without it, increasing the likelihood that terrorists will use the online forum to support their own malicious agendas. Hacking into America’s critical infrastructure operations to use “computers and the Internet connectivity between them to launch a terrorist attack” is the modus operandi (Eastom, 2014). Simultaneously, water, power, nuclear, transportation, and communication systems operating over computer-based programs entice hackers to infiltrate those programs. The ease of creating a weapon out of cyberspace has essentially removed the costs, risks, and preparation associated with carrying out an elaborate physical attack. Simply put, “computers can be used automatically to conduct attacks—even as their attackers sleep, snack, celebrate, and scheme” (Gewirt, 2013, p. 9).

While a cyber attack may not annihilate thousands of people at once, it could cause mass hysteria and a sense of helplessness—both goals of terrorism. What might a modern cyber terrorist attack look like? A terrorist located in Iran notes that a blizzard and subzero temperatures are forecasted to envelop the Midwestern United States in January 2015. By hacking into vulnerable computer systems and using them collectively to deploy distributed denial of service attacks, multiple electrical supply stations would be affected by information overload thus causing them to crash. An entire region would be without power, phones, and heat. Local businesses would shut down. If the attacker completely destroys the technology running those stations, an extended amount of time would elapse until normal operations resumed. At that point, the economy would suffer detrimental consequences and would require an extensive road to recovery. Many Americans would go through a period of hopelessness and would have a heightened sense of fear of future attacks.

This situation is not far-fetched. In 2003, a power outage referred to as “the biggest blackout in North American history” left upwards of 50 million Americans without power for a two-day span. In that short amount of time, approximately $6 billion in damage resulted (Kennedy, 2014). The National Research Council reports, “a systematically designed and executed terrorist attack could cause disruptions that would make the 2003 blackout pale in comparison” (Kennedy, 2014). The fact that terrorists can cause this amount of damage simply by introducing malware into a computer system makes the cyber threat credible.

THE THREAT HAS OFFICIALLY ARRIVED

While the United States has yet to see experience a successful cyberterrorism attack, a January 11th, 2013 Department of Homeland Security report stated, “the number of cyber attacks against nuclear, power, and water infrastructure more than doubled” in the United States between 2011 and 2012 (Department of Homeland Security, 2013, p. 1). Compare that with a “seventenfold” increase in these types of attacks between 2011 and mid-2013 and the threat becomes that much more imminent (Zakaria, 2014). America’s National Nuclear Security Administration reported eight cyber attack attempts on a daily basis (Zakaria, 2014). One successful attack can incapacitate these critical infrastructures and leave America’s livelihood in the hands of the enemy.

It is a matter of time before the evolution of malware, savvy hacking knowledge, and volatile foreign relations come together to produce a successful cyber terrorist attack. “The big fear is that an adversary, in the heat of a cyberwar, might try to take down the U.S. power grid, telephone network or transportation system” (Gjelten, 2010).
Disruption or destruction of these vital services poses serious risks to both national security and economic viability. In order to combat the threat of a major cyber terrorist attack the United States consistently must be one step ahead of its hacking adversaries by identifying and countering malicious intrusion capabilities and employing the most up-to-date, real-time detection and deflection techniques in daily operations. Individuals in the cyber security field believe that “we’re just in the eye of the storm” and, if correct, these precautions must be taken immediately (Hoffman, 2014, p. 1).

A CLOSER LOOK AT THE THREAT

Understanding severity of the cyber threat and develop techniques that eliminate or lessen the impact of a major cyber attack on America’s vital assets, involves greater knowledge of this weapon. Malicious software or malware is essentially a cyber predator. It is deployed with the intention of causing damage to and through computer systems (Malware Definition, 2006). The impending assault on critical infrastructure is one in which a particular type of malware will be utilized i.e. a Botnet Distributed Denial of Service (DDoS) attack. In recent years, American businesses have seen the effects of these attacks, especially where financial transactions are involved and information can be obtained for the attacker's personal gain. However, “more recent research found that ideologically motivated DDoS attacks are on the rise” (Botnet DDoS Attacks, 2014). For a terrorist or terrorist group seeking to penetrate the data networks of America’s vital assets, involves greater knowledge of this weapon.

A RAPID PROGRESSION AND CURRENT CAPABILITIES

Malware had its beginnings in the early 1980s when “Elk Cloner,” the first uncontained computer virus, was introduced to the operating system of Apple II computers (Kerner, 2013, p. 3). From that event the term “virus changed in meaning from infectious microorganisms to malicious computer code” (Kerner, 2013, p. 3). The computer virus soon became a popular and widespread form of malware.

A more recent trend in the world of malware is the DDoS attack which is the most likely weapon in a cyber terrorist’s arsenal. During the commission of a DDoS attack, malware is introduced to a computer in order to infiltrate and overload the system with requests beyond its capability, subsequently causing the server to crash (Holtfreter and Harrington, 2014, p. 33). If the attacker performs a DDoS attack using a botnet—a collection of infected computers from anywhere in the world used to further propagate the attack—the consequences can be increasingly detrimental. (“Bots and Botnets,” 2014).

Through the use of botnets, the strength of DDoS attacks has exponentially increased. Before 2013, the most powerful DDoS attack reported was 100 Gbps (gigabits per second, a measurement of internet traffic). In 2013, an attack referred to as the “attack that almost broke the Internet” reached 300 Gbps, and in 2014, there have been multiple reports of attacks reaching, and possibly surpassing, the 400 Gbps mark (Gilbert, 2014). Experts also predict that within the next year there will be a DDoS attack doubling what has already been witnessed (Gilbert, 2014). In only three years, there has been an 800% increase in the “bogus” traffic DDoS generate, meaning the forecasts for the near future could undoubtedly wreak havoc on America’s critical infrastructure operations and information technology.

Most modern DDoS attacks are “zero-day or zero-hour” attacks (Holtfreter & Harrington, 2014, p. 33). These attacks exploit vulnerabilities by using polymorphic code to automatically and continuously change how the string of code appears on the computer systems, increasing the amount of time available to disrupt a system. It also lengthens the time it takes to detect and generate a patch for an intrusion (Holtfreter & Harrington, p. 33). Polymorphic code and zero-day DDoS attacks sustain and perpetuate the amount of damage inflicted on the information technology infrastructure. Current firewall and intrusion detection system technology possess limited capabilities to detect new and morphing codes and behavior. These technologies are programmed to identify malware signatures from past intrusions and for which developers created a patch. As a result, the effects of these expanding DDoS botnet attacks could “disable trains all over the country… blow up pipelines… damage electrical power grids so that the blackouts would go on for a long time…” according to Richard Clarke, former counterterrorism advisor to President Bill Clinton and President George Bush (Clarke, 2010).

A disturbing trend in cyber warfare is the public dissemination of how to commence one’s own cyber attack as any person with a computer and an agenda is capable of launching a global attack. There are DIY botnet toolkits available for purchase over the Internet and Youtube “how-to” videos detailing the necessary steps to take. The process is both easy and inexpensive. The potential for abuse appears unlimited.

FOREIGN ADVERSARIES BEHIND AN ATTACK

The future possibilities of DDoS attacks would be of little to no concern if the United States were an enemy-free country. However, the United States faces opposition from other nations and independent groups alike. Political and economic disputes have resulted in tumultuous foreign relationships, giving radicals a source of motivation to maliciously use their resources and capabilities. But more specifically, “Russia, China, Iran, and North Korea were listed as cyber threats, along with terrorist organizations and cyber criminal organizations” (Hammond, 2014). Each of these nation-states has previously been involved in widespread cyber attacks using malware, and according to the National Security Agency, Russia and China
have both “probed the electrical grid to find vulnerabilities to exploit if they needed to attack it” (Wingfield, 2012).

It was reported that in 2008 China was responsible for “Ghost Net,” using malware to spy on Tibet for almost a full year (Hruska, 2009). North Korea was accused of using DDoS attacks multiple times since 2009 against the United States and South Korea to disrupt government and financial websites (Vlahos, 2014). In 2007, Russia began “Web War I” on Estonia with a DDoS attack aimed at collapsing the country’s most vital infrastructure through disruption of its electronic operations, marking the “first time that a botnet threatened the national security of an entire nation” (Davis, 2007). Iran has been accused of progressively sophisticated attacks over the last several years, from infecting U.S. banking and military networking systems (Harris, 2014). So, which of these countries poses the greatest potential threat to the United States? Many factors support the idea that a terrorist attack intended to cripple critical infrastructure might originate from Iranian terrorist actors. Not only is Iran capable of using the most sophisticated cyber measures to its advantage, but it is also known for its state-sponsorship of terrorism, particularly towards the United States and its allies. In 2014, Iran’s leaders declared that they are ready and willing to put their cyber warfare tools to use if the situation arises (Harris, 2014).

Although countries such as China and Russia have deeply rooted economic and political ties with the United States, and maintain a viable diplomatic relationship, the theocracy of Iran does not. For Iran’s political and military actors, Islamic ideologies influence their approach to foreign affairs. The combination of Iran’s acceptance and encouragement of physical terrorist attacks, its recent history of cyber attacks, and its ideologically driven decisions pose a significant threat to the United States. Iran has emerged as a cyber threat to monitor over the last several years, from infecting U.S. banking and military networking systems (Harris, 2014). So, which of these countries poses the greatest potential threat to the United States? Many factors support the idea that a terrorist attack intended to cripple critical infrastructure might originate from Iranian terrorist actors. Not only is Iran capable of using the most sophisticated cyber measures to its advantage, but it is also known for its state-sponsorship of terrorism, particularly towards the United States and its allies. In 2014, Iran’s leaders declared that they are ready and willing to put their cyber warfare tools to use if the situation arises (Harris, 2014).

CYBER SECURITY

Regarding malware and cybercrime, “the cybercriminals continue to stay one step ahead of the security experts” (Holtfreter & Harrington, 2014, p. 28). Understanding the web-based malware problem, by knowing what kind of attack to expect and what the attacker may be seeking to accomplish, is the first step in actively recognizing the threat and working towards the ability to counter it. The next step is developing appropriate and effective cybersecurity solutions. This must be done to offer critical infrastructure owners and operators the opportunity to implement the measures necessary to thwart a cyber attack intended to crash their systems. Finally, owners/operators must actually adopt these new measures.

Although various cybersecurity tools exist, in an environment of rapidly emerging malware capabilities, none represent an optimal solution to detect new threats. Instead, security experts must continue to play “catch-up” when developing new detection tools. The principal and foremost means of identifying malicious intrusions and behaviors have been based on recognizing the signatures and anomalies associated with existing malicious codes. When new malware exposes a previously unknown vulnerability, the experts create an update to patch that vulnerability after the fact. This solution is reactive; effective only to prevent future attacks of the same type, and incapable of countering more sophisticated efforts.

Current developments in the cybersecurity field focus on real-time detection technology. In order to address a serious threat as it happens, an intrusion must be identified and halted in real-time, reducing the amount of post-incident clean-up required to control the situation. Several companies have made this approach a priority. A partnership between Bromium, Inc. and ForeScout Technologies, Inc. resulted in a security solution that identifies when a malware attack has been initiated, analyzes associated information, and then isolates other potential vulnerable points within the network to prevent malware from infiltrating the entire system (“Bromium and ForeScout,” 2013). Because this technology collects “precise threat intelligence in real time,” the consequences of a malware attack on a network are far less than if the company were using traditional anti-malware software (“Bromium and ForeScout,” 2013). FireEye has also designated a real-time detection platform aimed at preventing “the next generation of cyber attacks” from devastating businesses and governments around the world (“FireEye,” 2014). Its “cloud-based” technology monitors and analyzes data as it becomes available so that an attack may be identified immediately (“FireEye,” 2014).

Real-time detection and aggressive incident response after an attack is not the optimal solution. The cybersecurity threat must be eliminated before the opportunity to attack a network arises. Prevention is the critical component. Cylance, Inc. has taken an innovative mathematical approach to malware defense. The company created CylancePROTECT, a cybersecurity measure described as having the ability to think almost like the brain of a human security expert, using a mathematical algorithm to identify what is safe and what is a potential threat to a network in real-time, in effect, neutralizing threats before they can attack and cause any damage (“Cylance,” 2014). Within a testing environment, the technology demonstrated a “95 percent detection rate” of malicious threats, and of those detected, it had “the ability to stop 100 percent of what [was] found” (“Cylance,” 2014). This capability appears to be the solution to countering zero-day attacks while minimalizing potential damage to targeted critical infrastructure information networks.

What if malware could be altered? Attackers use polymorphic code to enhance their attack capabilities. With a dynamic string of malicious code, the systems operating software does not recognize the malware as an attack thus permitting the infection to spread.
Throughout the computer network, Shape Security acknowledged the potential role of “real-time polymorphism” from a cybersecurity perspective and invented ShapeShifter, a prototype technology which uses this polymorphic capability to prevent cyber attacks (“Shape Security,” 2014). Knowing that attackers rely on the “static elements” (i.e. the static web codes) of information technology networks to spread their malicious codes, the company is experimenting with polymorphic code on websites to “simply disable the automation that makes these attacks possible” (“Shape Security,” 2014). The ShapeShifter presents a potential solution to eliminating the threat of a major DDoS attack.

CylancePROTECT and ShapeShifter represent cutting edge cybersecurity technology which both the government and private-industry businesses could employ to thwart cyber attacks. For example, to achieve a successful attack on a system currently utilizing polymorphic code in its cybersecurity defense, a terrorist would have to invest a greater amount of time and effort to infect a well-protected system. By that time, they could have moved on to an easier target. The rationale here should be that the United States does not want its critical infrastructure to be the easy target. However, will critical infrastructure operators use this type of forward-thinking technology in their daily operations, or will they remain the comparatively soft targets in the eyes of a terrorist?

A CYBERSECURITY FRAMEWORK & THE ISSUE WITH IMPLEMENTATION

There is undoubtedly a push for businesses to adopt the most up-to-date cybersecurity measures when they conduct vital operations in cyberspace. In 2013, President Obama issued Executive Order (E.O.) 13636, which addressed the cyber threat challenge and stressed the importance of critical infrastructure cybersecurity. E.O. 13636 directed the National Institute of Standards and Technology (NIST) to construct a cybersecurity framework applicable to the critical infrastructure community (Exec. Order, 2013).

Version 1.0 of the NIST framework for improving critical infrastructure cybersecurity was published February 12, 2014 (National Institute of Standards and Technology). The framework consists of three parts: core, profile, and implementation tiers. As a whole, it lays the foundation for businesses to conduct cybersecurity risk assessments and leverage existing best practices to improve cybersecurity overall. The framework allows businesses to map their own course for improvement and describes the key functions of cybersecurity as identify, protect, detect, respond, and recover (National Institute of Standards and Technology, 2014). It includes a list of vetted and proven cybersecurity standards used in the industry. Now that the framework is in place, it is likely to become “an industry standard in litigation,” even though it is currently only a voluntary practice (Adler, 2014). This puts pressure on critical infrastructure operators to adopt best practices in accordance with the framework. For example, should a data breach occur and the company had not implemented best practices available to protect their vital resources, victims could cite NIST framework version 1.0 as proof of the company’s negligence.

The cybersecurity framework recognizes current deficiencies in critical infrastructure systems and sets forth a plan to resolve those difficulties. However, several features render it useless in the event of a cyber terrorist attack. These are: voluntary not mandatory, best practices, and cost.

The first issue is the voluntary nature of the framework. By adopting a voluntary compliance approach, companies will conduct business as usual and invest their time, effort, and money into other operating costs instead of enhanced security measures.

The second issue promotes implementation of current industry standard best practices. These practices were already outdated and irrelevant shortly after E.O. 13636 was signed. If a targeted critical infrastructure operation is to survive the next generation of cyber attacks, it will implement innovative technologies such as CylancePROTECT and Shapeshifter. By relying on industry standards, the NIST framework fails to address the concern of zero-day attacks, which exploit previously unknown vulnerabilities. Only cutting edge technology can prevent such attacks from causing grave damage.

The final issue is the cost associated with making these operational changes. E.O. 13636 stipulates that the NIST framework is supposed to present a cost-effective approach to cybersecurity (Exec. Order, 2013). What defines cost-effective? According to a Bloomberg survey of 21 energy companies, “it would take an average annual budget of $344.6 million per company to stop 95 percent of the threats” (Wingfield, 2012). Unfortunately, the size of public and private-industry critical infrastructure companies varies as do their budgets.

In a 2013 SANS Institute security analytics survey of 647 businesses across critical infrastructure sectors (including government, military, telecommunications, and energy/utility industries), respondents recognized external malware-based threats and advanced persistent threats as the areas that could benefit most from better cybersecurity and admitted that they have gone from one day to ten months before detecting malicious code on their systems (Shackleford, 2013). However, respondents who knew their company’s IT budget reported that < 5% was spent on security management and response (Shackleford, 2013). As stated, it suggests that a tiny fraction of a company’s budget is invested in cybersecurity, and the NIST framework is not a priority.

Lastly, the call to action to improve cybersecurity may require too much change too soon. Many critical infrastructure systems run on
legacy architecture that has only recently become interconnected. Power plants, water supply stations, transportation systems, and other systems use industrial control systems i.e. supervisory control and data acquisition (SCADA) networks and "with the advent of internet-based systems…SCADA networks have gradually become…integrated into larger global networks" ("Cyber Threats," n.d.). For these types of companies, a major and costly transition to wireless remote monitoring systems has only recently occurred. (These systems provide ease-of-use for owners and operators.) Smart grid technology is so expensive that large companies like Baltimore Gas and Electric (BGE), the "nation's oldest and most experienced utility company" had to apply for hundreds of millions of dollars in grants to subsidize the costs of such an initiative (a major investment in cloud-based architecture, and the potential for greater cyber vulnerabilities) (Butts, 2010, p. 1).

Michael Assante, cybersecurity strategist and former chief security officer, National Electric Reliability Corporation, American Electric Power, states, “because the [NIST cybersecurity framework] program offers no financial incentives to help companies reduce the costs of implementing the guidelines, companies may opt not to participate” ("SANS NewsBites," 2014). Consider the ShapeShifter which may cost its customers over a million dollars each year it is utilized after the testing phase is complete (Greenberg, 2014). For large companies such as BGE, implementing the best cybersecurity technology is available may be viable and in line with its priorities, but for smaller businesses, where that figure of <5% of the IT budget is spent on cybersecurity, having the most up-to-date developments in cybersecurity may be cost-prohibitive.

THE PROBABLE OUTCOME

Americans rely heavily on an abundant and uninterrupted supply of resources from critical infrastructure businesses to fulfill basic, everyday functions. An interruption to the power grid, water supply, communications system, or other vital assets remains a credible threat whether conducted on the ground or in the Ethernet. Terrorists are quite capable of executing this type of attack in cyberspace. Countries with which the United States already has tumultuous relationships, including China, Russia, North Korea, and Iran, have proven that they are technologically ready and prepared to engage in a cyber war.

With constant innovation in malware capabilities and a lag in the implementation of effective cybersecurity measures across the critical infrastructure industry, a successful cyber terrorist attack appears probable. More than ten years after 9/11, with the country's most precious infrastructure conducting their operations in cyberspace, the United States has indeed focused a great deal of attention on cybersecurity, but not enough to implement those changes needed to protect these critical infrastructure systems. Only after a cyber attack moves this nation in the same capacity as 9/11 might we see the implementation of the cybersecurity measures necessary to prevent such an attack in the first place. In the words of former Director of National Intelligence, Mike McConnell, "the United States is fighting a cyber-war today, and we are losing" (McConnell, 2010). Cybersecurity cannot keep up with the cyber threat without a proactive approach and commitment of resources.

REFERENCES


KERA VALENTI

Ms. Valenti graduated from Stevenson University in 2009 with a Bachelor of Science in Business Administration. She is currently working towards her Master of Science in Forensic Studies. Ms. Valenti has been employed by the Department of Defense since 2010, where she serves as the lead writer/editor on a technology-focused communications team.
INTRODUCTION

In 2009, a major incident occurred with Internet powerhouses Twitter and Google. An unauthorized intruder accessed a significant amount of Twitter’s corporate and personal records which were stored remotely through the cloud-based application Google Apps. The intruder gained control of this information by accessing a Twitter employee’s email account, and thereby the remotely stored information on Google Apps. Fortunately, no major financial catastrophe occurred. However, the incident raised questions regarding the security environment of cloud computing operations.

Cloud computing is a technology that allows users to store information on virtual servers over the Internet. Users of cloud computing technologies often hire third party cloud providers to manage the data storage. Many businesses are becoming more interested in outsourcing their data processing to cloud providers because of the benefits the cloud offers; however, this fairly new technology comes with potential fraud risks. The attack on Twitter’s storage information servers identified weaknesses in the cloud provider’s security measures and highlighted the importance of implementing a dual security system to protect both the provider and the customer. Fraud prevention and detection techniques used by cloud providers and their customers can reduce potential attacks aimed at cloud-based servers.

THE CLOUD COMPUTING INDUSTRY

Although the computer era began in the early 1940s, this advanced technology was limited to government uses, such as the military. The challenge emerged: how to shrink room-sized supercomputers? And how to create a network of computers? The end results were the desk-size computer and the Internet. The Internet offers massive amounts of information while communicating and exchanging that information on a global basis in real time.

Allowing users to access and share information over the Internet has evolved into the virtual world of cloud computing. Cloud computing allows users to store information on virtual servers over the Internet. Users of cloud computing technologies often hire third party cloud providers to manage data storage over the Internet. On a more technical level, Nancy King, Oregon State College of Business, describes cloud computing as a convenient means of accessing information in real time from a “shared pool of configurable computing resources,” such as networks, servers, storage applications, and services, without significantly relying on service provider interaction (King & Raja, 2012).

The cloud industry appeals to businesses due to its cost efficiency, faster response times, and flexible support. (Cloud users have the ability to access data over the Internet, but the cloud of data is essentially different whether the user is an individual or a business (Griffith, 2013).) There are three types of cloud services that an organization may choose to implement: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). SaaS is a subscription-based service that allows business to subscribe to an application and access it over the Internet (Griffith, 2013). A popular SaaS on the market is Sales Force. Sales Force allows businesses to manage their sales from remote destinations and interconnect sales trends in real-time. PaaS is similar to SaaS, but instead of subscribing to an application, the business creates its own custom application. All users within the company can then access the custom application from any location. The final type of cloud service is IaaS. Businesses are consumers of IaaS when they use a third party’s equipment to support business operations, such as data storage, servers, hardware, and networking components (Rouse, 2010).

In a recent study, the International Data Corporation (IDC) predicts cloud related services, such as SaaS, PaaS, and IaaS, will become a $100 billion dollar industry by the year 2017 (Columbus, 2013). Many businesses have either considered using cloud services or already done so. In most cases, there are two main parties involved in the cloud: the cloud provider and the organization using the service. A factor that makes the cloud so appealing to the consumer is its cost efficiency. The cloud provider maintains the software and hardware and offers it as a service, which ultimately saves businesses from spending additional capital on purchase, installation, and maintenance costs (Unal & Yates, 2010). Other beneficial factors of the cloud include ease of accessibility and real-time access. Users connected on a network over the Internet are able to access cloud functionalities. The emergence of wireless Internet and Wi-Fi hotspots has enabled cloud users to access and share company’s files from any location at any time. As businesses learn more about what the cloud computing industry has to offer, there will be a significant increase in the amount of businesses offering cloud services, as well as businesses utilizing the cloud service.

DATA STORAGE IN THE CLOUD

As the computing industry matures, an increasing number of individuals and businesses store data on cloud servers. Cloud computing is open to any individual or business willing to pay a third party for services rendered and/or to an internal server for cloud-related functionalities. Not all data stored on the cloud is the same as it reflects the business or purpose for using the cloud.

Entertainment businesses, such as Netflix or Pandora, use cloud servers as infrastructures for their movie and music files. As a service provider for movies and television shows, Netflix offers their customers the ability to stream movies and shows over the Internet and view them remotely from their homes through the use of cloud-based network services. Commercial businesses, government agencies, and accounting firms use the servers to store sensitive information...
such as personal information revealing certain characteristics, i.e. ethnicity, political and religious beliefs, medical information, and criminal convictions or private financial data (King & Raja, 2012). In addition to storage, Netflix also maintains customer accounts, which contain such sensitive data as credit card numbers. All the sensitive information stored is then accessible by a third party, the cloud provider, should this service be outsourced.

Other information stored on cloud servers can be as basic as personal employee files and corporate records, as Twitter did with Google Apps. Similar to sensitive information, personal files and corporate records may contain information that is not for public consumption. In the Twitter incident, the attacker gained access to personal Twitter accounts. The most identifiable, illegally accessed account in the Twitter incident was that of President Barrack Obama (Pavanireddy, Srinivas, & Aruna, 2014). The vast amount of data now stored on cloud servers throughout the world presents an ideal target for fraudsters.

**POTENTIAL THREATS**

Cloud-based networks are vulnerable infrastructures subject to daily threats and intrusions. Advancements in technology allow criminals to target cloud servers and access an abundance of information and resources across the globe. Some of the major concerns in the cloud computing industry are inherent weaknesses found in access controls, authentication, and encryption. Data fraud attacks are executed by a perpetrator in order to gain access to information for malicious purposes and may occur from either an outside source or an associate of the company using the cloud (Pavanireddy, Srinivas, & Aruna, 2014).

The Cloud Security Alliance identifies attacks by a “malicious associate” as a top threat to the cloud computing industry (Pavanireddy, Srinivas & Aruna, 2014). A malicious associate is an individual who works for the cloud service provider and gains access to the data by stealing the Cloud customer’s passwords or private keys. Once the associate has the password or private key, he or she has access to all the customer’s data (Pavanireddy, Srinivas, & Aruna, 2014). This type of attack is of major concern to cloud customers because it is difficult to detect. Malicious associates in control of customer passwords can essentially access the customer’s data without alerting the customer to any unauthorized access (Pavanireddy, Srinivas, & Aruna, 2014).

Outside source data fraud attack is exactly as named. An example of outside source attack is the breach of Twitter’s personal and corporate documents stored on the cloud server, Google Apps previously discussed. Data fraud attacks from an outside source are easier to detect than malicious associate attacks because the service monitors the user’s access and activity.

Data fraud attacks are not the only type currently threatening the cloud computing industry. Instead of targeting the data within the cloud, attackers may target the resources of the cloud. Cloud consumers generally pay for the computational resources they consume, as an individual would for any utility service (Idziorek & Tannian, 2011). The cost basis for the resource utilized in the cloud relies on the cloud provider’s contract agreement, which outlines usage fees, support fees, computational costs and other expenses (Idziorek & Tannian, 2011). In fraudulent resource consumption attacks, attackers attempt to use cloud resources without paying for the service. Attackers typically try to infiltrate cloud resources by “mimicking legitimate client behavior” (Idziorek & Tannian, 2011). The perpetrators conceal themselves as legitimate users who will then be billed by the cloud provider for the fraudulent charges.

When an attacker aims his or her attack on cloud resources, such as RAM and network bandwidth, the cloud infrastructure becomes compromised (Booth, Soknacki & Somayaji, 2013). Fraudulent resource consumption attacks not only result in fraudulent charges to the legitimate consumer, but also decrease the performance and functionality of the cloud resources. In the 8th Annual Symposium on Information Assurance, Gehana Booth states, “Even the largest of providers have finite resources” (Booth, Soknacki & Somayaji, 2013). When an attacker is using a vast amount of cloud resources, the consumer will notice a decrease in the cloud server’s productivity and performance. An attack on cloud resources, which causes the consumer a decrease in performance, is referred to as a denial of service attack (Booth, Soknacki, & Somayaji, 2013).

Another threat to the cloud computing industry is the Structured Query Language (SQL) injection attack. Structured Query Language is a special type of programming language used to manage data in large databases. Attackers using SQL injection attacks attempt to bypass simple SQL commands to gain access to the database. For example, web-based databases, such as cloud server, typically require a username and password for authorized access. The username and password is verified by the web-based application using a series of planned commands. The SQL injection technique allows perpetrators to gain backend access to the database by using “specifically crafted SQL commands” (“SQL Injection: What is it”, 2014). The attacker is then able to access the information on the database without proper verification.

Data confidentiality remains an ongoing concern. As previously discussed, cloud servers may contain sensitive data that is extremely private. In some cases, the cloud consumer may not want the cloud provider to know the contents of the data being stored on the cloud. This raises issues with the relationship between the consumer and the provider. Currently, some cloud providers guarantee service level agreements comprised of data integrity and availability details (Booth, Soknacki, & Somayaji, 2013). However, not all providers are assumed
to be trustworthy service providers. Some malicious cloud providers may not offer trustworthy services, and as a result, have access to the sensitive information the consumers are storing on the cloud server.

THE IMPORTANCE OF SECURITY IN THE CLOUD

Cloud-based networks are becoming a critical component of the nation's economy. For cloud providers, security is an integral component of their business plan: adequate fraud detection and prevention measures reassure the customer base. Customers will not want to store data or financial information where a potential theft threat exists. Many users and businesses generate large amounts of data on a daily basis. According to ScienceDaily.com, "90% of all the data in the world has been generated over the last two years" (SINTEF, 2013). More data equates to a higher risk of a data fraud attack and a greater need for data security (Makryllos, 2014). The cloud provider and user may fall victim to the costly consequences of data fraud if proper security controls are not established.

Security measures need to be stronger as cloud computing makes its transition from a new technology to an everyday technology (Makryllos, 2014). As technology advances, so do the tools and techniques used for fraud (Makryllos, 2014). Strong fraud prevention practices and detection techniques are necessary to maintain data security and adapt to sophisticated data fraud attacks.

FRAUD DETECTION IN THE CLOUD

The Internet and cloud-based networks are vulnerable infrastructures. Advancements in technology allow criminals to target victims and access an abundance of information and resources across the globe. Because the Internet connects people on a global level, it is important to maintain proper security measures in order to protect sensitive information. An important factor in maintaining Internet security is the ability to detect network threats and intrusions in a timely manner. The market provides various tools and detection systems to ensure that network intrusions are identified on a timely basis and network security is maintained.

Intrusion detection systems (IDS) are used to detect unauthorized users on a network by recognizing anomalies, out-of-the ordinary activity, or registering activity that differ from an established baseline (Volonino, Anzaldúa, & Godwin, 2007). A successful IDS is able to recognize unauthorized use, misuse, and abuse occurring on a computer network (Mukherjee, Heberlein, & Levitt, 1994). Intrusion detection systems can be categorized into two types: signature-based and anomaly-based.

Signature-based systems, similar to antivirus software, attempt to identify known threats by triggering the IDS when a particular threat has the same signature as one of the threats in its database (Volonino, Anzaldúa, & Godwin, 2007). Signature-based systems are highly dependent on their databases. If a current database possesses up-to-date signatures and hacker techniques then a signature-based system is extremely efficient in detecting network intrusions (Brox, 2002). Despite its efficiency in detecting network intrusions, the signature-based system does have shortcomings. The first disadvantage is that attackers continually learn new techniques to access networks. If the signature is not stored in the IDS database, it will not be able to detect the attack and alert the network administrator (Brox, 2002). The second disadvantage is the lag time it takes to identify the attacks. If the threat does not match any of the current signatures in the database, the attack may go undetected for an increased amount of time before it is identified (Brox, 2002).

Anomaly-based systems identify changes in a network. Network administrators are able to adjust the security threshold so the IDS does not generate an excessive amount of benign alerts. Anomaly-based systems require more hardware and skilled personnel but ultimately provide more effective protection against hacker intrusions (Brox, 2002). Because the anomaly-based system uses the combination of hardware and skilled personnel, there is an added element of defense to identify new and emerging types of attacks (Brox, 2002). A common disadvantage with the system is that it is more reliant on company personnel and is labor-intensive, but the system's effectiveness offers a valuable defense from unauthorized intruders.

IDS are considered to be reactive security systems which require a network intrusion before the intrusion is detected. As the technology advances, the world of computer forensics has introduced a more active intrusion detection system, Network Forensic Analysis Toolkit (NFAT) (Volonino, Anzaldúa & Godwin, 2007). NFAT systems are used to "record network traffic related to an intrusion and provide the tools to perform forensic analysis of the event" (Volonino, Anzaldúa & Godwin, 2007). NFATs differ from IDS because NFATs are able to recreate and record how the network intrusion occurred. This feature is particularly beneficial for network administrators, such as cloud providers. System administrators benefit from these tools by recreating the incident to learn how the incident occurred and what security measures could prevent the incident from occurring again in the future (Volonino, Anzaldúa, & Godwin, 2007).

Network Forensic Analysis Toolkits allow system administrators to detect and monitor a network security breach in real-time. Because the NFAT detects and monitors in real-time, this reduces the lag time between a network attack and a detection alert. System administrators may benefit from this by quickly identifying cyber intrusions (Volonino, Anzaldúa, & Godwin, 2007). NFAT systems allow network administrators to protect the network from the attack while it is occurring. With real-time detection systems, the administrators have the ability to identify that an attack is occurring and attempt to counter the attack before damage transpires (Volonino, Anzaldúa, &
Godwin, 2007). As technology evolves, NFAT systems are becoming more effective and easier to use. Both NFATs and IDS are critical components of computer systems when attempting to detect network attacks and maintain cloud security.

**FRAUD PREVENTION IN THE CLOUD**

With an increased number of data fraud attacks occurring in the United States, many organizations focus on proactive efforts. By utilizing data fraud attack prevention techniques and educating the nation about cyber security threats, organizations are able to prevent threats and minimize the damages and costs associated with an attack.

One form of fraud prevention that cloud providers and users utilize is high-level encryption software. Encryption is used as a preventative measure by converting data into a form of text that cannot be understood by unauthorized users. Encryption software is used on a variety of platforms, such as physical, virtual and cloud environments. In order to convert encrypted text back into legible form, the authorized user must enter a recognized password ("Data Encryption," 2014). It is critical that cloud users maintain strong passwords in order to protect electronically stored information.

Cloud users must also implement techniques to prevent data fraud attacks. The Department of Homeland Security (DHS) believes that preventing threats requires the cooperation of the government, law enforcement, the private sector, and the public (DHS National, n.d.). Spreading cloud security awareness to these individuals helps "increase the resiliency of the nation in the event of a cyber incident" (DHS National, n.d.). The Department of Homeland Security offers publications directed at various age groups to increase awareness on the types of cyber risks or threats and tips to prevent attacks from occurring. The government understands "no country, community, or individual is immune to cyber risk," but certain steps may maximize online safety (DHS National, n.d.) Some of the steps aimed toward businesses include the following prevention techniques:

- Set strong passwords [change them regularly], and don’t share them with anyone;
- Keep your operating system, browser, and other critical software optimized by installing updates;
- Maintain an open dialogue with your colleagues about Internet safety.…. (DHS Cyber Security, n.d.)

Because it is extremely difficult to prevent attacks from occurring, the United States government educates citizens and organizations through program awareness. The DHS program is called "Stop. Think. Connect" as a part of President Obama's Cyberspace Policy Review. "Stop. Think. Connect" aims to help Americans understand the risks associated with using the Internet. The government also designated October as National Cyber Security Awareness Month (DHS Stop, n.d.). During National Cyber Security Awareness month, professional organizations and government agencies offer their guidance to cloud users for protecting themselves against malicious attacks. The Association of Certified Fraud Examiners (ACFE) is another organization that offers tips to minimize data fraud. Some of their fraud prevention guidelines for cloud users include:

- “Provide regular training sessions to increase data risk awareness and ensure that every employee feels a tangible responsibility for keeping data secure;
- Categorize all data to determine who should have access to what information and on which storage mediums it is allowed to be stored;
- Develop written policies regarding the use of cloud services;
- Implement encryption on sensitive data stored in the cloud;
- Restrict admin privileges where possible; and
- Consider software to monitor the data transmission of all ports” (Capers, 2013).

By following some of these recommendations, cloud users may be able to prevent dangerous data fraud attacks and aid the government “to help Americans understand not only the risks that come with using the Internet, but also the importance of practicing safe online behavior.” (DHS Cyber Security, n.d.)

**CONCLUSION**

The cloud computing industry is on the verge of becoming a $100 billion dollar industry by the year 2017. The cloud has become appealing to businesses because of its cost efficiency, faster response times, and flexible support. Individuals and businesses, which utilize cloud services, each contribute different types of data depending on their nature of business or purpose for using the cloud. The amount of data stored on cloud servers has grown substantially as businesses begin to convert their data processing to cloud providers. Approximately ninety percent of digital data has been created in the last two years (SINTEF, 2013). The vast amounts of data stored on cloud servers throughout the world makes cloud servers an ideal target for fraud.

Advancements in technology allow criminals to target cloud servers and access an abundance of information and resources across the globe. Everyday, there are more intruders attempting to gain unauthorized access onto secure networks. Some of the major concerns in the cloud computing industry are access controls, authentication, and encryption. Unauthorized users work to exploit weaknesses i.e. access controls, authentication, and encryption to gain access to valuable data stored on the cloud.

The market provides various tools and detection systems to ensure network intrusions are identified on a timely basis and network security is maintained. As technology evolves, it is important to implement detection techniques to maintain adequate cloud
security. Both Network Forensic Analysis Toolkits and Intrusion Detection Systems are critical components of computer systems when attempting to detect network attacks and maintain cloud security. Fraud prevention techniques are also an important tool when attempting to protect data stored on the cloud. With help from organizations such as the Association of Certified Fraud Examiners, businesses can continually improve data security. A combination of fraud prevention and detection techniques will provide strong defenses against the potential attacks threatening the cloud computing industry.

REFERENCES


SINTEF. (2013, May 22). Big data, for better or worse: 90% of world's data generated over last two years. Retrieved from http://www.sciencedaily.com/releases/2013/05/130522085217.htm


JONATHAN MAY

Mr. May graduated from Bloomsburg University of Pennsylvania in May of 2012 with a Bachelor’s degree in accounting and a concentration in fraud examination. He received his Masters in Forensic Studies in Accounting from Stevenson University in August of 2014. He currently works for the Pennsylvania Department of Revenue as a Revenue Tax Auditor.
Affinity Fraud: Identification and Prosecution
Christine Kreke

The Greek tragedian Sophocles said, “Things gained through unjust fraud are never secure” (Sophocles, n.d.). Individuals are frequently separated from their money or other possessions through fraud. Too often, these frauds target specific sectors of society such as religious affiliations, retirees, racial groups, or professional organizations. When an offender ingratiates himself within a group in order to gain trust, affinity fraud will result.

Regulators and other law enforcement personnel attempt to identify instances of affinity fraud in order to prosecute the perpetrator and return the fraudulently obtained goods to the victims. However, affinity fraud tends to be an underreported crime as victims may be embarrassed that they easily fell prey to the fraudster or may retain connected to the offender because of the engendered trust cultivated. Reluctance to report the crime can stem from a belief that the fraudster will ultimately do the right thing and return any funds. In order to stop affinity fraud, regulators and law enforcement must be able to detect and identify crime, caution potential investors, and prevent future frauds by taking appropriate legal actions against the perpetrators.

One of the most notorious affinity frauds was the scheme committed by Bernard L. Madoff, which ended in his arrest in 2008. The Madoff scandal is considered an affinity fraud because the vast majority of his clientele shared Madoff’s religion, Judaism. Over the years, Madoff’s clientele grew to include prominent persons in the entertainment industry, including Steven Spielberg and Larry King. This particular affinity fraud was unprecedented because it was perpetrated by Madoff over several decades, and customers were defrauded of approximately twenty billion dollars (Picard, n.d.).

It is debatable whether the poor economy, lack of investor education, or ready access to diverse persons over the internet has led to an increase in affinity fraud. Nevertheless, it is clear that affinity frauds have dramatically increased in recent years. In fact, affinity fraud has been identified as one of the top five investment schemes since 1998 (Perri & Brody Birds 34). The head of Alabama’s Securities Commission, Joseph P. Borg, cites several reasons for the increase in financial frauds including public fear, the economy, and distrust in the government’s ability to protect investors. Borg places primary blame for the increase on the proliferation of the internet (Blanton, 2012). With the advent of the internet, offenders who have no readily identifiable traits in common with potential victims can simply assume attributes comparable to the intended victim.

Fraud related crimes perpetrated under the guise of trust in various religious organizations are a considerable problem in Utah. An FBI study revealed that in 2010, more than 4000 citizens of Utah were defrauded of over $1.5 billion. Many of the offenders charged sought out their victims through faith-based organizations (Morgan, 2011).

Authorities attribute the problem to the fact that a high percentage of Utah’s population is Mormon. Specifically, the Mormons as a community are inclined to trust others and are hospitable to new community members. Affinity fraudsters used this trust to their advantage pursuing their schemes (Affinity Fraud: Fleeing, 2012).

The societal effects of affinity fraud are not limited solely to the amount of funds lost by investors. Once these frauds are uncovered, investor confidence can diminish the financial markets, and distrust can increase in the government’s ability to provide protection. Loss of confidence manifested itself after the Madoff fiasco with the effects evident throughout the economy. “Unfortunately, affinity fraud erodes the trust needed for such investments to occur and to foster our economy” (Sargian, 2012, p. 10). Essentially, affinity fraud victims become less likely to trust future monetary requests and legitimate charitable organizations could suffer from a loss of endowments. Subsequent to a large fraud being discovered, time is spent by regulators and law enforcement not only prosecuting these cases but also in assessing what went wrong. Time consuming investigations generally include implementation of changes in an attempt to assist in detection of these frauds in the future.

Affinity frauds assume different forms, e.g. information phishing expeditions, investment scams, or charity cons. However, most affinity frauds have a common element and entail a pyramid-type or Ponzi scheme. In these types of frauds, the offender uses new funds from fresh victims as payment to initial investors. This creates the illusion that the scam is profitable and additional victims would be wise to invest. These types of scams inevitably collapse when it either becomes clear to investors or law enforcement that the fraudster is not legitimate or there are no more financial backers for the fraud (Stopping Affinity, 2013).

Although most people may be familiar with the Madoff scandal, there are other affinity frauds perpetrated across the United States that continue to shape how regulators and other law enforcement approach these frauds. A prominent case which prompted discussion among regulators and law enforcement personnel is that of Seng Tan, a Cambodian immigrant, who, with her Canadian-Cambodian citizen husband, James Bunchan, swindled fellow Cambodian immigrants out of nearly $30 million in a pyramid scheme involving two multi-level marketing companies. Tan and Bunchan attempted to impress other Cambodian immigrants with their wealth and convinced them that they too, could live the American dream. Tan attended religious services with others in the community, spoke their language, and shared the horrors she experienced attempting to escape the regime in Cambodia prior to her immigration. The victims thoroughly trusted Tan and Bunchan. One investor even believed that “God sent her here to help our community.” Instead, Tan and Bunchan used the funds to live a lavish lifestyle (Perri & Brody Affinity).
As previously indicated, most affinity frauds contain an element of a pyramid or Ponzi scheme investment. In the case of the Tan and Bunchan fraud, Bunchan set up two multi-level marketing companies, World Marketing Direct Selling and Oneuniverseonline, which supposedly operated in a manner similar to legitimate companies like Avon or Amway. In these types of organizations, each new sales person is required to recruit additional product sellers. However, in a legitimate operation like Avon, product sales, as opposed to new recruits, drive the profitability of the company. In a pyramid scheme, commissions earned are based upon how many persons are brought into the organization. In the Tan and Bunchan case, they offered victims the opportunity to skip to a "Director I" level position in the business by paying Tan a lump sum of $26,347.86. At this level, the victim would get an immediate bonus and three hundred dollars a month for life. All payouts were supposedly earned without ever selling a single product. The scheme operated on several levels but each required a constant influx of additional personnel to continue payments to the original investors. Upon the cessation of new recruits, payments stopped, suspicions arose and investors complained to Tan. At that point, Tan manufactured excuses as to why the payments were late or nonexistent to include banking issues resulting from Hurricane Katrina. Illogical excuses are a common element in pyramid and Ponzi schemes when there is a lack of funds (United States, 2012).

Perpetrators of affinity frauds are able to make their scams appealing to their targeted victims. Once the offenders have targeted a community or group, they seek out respected community leaders to vouch for them to potential investors. By having an esteemed figurehead who appears to be knowledgeable about the investment and endorses it, the offender creates legitimacy for the con. Additionally, others in the community are less likely to ask questions about a venture or investment if a community leader recommends or endorses the fraudster. In the Madoff case, Madoff himself was an esteemed member of the community. As a former chair of the National Association of Securities Dealers (NASD) and owner of a company ranked sixth largest market maker on the National Association of Securities Dealers Automated Quotations (NASDAQ), Madoff’s reputation in the financial services industry was impeccable and people were eager to invest with him (Ragothaman, 2014, p. 272).

Projection bias is another reason why affinity fraudsters are able to continually perpetrate these types of crimes. Psychological projection is a concept introduced by Sigmund Freud to explain the unconscious transference of a person’s own characteristics onto another person. The victims in affinity fraud cases project their own morals onto the fraudsters, presuming that the criminals are honest and trustworthy. However, the similarities are almost certainly the reason why the fraudster targeted the victims in the first place. In some cases when victims are interviewed after the fact, they indicate to law enforcement that they trusted the fraudster as if they were a family member because they believed that they shared the same value system (Perri & Brody Optics 361).

Regulators and law enforcement must examine how the fraudsters are succeeding with these schemes. Lisa M. Fairfax, Research Professor of Law, George Washington University Law School, stated, “Success of affinity fraud stems from the higher degree of trust and reliance associated with many of the groups targeted for such conduct” (Fairfax 5). Because of the victim’s trust in the offender, the targeted persons are less likely to fully investigate the investment scheme presented to them. Judicial Law Clerk, Utah Second District Court Karina Sargsian wrote, “The underlying rationale [of affinity fraud] is that people tend to be more trusting, and, thus, more likely to invest with individuals they have a connection with—religious, ethnic, social, or professional” (Sargsian, 2012, p. 2) Affinity frauds are often difficult to detect because of the right-knit nature common to some groups targeted for these schemes. Victims of these frauds are less likely to inform appropriate law enforcement of the problems and the frauds tend to continue until an investor or outsider to the target group finally starts to ask questions (Stopping Affinity, 2013).

Because victims in affinity frauds are less likely to question or go outside of the group for assistance, information or tips regarding the fraud may not ever reach regulators or law enforcement. An article in the The Economist asserts, “In religious cases, there is often an unwritten rule that what happens in church stays there, with disputes handled by the church elders or the minister” (Affinity Fraud: Fleecing). Once the victims place their trust in the fraudster, they are “less likely to believe they have been defrauded” and also unlikely to investigate the con (Perri & Brody Optics 358).

Regulators and other law enforcement personnel can also learn from prior failures in identifying or stopping affinity frauds. Because the Madoff fraud is one of the largest frauds in history, many studies have been conducted to determine how this fraud could have been stopped sooner. In hindsight, there were numerous red flags that indicated Madoff’s activity was fraudulent; however, appropriate actions were not taken to halt the scheme. The United States Securities and Exchange Commission (SEC) received several complaints against Madoff as early as 1992, including several official complaints filed by Harry Markopolos, a former securities industry professional and fraud investigator. Every step of the way, Madoff appeared to use “his charm and manipulative ways to explain away his dealings to the SEC inspection teams” (Ragothaman, 2014, p. 277). The complaints were not properly investigated and subsequent to Madoff’s arrest, the SEC was the target of a great deal of criticism. The regulators obviously did not apply appropriate professional skepticism while doing their jobs and relied on Madoff’s reputation and representations rather than evidence to the contrary. In the wake of this scandal, regulatory reforms were deemed a priority at the SEC and other similar agencies.
People often correlate the criminals who perpetrate affinity frauds to the white collar crimes they commit and assume that these offenders do not exhibit behaviors most often associated with perpetrators of street crime. This is an incorrect assumption as studies have indicated that the profile of an affinity fraudster is akin to offenders who commit conventional crimes (Perri and Brody, 2000). Perpetrators of affinity fraud are often regarded as “predatory” because they target specific communities or organizations. These offenders frequently exhibit the ability to interpret their victims’ behaviors and fine tune their approach to anticipate and dispel any objections by the targeted individuals. Convicted affinity fraudsters interviewed in a study displayed antisocial behaviors: pathological lying, lacking empathy, and blaming the ignorance of their victims (Perri & Brody, 2006). If regulators and other law enforcement personnel remained attentive to the profile of an affinity fraud offender, they might be able to more readily identify the perpetrators and hopefully impede the progression of the frauds.

A belief commonly held among Americans is that affinity fraudsters are not prone to violence because their scheme is a white-collar crime. This is a misconception and investigations have proven that white-collar criminals, like those who commit affinity frauds, are likely to turn violent when there is a risk of the fraud being uncovered or prosecuted (Perri & Brody, 2006). An example of this type of violence is demonstrated in the Tan and Bunchan case. When Bunchan was finally incarcerated for financial fraud he sought to hire a hit man to murder the Cambodian victims who were prepared to testify against him. Bunchan believed that if the victims went away so would the power of law enforcement to prosecute him for the affinity fraud. Unfortunately for Bunchan, the hit man he attempted to hire was an FBI agent, so he was convicted of a murder for hire scheme in addition to the original charges related to the affinity fraud (Perri & Brody, 2006). White collar criminals who turn violent when confronted with the likelihood that their schemes will be exposed are referred to as red collar criminals. The term red collar criminal was coined by Frank Perri, an Illinois attorney who has written several scholarly articles on affinity fraud (Perri, 2006). Violent acts perpetrated by red collar criminals are generally well thought out or premeditated in contrast to violent acts committed by conventional street criminals (Perri & Brody, 2000). In order to prevent violent crimes like the attempted murders planned by Bunchen, law enforcement should be aware of the potential for this type of plan to be carried out.

Therefore, prevention has been primarily focused on widespread public investor education. It is unknown where affinity fraudsters may strike next. Some experts believe that the United States federal government’s attempts to educate the public on the dangers of affinity frauds have been woefully insufficient. Specifically, these professionals expressed that the SEC has pursued several cases after the fact in reaction to exposed frauds but are slow to actually inform investors how to avoid these frauds. One former SEC employee stated that the agency “has chosen to stick some ambulances at the bottom of the cliff rather than build fences at the top” (Affinity Fraud: Fleecing, 2012). If affinity frauds are going to be prevented rather than identified after they occur, regulators and other law enforcement must take steps to augment their efforts in educating potential investors.

Affinity fraud education is not only necessary for the potentially targeted victims of these frauds but also for industry professionals so that these frauds can be identified sooner. In the Madoff case, there were multiple failures by multiple people to identify and stop the scheme. The SEC investigators failed to promptly and completely investigate tips from other industry professionals regarding the feasibility of actual investments claimed by Madoff. The Certified Public Accountant (CPA) for Madoff’s companies and hedge funds was not qualified to audit such a large venture. The CPAs for the feeder funds invested with Madoff did not perform appropriate reviews. The industry professionals who managed these feeder funds did not perform due diligence before they invested their companies’ funds. Finally, Madoff employees turned a blind eye to discrepancies and other red flags encountered during their employment (Ragothaman, 2014, pp. 277-278).

Because of failures noted in the Madoff example, changes were made to how regulators and other workers perform their key functions. Most regulators now review the qualifications and reasonableness of the engaged CPA and key employees. Credence is given by law enforcement to tips received from the public and law enforcement personnel to thoroughly investigate any possible unlawful activity. Because tips are a primary way that frauds in general are identified, many companies are also instituting whistleblower programs so that fraud can be identified sooner. Additionally, there is a prevailing emphasis on fraud education in the financial services industry where many of the high profile affinity frauds like Madoff’s have occurred.

In recent years, several states have taken steps to make changes to existing laws to address the problems of affinity frauds. Utah has enacted two new laws that specifically target reducing the impact of affinity fraud. Both laws were sponsored by Utah State Senator Ben McAdams who has publically criticized the considerable amount of affinity frauds occurring in Utah. One of the laws included increased penalties for crimes that involve an abuse of trust while the other provides for up to 30% of any funds recaptured from these frauds to be paid to whistleblowers. Utah avowed if there is probable cause that an affinity crime has been committed, the state can seize the suspect’s property even before charges are filed (Affinity Fraud: Fleecing, 2012). One of the new laws modified the Utah Uniform Securities Act and included harsher penalties if the victim of the fraud is a “vulnerable adult.” If the victim in a fraud scheme is deemed to be a vulnerable adult under the law, prosecutors would be able to file second-degree felony charges against the perpetrator (Morgan, 2011).
Another prominent Utah politician and attorney, Sean Reyes, the current Utah Attorney General, is championing a crusade to construct a “fraudsters registry.” This listing would function similarly to the sex offender registries. Reyes stresses such a registry is needed because there is a high incidence of repeat offenders committing affinity frauds. Reyes’ campaign for attorney general included a desire to study the premise of lessening fraudster sentences if they disclose the location of hidden assets acquired through their schemes. The basis behind sentence reduction is that in most frauds, the assets recovered actually returned to victims are minimal, as the funds are often squandered by the offender prior to detection of the fraud (Affinity Fraud: Fleecing, 2012).

Indiana has experienced numerous affinity frauds. In 2009, Indiana enacted a law amending two provisions in the state’s securities act so as to impose stricter punishments against fraudsters who target victims based on religion or age. Specifically, the changes make it possible for prosecutors to charge fraudsters with a Class B felony if the offenders prey on the elderly (defined in the statute as at least sixty years of age) or victimize persons based on religious affiliation. The sentencing guidelines for a Class B felony in Indiana includes a fixed minimum term between six and twenty years. Prior to this amendment, prosecutors would have been able to charge the offenders with a Class C felony which includes a sentencing guideline of between two and eight years (Sargsian, 2012, pp. 17-19). With the introduction of these harsher punishments, the elected representatives in Indiana hope to deter future frauds of this nature in their jurisdiction.

In the enactment of the laws in Utah and Indiana, there was some dissent in increasing penalties for affinity frauds. Specifically in Utah, Benji McMurray, a federal public defender, criticized the move to amend the laws to provide for enhanced punishments for fraudsters who target particular groups. McMurray argued that there were already laws and applicable punishments in place to prosecute fraud and did not see why these fraudsters should be treated differently. Researchers countered his argument by citing federal sentencing guidelines which rationalize that those who abuse positions of trust as “insiders” rather than commit frauds of opportunity should be subject to augmentation of sentences (Sargsian, 2012, p. 23).

Fairfax expanded the argument in favor of enhanced sentences for affinity fraudsters by comparing affinity crimes to hate crimes. Fairfax’s argument is based on the fact that no homogeneous definition of the term hate crime exists across states; however, a universal component of hate crimes is the bias that the criminal has against a particular group. A dissenting opinion counter argues that the perpetrator of affinity fraud is often a member of the same group targeted in their fraud scheme. How can it be a hate crime if this is the case? All but one of the state hate crime statutes do not require that the offender “belong to a social group different than the victim.” Additionally, most people associate hate crimes with violent offenses; however, several states’ statutes on hate crime do not specifically relate hate crimes to violent acts. In those states, Fairfax contends that the essential characteristics of affinity frauds could be prosecuted under the statutes related to hate crimes. Prosecution as a hate crime would ultimately result in stiffer punishments than prosecuting an affinity fraud as a standard crime (Fairfax, 2013, pp. 6-9). By such innovative thinking, prosecutors may be able to develop alternative theories to take legal action against perpetrators of affinity frauds.

The problem of affinity frauds is not diminishing even with increased efforts by regulators and law enforcement. Fraudsters are continuously finding new ways to ingratiate themselves into various communities in order to deceitfully procure the targeted victims’ assets. A recent affinity fraud scheme was halted because the government filed a complaint in the United States District Court in the District of Massachusetts. Specifically, the SEC filed official charges against several parties on April 17, 2014, for a pyramid scheme that targeted Dominican and Brazilian immigrants in twenty-one different states and abroad. In conjunction with the issuance of this complaint, the SEC was able to effectively freeze the assets of the defendants. The complaint alleges that two Telexfree companies and eight individually named defendants operated a multi-level marketing company that purportedly sold local and international calling plans. The defendants sold memberships in the company, and promised returns to the investors of two hundred percent or more. Investors in the scheme could earn more money by recruiting additional members into the organization. In reality, the fraud was an elaborate pyramid scheme that raised at least $300 million from the scam victims. Similar to the squandered or secreted assets in other similar frauds, the whereabouts of the illicit funds are not known (Securities, 2014).

In order to combat affinity frauds, regulatory and law enforcement agencies need to ensure that they are properly staffed to handle the complex issues involved. This includes hiring employees with the appropriate experience and training in areas of financial frauds. Frank Casey, a financial industry professional who is credited as a whistleblower in the Madoff case, attributes some of the fault in identifying the Madoff fraud to the inexperience of the SEC regulators tasked to investigate the complaints and review Madoff’s operations. Specifically, the majority of the SEC staff were attorneys who did not have the appropriate knowledge about the intricacies of the stock and derivative transactions in question (Lee, 2013). If the regulators, accounting professionals, and law enforcement personnel are educated properly, they will be able to more adeptly identify the red flags of affinity frauds and hopefully deter future losses for victims.

State legislatures also need to take steps similar to Utah and Indiana to place harsher penalties on affinity fraudsters that could
potentially deter fraudsters and prior offenders from committing additional crimes. When Senator McAdams was debating the statute amendments he argued, “This [bill] won’t put an end to fraud…. it’s a mechanism for us to say that it is outrageous, we will not tolerate it, and we will fight it with enhanced penalties and enhanced fines” (Sargsian, 2012, p. 29). Amendments to the laws can also encourage the reporting of these frauds if they include whistleblower provisions. New laws are not a failsafe though, and should not be the only means by which law enforcement seeks to confront the problem of affinity fraud.

In order to stop affinity frauds from occurring in the first place, increased educational efforts need to be established. Education is especially important in areas where tight-knit cultural communities who are vulnerable to these frauds. By reaching out to the same cultural or religious leaders that fraudsters often target in their schemes, law enforcement could launch collaborative relationships with these groups in their education efforts. In Canada, the British Columbia (BC) Securities Commission commenced an educational endeavor in 2011 designed to specifically educate ethnic groups in BC on investment frauds. It is important to note that the BC Securities Commission ensured the promotional campaign was provided in several languages native to the communities they were attempting to reach (Sargsian, 2012, p. 31). States would be smart to adopt similar promotions to target vulnerable groups or communities in their jurisdictions.

Affinity frauds acquired a poster boy in Bernie Madoff because of the devastation caused by his unprecedented fraud scheme. But frauds such as this are occurring daily and on a much smaller scale in communities across the United States. The effects of these affinity frauds are widespread and the emotional consequences experienced by the victims of these frauds cannot easily be measured. Regulators and other law enforcement personnel need to assess the harm caused by affinity fraud and determine what steps need to be taken to effectively confront these types of frauds. Laws should be reviewed and amended where necessary to ensure appropriate enhanced sentencing is enforced for egregious crimes involving affinity fraud. Regulators and law enforcement should approach fraud cases from different angles in an attempt to determine if new methods may be more effective. Additionally, education is needed for the investing public and the regulators and law enforcement personnel to ensure that they all have the proper knowledge and tools to be able to understand, detect, stop, and prevent these types of frauds. Affinity frauds are not easily anticipated by the victims. Madoff whistleblower Markopolos asserted that "nobody thinks one of their own is going to cheat them" (Perri & Brody Birds, 2011). Affinity frauds will not be curtailed unless the public, regulators and other law enforcement personnel are involved.

REFERENCES


CHRISTINE KREKE

Christine Kreke graduated in 1994 with a Bachelor's of Science degree in both Accounting and Finance from Indiana University in Bloomington, Indiana. Christine is employed at the National Futures Association, the industry wide, self-regulatory organization for the U.S. futures industry. She is an Examination Manager in the Compliance Department and is responsible for presiding over examinations and supervising examination teams. Christine is also a Certified Public Accountant and Certified Fraud Examiner. She is currently working on her Master's Degree in Forensic Studies in the Interdisciplinary Track at Stevenson University.
Recent Trends of Enforcement and Compliance with the Foreign Corrupt Practices Act

William Olsen

Recent enforcement action by the Securities Exchange Commission (SEC) and Department of Justice (DOJ) against Hewlett Packard (HP) sent a clear message to United States (US) corporations and other companies traded on the US markets. Hewlett Packard recently agreed to pay $108 million in fines and penalties to the SEC and DOJ to resolve a wide range of Foreign Corrupt Practices violations throughout its worldwide network (King, 2014). HP was fined for paying “commissions” to obtain software contracts around the world. The company has agreed to embark on extensive improvement of their internal controls and also enhance their Corporate Governance program “to include strong, visible and explicit support for anti-bribery and corruption laws and regulations” (Alfaro, 2013).

The Foreign Corrupt Practices Act (FCPA) was enacted in 1977 but aggressive enforcement did not occur until around 2005 when there were twelve enforcement actions. 2008 was a record year for enforcement actions with forty-two cases (Krakoff, 2009). Although the number has declined since then it still remains a very aggressive environment. The purpose of the FCPA was to prevent the bribery of foreign government officials when negotiating overseas contracts. The FCPA imposes heavy fines and penalties for both organizations and individuals. The two major provisions address: 1) bribery violations and 2) improper books and records and/or having inadequate internal controls. Methods of enforcement and interpretation of the law in the US have continued to evolve.

The FCPA created questions of definition and interpretation, i.e., Who is a “foreign official?” What is the difference between a “facilitation” payment and a bribe? Who is considered a third party? How does the government define adequate internal controls to detect and deter bribery and corruption?

The enactment of the United Kingdom (UK) Bribery Act in July 2010 was the first attempt at an anti-bribery law to address some of these issues. The UK Bribery Act introduced the concept of adequate procedures, that if followed could allow affirmative defense for an organization if investigated for bribery. The UK Bribery Act recommended several internal controls for combating bribery and offered the incentive of a more favorable result for those who could document compliance. These include:

- Established anti-bribery procedures
- Top level commitment to prevent bribery
- Periodic and documented risk assessments
- Proportionate due diligence
- Communication of bribery prevention policies and procedures
- Monitoring of anti-bribery procedures (Ministry of Justice, 2011).

The concept of an affirmative defense for adequate procedures creates quite a contrast to FCPA which only offers affirmative defense for payments of bona fide expenses or small gifts within the legal limits of the foreign countries involved.

The UK Bribery Act equated all facilitation and influence payments to bribery. Finally, the UK Bribery Act dealt with the problem of defining a foreign official by making it illegal to bribe anyone regardless of government affiliation. Several countries such as Russia, Canada and Brazil have enacted or updated their anti-bribery regulations to parallel the guidelines presented in the UK Bribery Act. The key to the effectiveness remains enforcement.


The hallmarks include:

- Establish a code of conduct that specifically addresses the risk of bribery and corruption.
- Set the tone by designating a Chief Compliance Officer to oversee all anti-bribery and corruption activities.
- Training all employees to be thoroughly prepared to address bribery and corruption risk.
- Perform risk assessments of potential bribery and corruption pitfalls by geography and industry.
- Review anti-corruption program annually to assess the effectiveness of policies procedures and controls.
- Perform audits and monitor foreign business operations to assure compliance with the code of conduct.
- Ensure proper legal contractual terms exist within agreements with third parties that address compliance with anti-bribery and corruption laws and regulations.
- Investigate and respond appropriately to all allegations of bribery and corruption.
- Take proper disciplinary action for violations of anti-bribery and corruption laws and regulations.
- Perform adequate due diligence that addresses the risk of bribery and corruption of all third parties prior to entering into a business relationship.

The SEC and DOJ entered into the first ever Non-Prosecution Agreement (NPA) for Foreign Corrupt Practices violations on April 22, 2013 with Ralph Lauren Corporation (RLC). This decision has been seen as a harbinger from the DOJ and SEC with regard to future enforcement actions. The NPA highlighted the “extensive remedial measurements and cooperation efforts” that the RLC demonstrated during the course of the investigation. The corporation paid only $882,000 in fines because they were able to “demonstrate a strong tone from the top and a robust anti-corruption program” (U.S. DOJ Ralph Lauren Corporation, 2013).
Conversely, there are stark differences between the agreement reached with Ralph Lauren Corporation and that with Hewlett Packard (HP). HP was fined $108 million dollars versus $882,000 for RLC. This illustrates the scope of penalties that the government can levy based upon their investigation of the organization’s response to bribery and corruption risk.

Based upon the prosecutor’s comments, it appeared that the government believed the RLC had an effective, robust, anti-bribery program whereas HP apparently did not.

Under a Deferred Prosecution Agreement (DPA) the DOJ files a court document charging the organization while simultaneously requesting prosecution be deferred in order to allow the company to demonstrate good conduct going forward. The DPA is an agreement by the organization to: cooperate with the government, accept the factual findings of the investigation, and admit culpability if so warranted. Additionally, companies may be directed to participate in compliance and remediation efforts, e.g., a court-appointed monitor. If the company completes the term of the DPA the DOJ will dismiss the charges without imposing fines and penalties.

Under the Non-Prosecution Agreement the DOJ maintains the right to file charges against the organization at a later time should the organization fail to comply. The NPA is not filed with the courts but is maintained by both the DOJ and the company and is posted on the DOJ website. Similar to the DPA, the organization agrees to monetary penalties, ongoing cooperation, admission to relevant facts, as well as compliance and remediation of policies, procedures and controls. If the company complies with the agreement, the DOJ will drop all charges.

The key differences between the RLC and the HP cases was the initial response to the discovery of improper payments. The RLC response included “prompt self-reporting, full cooperation with the government and the serious remedial steps taken,” including termination of a customs broker and the winding down of their operations in the country where the violations occurred. Additionally, the RLC discovered the improper payments while in the process of enhancing their anti-bribery and corruption controls. The SEC’s FCPA Unit Chief indicated that it was “RLC’s self-policing and self-reporting that were the reasons for the amicable resolution” (U.S. DOJ Ralph Lauren Corporation, 2013).

DIFFICULTIES WITH FCPA COMPLIANCE

The FCPA defines a Foreign Official as “any officer or employee of a foreign government; or any department, agency, or instrumentality thereof; or of a public international organization; or any person in an official capacity for or on behalf of any such government or department, agency or instrumentality.” Such an all-encompassing definition poses a compliance challenge to US businesses. This problem is exacerbated with regard to the state owned or state-controlled entities referred to in the FCPA as “instrumentalities” (U.S. Department of Justice A Resource Guide to FCPA).

On May 16, 2014, the 11th Circuit Court of Appeals upheld the broad definition in US vs. Esquenazi (King, 2014). The 11th Circuit Court is the first appellate court to rule on this issue thus its ruling will have a broad impact on all future business transactions subject to the FCPA. The FCPA section on foreign officials is one of the most difficult areas to interpret and the subject of “instrumentality” remains vague when applied to foreign officials. Historically, the government has used this vagueness to their advantage by expanding the scope and reach of the investigation.

In-depth analysis of the entity’s ownership, function and relationship to the foreign state is required in order to ascertain if an entity is an instrumentality of a foreign government. This analysis must determine if key officers and directors of the entity are government officials or have some relationship to the government in question. The 11th Circuit Court of Appeals upheld the DOJ definition of “instrumentality” as “an entity controlled by the government of a foreign company that performs a function the controlling government treats as its own” (U.S. DOJ A Resource Guide to FCPA).

Four questions are considered when determining if an entity equals an instrumentality. These include: 1) Has the entity been designated by the state? 2) Does the government have a majority interest? 3) Is the government involved with appointing or terminating the entity’s principals? 4) Is the government involved with managing profits and losses?

The Esquenazi decision expands the number of foreign entities within the FCPA’s domain. The Court has clearly indicated that an entity with minor government ownership could be deemed an instrumentality if the entity performs a government function. This creates further compliance problems for US companies.

On April 16, 2013, Parker Drilling entered into a three year Deferred Prosecution agreement with the DOJ, paid $11,760,000 in fines and agreed to implement an enhanced compliance program. The settlement alleged that Parker Drilling “violated the bribery, books and records, and internal control sections of the FCPA by making $1.25 million in improper payments through a third party intermediary that Parker knew would use the funds to entertain Nigerian Customs officials in order to influence them to agree to $3 million in reduced customs fines” (U.S. DOJ Parker Drilling).

The use of third party intermediaries poses a challenge for US organizations attempting to comply with the FCPA. First, it is difficult to manage the actions of a third party operating in a foreign country, engaged in different business practices and customs than the United States. Second, there appears to be a misconception by executives that a company is not liable for actions taken by a third party conducting business on the US Company’s behalf. Avoidance
of actual knowledge or ignorance of bribery remains a poor defense as Congress has stated that just the “high probability” of a bribe occurring is sufficient to hold the business accountable for the actions of the third party (U.S. Department of Justice A Resource Guide to FCPA).

Unlike the UK Bribery Act, the FCPA contains an exception for payments to facilitate or expedite services so as “to further routine government action” (U.S. Department of Justice A Resource Guide to the FCPA). These exceptions address non–discretionary acts e.g., processing paperwork or expediting government documents. The FCPA does not provide a monetary limit on payments, however the size of the payment is often a factor in determining the corrupt intent to influence a non-routine government action. Such proposed transactions or facilitation payments should undergo legal review and determination by qualified counsel prior to actual payment. Companies are also subject to legal action should their activities violate the host country’s laws regarding transaction or facilitation payments.

**FCPA ENFORCEMENT TRENDS**

On April 14, 2014, the DOJ unsealed an indictment regarding two broker-dealer executives who were charged with FCPA violations in connection with the payment of bribes to a representative of a state-owned Venezuelan bank. The CEO and Managing Partner of Direct Access Partners, in coordination with other third parties, including the wife of the CEO, conducted a bribery scheme where millions of dollars were paid to a bank official so she would direct bank business to the firm. The two executives garnered over $60 million in commissions, transferred their gains to offshore bank accounts to evade detection and taxes, and returned a percentage to the bank official.

The Direct Access Partners case illustrated the DOJ’s methodology when pursuing FCPA violations. These include: 1) using full range of laws and federal statutes applicable to the case, e.g., FCPA, travel act, money laundering; 2) coordination efforts in a transnational environment; 3) indicting top tier leadership. The assistant attorney general in this case stated “…we will aggressively pursue individual executives, all the way up the corporate ladder, when they try to bribe their way ahead of the competition” (Alfaro, 2013). This case is just one of many cases that DOJ and SEC have brought against individuals for FCPA violations.

The trend of transnational law enforcement agency cooperation and coordination to enforce FCPA was noteworthy in the AON case. In December 2011, the US settled FCPA charges against AON, two years after the UK Financial Services Authority (FSA) had investigated the UK subsidiary and found that the UK subsidiary was bribing government officials in Costa Rica. Heavy fines and penalties were levied by the US government for poor controls over bribery and corruption risk. More recent cases have indicated increased cooperation between the US, UK, Australia and Canada, since the establishment of the International Foreign Bribery Task Force in May 2013 (IFBT). This type of international cooperation will increase as more countries begin to enforce their anti-bribery laws.

Industry sweeps appear to be increasing. An industry sweep occurs when the government expands an investigation of one entity into others in the same industry. For example pharmaceutical and medical device companies including Johnson & Johnson and Novartis recently disclosed bribery and kickback violations. The financial services industry, including Deutsche Bank and Citi Group have also had several investigations pertaining to their dealings with sovereign wealth funds. Companies in the technology industries (IBM, Converse Technology and Maxwell Technologies) also disclosed settlements for FCPA related issues in recent years.

Both the DOJ and SEC have focused on Successor Liability issues. These are enforcement actions against companies for FCPA violations occurring before or after mergers or acquisitions. When a company merges with, or acquires another company, the successor company assumes most of the predecessor’s liability in criminal and civil actions to include FCPA violations.

Armor Holdings Inc. paid $16 million to the SEC and DOJ to settle FCPA violations disclosed prior to being acquired by BAE Systems Incorporated (Alfaro). The differed–prosecution agreement noted that the government agreed to settle due to Armor Holding Inc.’s transparency and cooperation with the government as well as its implementation of extensive remedial efforts throughout the acquisition process (Alfaro, 2013).

Diageo PLC also paid the SEC and DOJ $16 million to settle FCPA charges relating to improper payments made to government officials in Asia (Alfaro). The SEC disclosed deficiencies in the FCPA compliance program of Diageo which allowed violations to go undetected as Diageo expanded through multiple mergers and acquisitions. The SEC concluded Diageo PLC was aware of the deficiencies in controls but ignored them until the corrupt payments were uncovered, after the transfer of ownership occurred (Alfaro, 2013).

The SEC and DOJ encourage US companies to conduct pre–acquisition due diligence. Due diligence evaluates internal policies, procedures and controls before acquisition. Poor accounting and internal controls may signal a less valuable commodity; disclose corrupt business practices i.e., bribery which can be resolved prior to the acquisition, and identify business and geographical risks to be offset during the post-acquisition and subsequent integration of corporate compliance and internal controls.
Due diligence, with regard to mergers and acquisitions sets the tone and sends the message to regulators that the expanded organization is committed to detecting and deterring bribery and corruption. When companies voluntarily disclose and remediate improper conduct identified during the process of a merger or acquisition, the SEC and DOJ appear to be more lenient. In fact, the DOJ and SEC have only taken action against successor companies when the illegal activity is blatant and sustained or when the successor company fails to stop the violations or participates in the illegal activity.

Originally allegations of FCPA violations were received through a company's internal whistleblower hotline. That trend changed with the enactment of the Sarbanes Oxley Act in 2002 and the Dodd-Frank Act in 2012. These laws created other means and mechanisms for reporting suspicions of illegal activity and provided protections from retaliation against whistleblowers. The Dodd-Frank Act also has monetary incentives of 10% to 30% of the amounts recovered by the government as a means to encourage whistleblowers to come forward (U.S. Department of Justice A Resource Guide to FCPA). Companies considering whether to disclose potential anti-corruption problems to the SEC must now consider the possibility that a potential whistleblower may report it first to the government thus creating greater liability for the organization.

ROLE OF NON-GOVERNMENT ORGANIZATIONS (NGO)

The Organization for Economic Cooperation and Development (OECD) has been in the forefront of anti-bribery acts since the development of the OECD Anti-Bribery Convention in 1997. The “Good practice guidance on internal controls, ethics and compliance” offers excellent guidelines for companies establishing controls to specifically address the risk of bribery and corruption (Office of Economic Cooperation and Development). The OECD has been proactive in working with countries to improve or establish quality anti-bribery legislation and enforcement i.e., influencing Canada to add a books, records and internal control section to their Bribery Act issuing a second report on Russia's efforts to implement the OECD Anti-Bribery Convention. This report highlighted “Russia's efforts to disallow the tax deduction for bribes and for passing requirements that Russian companies must implement anti-corruption policies within their organizations” (Office of Economic Cooperation and Development). Organizations like the OECD have a critical role in combating global bribery and corruption because they raise public awareness and help bridge the divide between the public and the private sectors.

The World Bank has also raised awareness and fought bribery especially through the World Bank Institute (WBI). The WBI released the "Business Case for Collective Action against Corruption" in 2008 which lays the foundation for government, private industries and non-government organizations to work together to combat global corruption (World Bank). The WBI message emphasizes that contrary to popular belief, an anti-corruption approach actually makes good business sense when overall costs are calculated. High profile cases result not only in revenue loss due to fines, penalties, legal and consulting fees but also the business's reputation, customer loss and disruption of operations. Money diverted to pay fines and penalties is lost income for research and development, innovations, and investment. Risk assessment and cost benefit analysis are critical to successful operation in the global marketplace.

To combat global corruption the players must understand the root causes of corruption. However, the business community does not control all the causal factors, thus the incentive to work with non-government organizations such as the OECD, United Nations and World Bank to address these environmental issues which fosters corruption.

Djordjija Petkoski, former Head of Business, Competiveness and Development program at the World Bank Institute is a lecturer and Senior Fellow at Lawrence Zicklin Center for Business Ethics Research, Wharton School, University of Pennsylvania. He also serves as an adviser and consultant to the World Bank, Organization of American States, and other development organizations. He believes the new oversight and compliance guidelines “can create a transparent business and policy ecosystem that will benefit the citizens and the private sector. Through responsive regulations, governments can create an environment of fair competition. The main benefits that companies can provide to society is offering quality goods and services at affordable prices. This can only be achieved in a market place free of corruption” (D. Petkoski).

Transparency International (TI) is a global civil society organization in the forefront of the fight against corruption. In October 2013, TI released the third edition of their Business Principles for Countering Bribery (Transparency International Business Principles). The Business Principles were developed through a steering committee comprised of academia, business, trade unions and other non-government bodies.

The latest addition of the Business Principles focuses on providing information to assist companies in developing and strengthening their anti-bribery programs. One interesting new recommendation suggests an independent voluntary review be conducted regarding the design, implementation and effectiveness of a company’s anti-bribery program. Public disclosure is also recommended.

shruti Shah, Senior Policy Director of Transparency International—USA, has been very involved in the development of the Business Principles for Countering Bribery and the Verification of Anti-Corruption Compliance Programs which was released in July 2014. Shruti stated that good progress over the last decade has occurred in the development and implementation of US organizations’
compliance programs. Benefits have been realized based on recent DOJ and SEC decisions with regard to FCPA actions. Companies continue to struggle due to lack of resources to provide proper oversight of existing compliance program. Shruti stated that the performance of risk assessments is a critical element of compliance programs as this process allows companies to take a risk-based approach to program monitoring. Shruti states, “the verification of the effectiveness of the program is the most important aspect of a compliance program” (S. Shah, 2014).

According to Shruti, the term verification refers to all efforts, both internal and external, to assess a company's program effectiveness in preventing and detecting corruption. The verification process does not have to be performed by outside experts to be independent, as long as the process is free from management interference and/or fear of retribution. However, Shruti does recommend working with outside attorneys, forensic accountants and consultants as partners to help organizations recognize program gaps and assist in strengthening internal controls.

Shruti further states that “public confidence in corporate self-regulation is currently very low,” therefore companies need to be more transparent and provide greater public disclosures about their compliance programs and their verification process. Actions should include routine communications with regulators, analysts and the media in order to regain the public trust. In summary, Shruti stressed the importance of corporate compliance programs combating corruption with the goal to bring corruption under control by reducing demand. This is the mission of Transparency International and other Non-Government and Civil Society Organizations.

**CURRENT STATE OF REGULATORY COMPLIANCE**

Between January and February 2013, American Lawyer Media (ALM) marketing services conducted a survey of 243 Chief Legal Officers of global companies to assess the corporate counsel’s opinion regarding the greatest threats to their organization’s growth. Respondents were asked to rank their top three concerns. Not surprisingly, economic uncertainty was at the top of the list with 57% of the respondents ranking it their top three. The unexpected finding was that 53% of the respondents named regulatory compliance and enforcement as well (2013 Corporate General Counsel Survey).

When asked to specify which laws in particular caused them the most concern 28% identified the FCPA and 15% identified the UK Bribery Act. This means 43% of the respondents named anti-bribery laws as one of their top three concerns, more than any other law or regulation identified. When asked about the resources spent on regulatory compliance and enforcement the response was also surprising as only 38% of the corporate counsel who identified regulatory compliance and enforcement as a threat, are expending resources to address the threat (2013 Corporate General Counsel Survey).

As a follow up to the 2013 survey, ALM conducted a second survey in early 2014 to gain further insight into corporate counsels’ ability to address regulatory and compliance threats. This time 256 respondents were surveyed, 62% of whom stated that their organization is designing or building some type of robust internal compliance program. Although this is movement in the right direction, over a third of the organizations surveyed still may not be prepared to detect or deter bribery and corruption. Most significantly, they will not be prepared to meet government expectations if a violation occurs and self-reporting is required. Lastly, 54% of the respondents stated that they are building or expanding their in-house systems to address this threat. Many believe that compliance technology is the appropriate answer as regulators prefer technical solutions to these problems, because they are viewed to be sophisticated and state of the art (2014 Corporate General Counsel Survey).

In conclusion corporate compliance programs continue to mature, and are accepted as a cost of conducting business in a global marketplace. The US government is clarifying expectations with regard to corporate responsibility at home and abroad, and working with international partners and their compliance programs. Increased cooperation between public and private sectors to address these issues will assist in leveling the playing field in the global marketplace. Non-government and civil society organizations, i.e. World Bank and Transparency International play a key role in this effort. These organizations set standards, apply pressure on foreign governments to enact stricter anti-bribery and corruption laws, and enforce those laws. Coordination and cooperation among government, business and civil entities, reduce the incidences of bribery and corruption and increase opportunities for companies to compete fairly and ethically in the global marketplace.
WORKS CITED


WILLIAM OLSEN, CFE, CIA, CAMS

Bill Olsen is a Principal and practice leader of the Forensic, Investigation and Dispute Services practice for the Atlantic Coast Region of Grant Thornton. He is also the National Practice leader for Cross Border Investigations and Anti-Corruption services.
Disrupting Terrorist Financing: Interagency Collaboration, Data Analysis, and Predictive Tools
Andrea Lynch Pyon

INTRODUCTION

Dr. Thomas Riley Kennedy O’Connor, a comparative criminologist in the field of terrorism and homeland security, stated that locating and halting the source of terrorist financing involves two tactics, “follow the money and dry up the money” (O’Connor, 2013). There are several fraudulent activities involved with funding terrorist organizations such as: money laundering (trade-based money laundering), Bitcoin operations, cross-border wire transfers, and organized crime (drug trafficking). Law enforcement and government agencies in collaboration with forensic accountants play key roles in tracing the source of terrorist financing to the activities used to inflict terror on local and global citizens. Law enforcement agencies utilize investigative and predictive analytics tools to gather, dissect, and convey data in an effort to distinguish patterns leading to future terrorist events. Government agencies employ database inquiries of terrorist-related financial information to evaluate the possibilities of terrorist financing and activities. Forensic accountants review the data for patterns related to previous transactions by utilizing data analysis tools, which assist in tracking the source of the funds.

According to the Association of Certified Fraud Examiners (ACFE), forensic accountants use a combination of “accounting knowledge with investigative skills in...litigation support and investigative accounting settings” (ACFE, 2014). Several types of organizations, agencies, and companies often employ forensic accountants to provide investigative services. Some of these organizations are public accounting firms, law firms, law enforcement agencies, The Internal Revenue Service (IRS), The Central Intelligence Agency (CIA), and The Federal Bureau of Investigations (FBI).

In 2009, the FBI officially created a forensic accounting position within the Bureau to complement its standard criminal investigations. According to the FBI web page, the Agency utilizes forensic accountants to investigate terrorists “involved in financial wrongdoing” ("FBI Forensic Accountants," 2012). FBI forensic accountants use various investigative tools to track terrorist financing, i.e. government-wide databases and Financial Crimes Enforcement Network (FinCEN) data inquiries to trace illicit funds of suspected terrorists. The search for illicit funding sources commences after Government agencies share information regarding red flags of possible terrorist activities such as money laundering.

Dennis Lormel, a retired FBI Special Agent, has written several papers regarding inter-agency collaboration efforts to impede future terror attacks. According to Mr. Lormel, hybrid terrorism is the new frontier for today’s terrorist groups. In order to run day-to-day operations, terrorists must “continually…[seek new and covert] funding sources” (Singleton, 2011, p. 4). If funds are not available, terrorist groups must raise capital by legal or illegal means. Law enforcement agencies become involved when terrorists engage in illegal activities. Forensic accountants and law enforcement agencies utilize special investigative tools to achieve a higher probability of obstructing the flow of money that finances terrorist activities.

TERRORIST FINANCING

Obstructing terrorist financing requires an understanding of both the original and supply source of the illicit funds. As the financing is derived from both legal and illegal funding sources, terrorists may attempt to evade detection by funneling money through legitimate businesses thus making it difficult to trace. Charitable organizations and reputable companies provide a legitimate source through which terrorists may pass money for illicit activities without drawing the attention of law enforcement agencies. Patrons of legitimate businesses are often unaware that their personal contributions may support terrorist activities. However, terrorists also obtain funds from obvious illegal sources, such as kidnapping, fraud, and drug trafficking (Perri, 2010). Terrorists often change daily routines to evade law enforcement agencies as predictable patterns create trails that are easy for skilled investigators to follow. Darrell Dorrell, a recognized author in the field of forensic accounting and litigation, stated audit "trail[s] can be [traced] from the donor source…to the terrorist" by forensic accountants and law enforcement agencies tracking specific indicators. Audit trails reveal where the funds originate and whether the funds came from legal or illegal sources. Money laundering is a specific type of illegal funding source, which provides a clear audit trail (United States Dept. of Justice, 2014, p. 3).

MONEY LAUNDERING

Money laundering is the process of obtaining and funneling illicit funds in order to disguise the connection with the original unlawful activity. Terrorists launder money in order to spend the unlawfully obtained money without drawing attention to themselves and their activities. In order to remain undetected by regulatory authorities, the illicit funds being deposited or spent need to be “washed” to give the impression that the money came from a seemingly reputable source. There are particular types of unusual transactions that raise red flags associated with money laundering in financial institutions. The more times an unusual transaction occurs, the greater the probability it is the product of an illicit activity.

Money laundering may be quite sophisticated depending on the strategies employed to avoid detection. Some identifiers indicating a possible money-laundering scheme are: lack of identification, money wired to new locations, customer closes account after wiring or transferring large amounts of money, executed out-of-the-ordinary business transactions, executed transactions involving the customer’s own business or occupation, and executed transactions falling just below the threshold trigger requiring the financial institution to file a report.
Money laundering takes place in three stages: placement, layering, and integration. In the placement stage, the cash proceeds from criminal activity enter into the financial system by deposit. During the layering stage, the funds transfer into other accounts, usually offshore financial institutions, thus creating greater distance between the source and origins of the funds and its current location. Legitimate purchases help funnel the money back into the economy during the integration stage, the final stage.

All financial institutions conducting business in the United States are required to know the identity of their clients. The placement stage represents the first and best opportunity to train employees to identify the red flags associated with money laundering. By establishing a customer relationship, both the employee and law enforcement can detect suspicious activity in a timely manner, promote adherence to state and federal laws, and minimize illegal money laundering in financial institutions (A Money Services, n.d.). Financial institutions should maintain professional skepticism of their clientele. When financial institutions complete a Suspicious Activity Report (SAR), they give law enforcement agencies another tool for investigating and preventing financial crimes. Law enforcement agencies use SARs to build cases against known or suspected persons of interest. Unfortunately, terrorists are circumventing regulatory oversight means to monitor suspicious activity and searching out new covert ways to transfer funds from illicit activities across national and international borders.

VIRTUAL CURRENCY

Virtual currency, unlike traditional forms of money, does not leave a clear audit trail for forensic accountants to trace and investigate. Cases involving virtual currency, i.e. Bitcoins, create anonymity for the perpetrator and create obstacles for investigators. Bitcoins have no physical form and provide a unique opportunity for terrorists to launder money across international borders without detection by law enforcement or government agencies. Investopedia describes Bitcoins as "long strings of numbers and letters linked [by using] mathematical encryption algorithms" ("Bitcoin," 2014). A consumer uses a mobile phone or computer to create an online wallet with one or more Bitcoin addresses before starting electronic transactions ("Bitcoin for Individuals," 2014). Bitcoins may also be used to make legitimate purchases through online retailers such as Overstock.com.

The Federal Deposit Insurance Corporation (FDIC) does not regulate or offer "standard deposit protections for Bitcoin transactions" ("Bitcoin for Individuals," 2014). Essentially, this represents a high risk for consumers conducting virtual currency business due to the lack of regulatory oversight. Using Bitcoins to buy illegal goods and services from unlawful online trading services such as Silk Road is one example of high-risk consumerism. In order to obtain anonymity on Silk Road, users accessed a "Tor network (a software protocol that reroutes traffic through hundreds of computer servers to conceal identities)" (Check, 2013). Consumers then anonymously purchased illegal drugs, weapons, fake passports, and the services of computer hackers and hit men using Bitcoins. This virtual shroud of obscurity makes illegal activities difficult to follow; however, the FBI was able to successfully locate and shut down Silk Road in October 2013 because of the sale of "illegal drugs, computer hacking tools and other illicit goods and services" (Smith, 2013).

Ross Ulbricht, the website administrator of Silk Road, was charged by a New York Grand Jury "for participation in a narcotics trafficking conspiracy, a continuing criminal enterprise, a computer hacking conspiracy, and a money laundering conspiracy" (United States of America v. Ross William Ulbricht, 2014). The arrest of Ulbricht played an important role in the fight to eradicate virtual fundraising for terror activities with the use of virtual currency even as the global effects of illicit Bitcoin operations continue to expand.

“On March 18, 2014, David S. Cohen, the Under Secretary of Terrorism and Financial Intelligence, delivered a press release explaining that virtual currency exchangers such as Bitcoin operators and distributors, like Ulbricht, are among a fast growing population of illicit financiers” (Cohen, 2014). Current international anti-money laundering laws aid in fighting the war against terrorist financing; however, international laws “require actual cash shipments between countries and criminal networks (or at the very least funds transfers between banks)” (Check, 2013). International laws are not applicable to virtual currency transactions, as they do not consist of actual cash shipments. According to the website Bitcoin.org, “Bitcoin uses peer-to-peer technology to operate with no central authority or banks” ("Bitcoin for Individuals," 2014). The United States Government Accountability Office (GAO) confirmed this fact to the Committee on Homeland Security and Governmental Affairs, in a report discussing the lack of oversight and accountability of Bitcoins in the regulatory system (United States Government Accountability Office, 2011). The GAO discussed the emerging trend of financial anonymity of Bitcoins and the need for regulators of traditional banking institutions to become more aware of suspicious activities with respect to virtual currency. According to the GAO “because they operate over
Terrorist organizations find virtual currency to be an effective method for raising illicit funds because, unlike cash transactions, cyber technology offers anonymity with less regulatory oversight. Due to the anonymity factor, Bitcoins are an innovative and convenient way for terrorists to launder money and sell illegal goods. In Mr. Cohen’s press release, he stated, “virtual currencies are appealing for terrorist financiers since funds can be swiftly sent across borders in a secure, cheap, and highly secretive manner” (Cohen, 2014). The obscurity of Bitcoin allows international funding sources to conduct exchanges without a trace of evidence. This co-mingling effect is similar to money laundering but without the regulatory oversight. Government and law enforcement agencies must be able to share information with public regulators when they become suspicious of terrorist financing.

**HYBRID TERRORISTS**

Over the past decade, fanatic religious ideologists have evolved to become hybrid terrorists demonstrating exceptional versatility, innovation, opportunism, ruthlessness, and cruelty. Hybrid terrorists are a new breed of organized criminal. Merriam-Webster defines hybrid as “something that is formed by combining two or more things” (“Hybrid,” 2014). In the twentieth century, the military, intelligence forces, and law enforcement agencies each had a specialized skill-set to employ in response to respective crises involving insurgency, international terrorism, and organized crime. Military forces dealt solely with international insurgent threats to the government; intelligence forces dealt solely with international terrorism; and law enforcement agencies focused on their respective country’s organized crime entities. In the twenty-first century, greed, violence, and vengeance motivate hybrid terrorists. According to Mr. Lormel, hybrid terrorists rely on organized crime such as money laundering, wire transfer fraud, drug and human trafficking, shell companies, and false identification to “sustain their organizational operations” (Lormel, “Assessing the Convergence” p. 3). Mr. Lormel described Transnational Criminal Organizations (TCOs) as entities, which “carry out criminal operations across international borders” (2). TCOs usually operate in areas of conflict and upheaval because the citizens are less resistant to corruption and engagement in unlawful activities.

Mr. Lormel described a hybrid terrorist case in which a traditional money-laundering scheme successfully merged with the world of drug trafficking (Lormel, 2013, p. 5). In this case, the Lebanese terrorist group, Hezbollah, joined forces with a known drug trafficking organization called Joumaa. Hezbollah is a profitable hybrid terrorist group in Lebanon. According to the House of Representative Committee on Foreign Affairs, Hezbollah operates with the Lebanese Shia community in productive criminal endeavors and offers socially acceptable aid by operating local schools. The Hezbollah group also “fields its own large paramilitary force, which is considered more powerful than the armed forces of Lebanon” (Terrorist Groups in Syria, 2013). In 2012, Hezbollah was in charge of terrorist plots and assaults on Israeli targets around the world (Terrorist Groups in Syria, 2013).

The Drug Enforcement Administration (DEA) investigated the trade-based money-laundering scheme involving Hezbollah and the Lebanese Canadian Bank (LCB). The court documents noted that LCB was engaged in a trade-based money laundering “through the United States financial system and the used car market” (United States of America v. Lebanese Canadian Bank, 2012, p. 3). Cash raised through Joumaa illicit drug trafficking was then wire-transferred from Lebanon to the United States in order to purchase used cars for follow-on shipment to Africa and eventual resale.

**U.S. CITIZENS: THE RISK OF TERRORIST ACTIVITIES ON PUBLIC TRANSPORTATION SERVICES**

Public transportation service is especially vulnerable to terrorist attacks as evidenced by the 2005 bombings of the London subway, because violence in a highly concentrated area has an immediate disruptive impact on society. Transportation and mass transit industries face increased risk of terrorist attacks as does airport security screening, passenger processing and luggage handling terminals. The Office of the Inspector General (OIG) for the Department of Homeland Security (DHS) conducted an audit of Transportation Security Officers (TSO) in 2012. The audit reported lapses in security screenings at several national airports. The TSO did not provide full security screenings on checked baggage in airports (Office of Inspector General, 2012). The Aviation and Transportation Security Act requires regulated safety procedures for all passengers and baggage entering security checkpoints in the nation’s airports (Office of Inspector General, 2012). The OIG report presented multiple security infractions by the TSO, mainly attributed to lack of training and oversight by management.

The Secure Flight Program, implemented in October 2008, was intended to secure the nation’s transportation sectors after the September 11, 2001 terrorist attacks. To date, however, points of entry into the United States remain vulnerable. The OIG report included numerous instances in which security vulnerabilities would allow terrorists to smuggle explosives onto aircraft and illegally obtain airport security badges to gain access to secure areas.

**GOVERNMENT TASK FORCES**

The U.S. government has created several task forces whose sole mission is to trace terrorist financing locally and globally. These
task forces include: Financial Action Task Force (FATF), Financial Fraud Enforcement Task Force (FFETF), Terrorist Finance Tracking Program (TFTP), and Terrorism and Financial Intelligence (TFI) Task Force.

In 1989, the Financial Action Task Force (FATF) was established to address mounting concerns regarding terrorist organizations using financial systems to launder money for illicit activities. This group is “an international policy-making and standard-setting body, dedicated to combating money laundering and terrorist financing” (“About Us,” 2014).

In November 2009, President Barack Obama created the Financial Fraud Enforcement Task Force (FFETF). The FFETF is one of “the broadest coalitions of law enforcement, investigatory and regulatory agencies ever assembled to combat fraud” (“About the Task Force,” n.d.). The FFETF investigates and prosecutes fraudsters who perpetrate significant financial crimes, take advantage of economic recovery efforts, and recover proceeds of these crimes for victims. “More than twenty federal agencies, ninety-four U.S. Attorney's Offices and state and local partners represent” the task force (“About the Task Force,” n.d.). In order to combat financial fraud across the country, the Task Force has established coordinators in every U.S. Attorney's Office. The FFETF combats many different aspects of financial fraud such as mortgage and predatory lending fraud, Ponzi schemes, procurement fraud, and securities fraud (“About the Task Force,” n.d.).

The Department of the U.S. Treasury enacted the Terrorist Finance Tracking Program (TFTP) after the terrorist attacks on September 11, 2001. The purpose of the TFTP is “to identify, track, and pursue terrorists such as [Hezbollah] and their networks” (“Resource Center,” 2014). Since enactment, the TFTP has disrupted terrorist activities and organizations and saved countless lives. The successful disruption of terrorist activities is due largely to the valuable intelligence provided by both the U.S. and global government agencies. This information led to the “prevention or investigation of many violent terrorist attacks of the past decade” (“Resource Center,” 2014). In recent years, the TFTP has continued to yield reliable information leading to the prevention of terrorist attacks. The Program provides investigative aid to local and state agencies after attacks perpetrated by terrorist violence. Some of the better-known terrorist attacks investigated or prevented by TFTP are the 2012 threats to the London Summer Olympic Games and the “plot to assassinate the Saudi Arabian Ambassador” U.S. in 2011 (“Press-Center,” 2011).

The U.S. Department of Treasury's Office of Terrorism and Financial Intelligence (TFI) persistently seeks out terrorist financing at all levels. TFI accomplishes this by employing the aid of foreign regulators and ministries who strive to make terrorist financing more difficult and eventually obsolete. In his press center brief before the Center for a New American Security, Mr. Cohen described how the TFI found Osama bin Ladein’s “receipts and scribbled on post-it notes” (Cohen, 2014), documenting financial “expenditures on everything from salaries for fighters and their families, to floppy disks, and receipts for explosives” (Cohen, 2014). This information is crucial in the world of financial forensics because even in the foothills of Al-Qaida territory, financial experts can locate receipts and records to analyze and possibly prevent future terror threats. Receipts obtained from Al-Qaida suggest the cost to plan and execute numerous terrorist activities totaled less than $5,000. While the TFI was able to locate Al-Qaida's receipts and documents, the government agency may require the assistance of forensic accountants who are better equipped for the specialized task of tracing and investigating the financial activities of terrorists. Forensic accounting statistical analysis tools strengthen the “identification, analysis, investigation, and prosecution of terrorist and terrorist-related organizations” (Dorrell & Gadawski, 2005).

FORENSIC ACCOUNTING STATISTICAL PROCEDURES

Forensic accountants utilize data analysis tools and technology to aid law enforcement and government agencies in order to track terrorist financing. Traditional types of data analysis tools used by forensic accountants are: Benford’s Law, Accounting Command Language (ACL) software, Interactive Data Extraction and Analysis (IDEA) software, data mining software, and financial statement analysis ratios.

In their Forensic Accounting and Fraud Examination textbook, Kranacher, Riley and Wells discuss how forensic accountants gather data points to decipher patterns in known terrorist financing and activities. Additionally, the authors describe how forensic accountants find correlations between past and present criminal investigations utilizing digital tools and techniques (2011).

BENFORD’S LAW

In 1938, renowned physicist Frank Benford discovered a predictable sequencing pattern when sampling large groups of numbers. Benford found that in any table of data “the first digit’s frequency follows a predictable pattern” (Dubinsky, 2001). Mark J. Nigrini, PhD, professor and author has researched advanced theoretical work on the “applications of forensic analytics to contemporary topics such as the detection of Ponzi schemes, financial statement fraud…and the legal framework of fraud convictions” (2014). Money laundering is one fraudulent financial activity detected by forensic accountants who use Benford’s Law during the course of an investigation into unusual bank deposit activity. Benford’s Law illuminates uncharacteristically high rates of transactional information and is a useful tool to detect and prosecute fraudulent activity. In fact, according to the Director of Forensic Accounting, Tommie Singleton, Ph.D., “Benford’s Law
is legally admissible as evidence in U.S. criminal cases at the federal, state, and local levels. This fact alone substantiates the potential usefulness of using Benford’s Law” (Singleton, 2011). Conversely, one disadvantage of Benford’s Law is the large-scale approach used to detecting fraudulent information. A Benford’s Law analysis populates a broad view of where the fraud could be taking place, instead of a narrowly focused view. This broad view could waste the time and resources of forensic accountants who are searching through a wide array of fraudulent possibilities.

ACCOUNTING COMMAND LANGUAGE (ACL) SOFTWARE

Accounting Command Language (ACL) software aids forensic accountants who analyze transaction data to identify risk and compliance within an organization, and has transformed the way “risk and compliance groups identify, investigate, and mitigate business risks” (“Products,” 2014). Forensic accountants utilize ACL software to uncover instances of fraud, lapses in internal controls, and the misappropriation of funds, as well as quickly analyze and log transactional data to seek instances of duplicate and overpriced vendor invoices, employee mismanagement of funds, fictitious vendors, and other instances of fraud, waste, and abuse. The best use of ACL software is to analyze business records (i.e. payroll and accounts payable and receivable) for company fraud. ACL is also applicable in small businesses that do not house a large amount of data such as small not-for-profits and charities. Interactive Data Extraction and Analysis (IDEA) software is better equipped to handle the size and brevity of large data sets of information.

INTERACTIVE DATA EXTRACTION AND ANALYSIS (IDEA) SOFTWARE

Forensic accountants use the IDEA Data Analysis software, which is similar to ACL software, to analyze large amounts of transaction data within an organization. IDEA software allows the user to recognize patterns, relationships, and anomalies imported from multiple data sets (“IDEA,” 2014). According to the IDEA manual, the user will be able to “perform [an] analysis of data, including [the] calculation of comprehensive statistics, gap detection, duplicate detection, summaries, and aging” (2014). IDEA software is more applicable to audits than forensic accounting investigations. Forensic accountants use IDEA software to expedite the investigation, thus allowing faster analysis of the data. “Data analysis tools allow you to look at the data from different angles to get to the root cause of fraud...Some of the ways data analysis is being used to search for fraud include trend and pattern analysis to look for indications of diversion of funds or theft, behavioral analysis and monitoring of spending trends” (“Top 10,” 2012).

DATA MINING SOFTWARE

Data mining software is a tool utilized by forensic accountants to “look for patterns in large batches of data” (“Data Mining,” 2014). Data mining is useful in tracking terrorist’s financial sources because it is capable of discerning unusual patterns and identifying out-of-the-ordinary transactions (not attributable to normal business transactions).

The Department of Homeland Security (DHS) uses data mining tools to collect an individual’s identifying markers. Some of these markers include educational or employment background and financial transactions “that contain [the] name or the identifying number…assigned to the individual” (5 USC 552a, 1975). DHS utilizes data mining software in an effort to protect citizens from terrorists and national threats of terrorism. However, personal information is sometimes used against the same citizens it was meant to protect. One example of DHS using personal information against a United States citizen was in 2012. DHS used social media monitoring to single out a photographer for the local Miami-Dade Police. The photographer, Carlos Miller, “was going to be taking photographs of the protests at Occupy Miami. DHS said their [practice of] Facebook monitoring is a normal procedure” (Smith, 2013). However, Miller felt DHS infringed on his Constitutional rights.

An audit report produced by the Government Accountability Office (GAO) noted misuse by the DHS of data mining techniques. They found DHS shared information from the Immigration and Customs Enforcement Pattern Analysis as well as the Information Collection program with state and law enforcement agencies thereby violating privacy rules (United States Government, Accountability Office). The GAO investigated the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) data mining tool to determine if privacy risks and inadequate controls were present. The ADVISE data mining tool analyzed the relational data patterns among people, organizations and events, producing visual representations of these patterns. There are risks associated with the ADVISE program include “the potential for erroneous association of individuals with crime or terrorism, the misidentification of individuals with similar names, and the use of data that were collected for other purposes” (Strohm, 2014).

The U.S. Immigration and Customs Enforcement (ICE) office oversees the U.S. and the Data Analysis and Research for Trade Transparency System (DARTTS). DHS uses DARTTS to investigate anomalies in trade-based money laundering and trafficking of stolen goods, as these types of crimes are typical of terrorist activity. The Immigration and Customs Enforcement Pattern Analysis and Information Collection (ICEPIC) program use “multiple data sources” (United States Government, Accountability Office) to compile unique information on subjects who are being investigated for criminal activity. ICEPIC features “the Law Enforcement
Information Sharing Service, a Web service that links federal, state, and local law enforcement information-sharing partners to ICEPIC’s searchable data sets” (United States Government, Accountability Office). According to the DHS 2013 Data Mining Report to Congress, the Agency used a mixture of experience, judgment, and intuition to determine if an individual is actually a person of interest, rather than relying solely on its data mining results. When utilizing data mining techniques, DHS can uphold privacy rights of citizens without jeopardizing the protection from terrorist threats.

**FINANCIAL STATEMENT ANALYSIS RATIOS**

**Acid-Test Ratio**
Organizations use a financial statement analysis to determine if fraudulent activity is occurring. Forensic accountants use a comparative balance sheet to analyze financial data from the previous accounting period relative to the current period. The acid-test ratio determines if the accounts receivable is fictitious. Fictitious accounts receivable indicate inflated sales on a business’s financial reports. Inflated sales may be the result of a shell company used to launder money for terrorist groups. The acid-test ratio divides any cash, securities, and receivables by current liabilities. If the acid-test ratio is abnormally high and the business has no current liabilities to offset the accounts receivable, this could be an indicator of fraudulent activity. The acid-test ratio is one tool in which forensic accountants locate shell companies used to launder money for terrorist activities.

**Profit Margin Ratio Test and the Net Worth Method of Accounting**
The income statement provides the basis for the profit margin ratio test. The profit margin ratio test divides net income by net sales and shows profits earned per dollar of sales. An indicator of fraud is overstated net income with an abnormally high profit margin. The profit margin ratio test is performed to identify whether further analysis of the business entity is required.

The net worth method of accounting was a simple equation implemented in the eventual arrest and prosecution of Al Capone, the famous American gangster, on tax evasion charges. Law enforcement agencies and forensic accountants use the net worth method to determine if fraudulent activities were occurring. The net worth method utilizes a simple equation of an individual’s income less any expenses. If an individual’s net worth is higher than income, this may be an indicator of fraud. The person is not reporting all income to the Internal Revenue Service for the proper withholding of taxes. Forensic accountants and law enforcement agencies analyze the individual’s income and expenses to determine if further investigative measures are needed.

**Gross Profit Margin**
The Gross Profit Margin Test is used to “assess a firm’s financial health by revealing the proportion of money remaining from revenues after accounting for the cost of goods sold” (“Gross Profit Margin,” 2014). A forensic accountant uses the gross profit margin test to determine if money laundering is occurring within the business. To calculate the gross profit margin, the accountant divides an organization’s revenue, less the cost of goods sold, by revenue. The resulting ratio should remain approximately the same from one period to the next on the company’s income statement. Drastic changes in the resulting ratio should trigger a red flag indicating a possible money-laundering scheme, with further investigation necessary.

**LAW ENFORCEMENT AGENCIES**

**Predictive Analytics**
Law enforcement agencies use statistical methods to measure risk and predict criminal activity. Some of these techniques use software such as: ArcView Geographic Information Systems (ArcGIS), Statistical Package for the Social Sciences Predictive Analytics (SPSS), Probability Grid Method (PGM), and Risk Terrain Modeling (RTM).

**ArcView Geographic Information Systems (ArcGIS)**
ArcGIS is an analysis tool used by law enforcement agencies to create a complete framework that permits individuals to gather, arrange, oversee, dissect, and convey geographic data (“Introduction to ArcGIS,” 2014). State, local, and federal government agencies use the Geographic Information Systems (GIS) feature to produce and compile information into intelligent maps. Spatial analysis tools apply “geographic, statistical, and mathematical operations to...mapped data” (“Introduction to ArcGIS,” 2014) that aid law enforcement agencies in tracking terrorist activities. GIS technology aids law enforcement agencies in determining where particular crimes are occurring, the types of crimes committed, and the number of officers and patrols to deploy during peak times of criminal activity. Arc/GIS technology became necessary immediately following the attack during the Boston Marathon bombing in 2013. Arc/GIS was used to “assist local emergency response teams and news agencies with essential map services...of the marathon route, points of interest, and the locations of the bomb explosions” (“ArcNews,” 2013).

**IBM Statistical Package for the Social Sciences Predictive Analytics (SPSS)**
IBM’s SPSS gives law enforcement and government agencies the ability to anticipate unlawful actions of terrorist organizations. SPSS gathers and analyzes a vast array of data from various sources to determine fraudulent activity and future threats. SPSS assists clients through intelligent decision-making, “sophisticated pattern recognition, and anomaly detection...capabilities” (“Public Safety,” 2010). Government agencies use SPSS predictive analytics to “perform risk analysis” to detect money laundering and terrorist financing (“Public Safety,” 2010). The sheer volume of data the software is equipped to measure makes it extremely useful to create profiles of past activity and detect current suspicious activities. The IBM SPSS predictive information software is easily accessed and...
utilized by government agencies for surveillance, communication interception, and to trace the online presence of terrorist groups. The IBM SPSS aids law enforcement and government agencies in anticipating and preventing terrorist activities both before and in real-time, rather than after the fact.

**Probability Grid Method (PGM)**
Paul Catalono, Brennan Long, and Bryan Hill developed the Probability Grid Method (PGM), a tool that predicts criminal activity before it occurs. In Phoenix, Arizona, law enforcement agencies used PGM methodology in criminal cases involving arson, burglary, and theft. PGM works together with ArcGIS software to analyze data from different sources to distinguish spatial patterns, trends, and future events. PGM enables law enforcement to utilize statistical methods along with practical experience in a particular area of interest. PGM software would be beneficial in aiding law enforcement agencies with predicting and tracking terrorist activities.

**Risk Terrain Modeling (RTM)**
Law enforcement agencies continuously look for efficient ways to anticipate unlawful behavior. During peak times of criminal activity, law enforcement agencies could use predictive analytic tools, such as Risk Terrain Modeling (RTM) for greater proficiency in monitoring and anticipating criminal movement. RTM creates a high-risk map by inputting data of past behavior, physical qualities, and criminal wrongdoings for a particular geographical area. Law enforcement agencies are then able to determine the risk factors of particular criminal activity occurring over time. For example, law enforcement agencies utilize the RTM technology to assign more officers to areas with a higher amounts of criminal activity during specific times of the day. RTM technology is one method law enforcement agencies utilize to determine possible terrorist activity in the United States mass transit system. Armed with RTM predictive analytic technology, law enforcement agencies are better equipped to protect U.S. citizens from violent acts of terror.

**Government Database Inquiries**
Government agencies employ database inquiries to look at terrorism-related financial information to investigate the possibilities of terrorist financing and activities. Forensic accountants utilize those government-wide database inquiries to conduct additional financial inquiries into the credit history and bank account activity of suspected terrorists. The information obtained within the database provides information such as “business data, source of income, tax status, education, and travel information, limited credit information, and telephone subscriber information” (U.S. Dept. of Justice, 2014). FBI database inquiries permit users to create a query within the Automated Case Support (ACS) system and the Universal Index for FBI case files. FinCEN data inquiries allow the user to search for and investigate financial transaction information at the federal, state, local, and international level (U.S. Dept. of Justice, 2014). The FinCEN database includes all banking and money-laundering SARs and personal information such as bank account numbers, known addresses, business associates, and potential criminal activity (U.S. Dept. of Justice, 2014).

**INFORMATION SHARING**
Government agencies may have had information about a possible terror attack leading to the 9/11 terrorist attacks. “According to the 9/11 Commission Report the biggest impediment to…connecting the dots is the human or systemic resistance to sharing information” (“National Commission,” 2004). The following is “an FBI agent’s reaction after 9/11 on discovering the CIA possessed information relevant to the investigation of al-Qa’idah” (Lamb & Staine-Pyne, 2014).

For about a minute, I stared at the pictures and the report, not quite believing what I had in my hands. We had asked the CIA repeatedly during the USS Cole investigation if they knew anything about why Khallad had been in Malaysia…. Each time we had asked—in November 2000, April 2001, and July 2001—they had said that they knew nothing. But[sic] here in the file was a very different answer: they had in fact known…. I walked out of the room, sprinted down the corridor to the bathroom, and fell to the floor next to a stall. There I threw up…. The same thought kept looping back: If they had all this information since January 2000, why the hell didn’t they pass it on (Lamb, Christopher, & Staine-Pyne).

The 9/11 Commission Report discussed the many levels of hierarchy required for interagency collaboration. These levels of hierarchy led to wasted time in implementing and responding to terror threats. Members of the 9/11 Commission Report stated, “we had to fight to get access to documents we needed, fight to get people we needed to testify to make our cases. Nothing was easy” (Grumet, Hamilton, & Kean, 2014). The 9/11 Commission found Congress to be “resistant to needed reforms” (Grumet, Hamilton, & Kean, 2014). In 2004, the DHS “reported to 88 committees and subcommittees of Congress. The Commission urged Congress to reduce that number. Incredibly, it has since increased to 92’” (Grumet, Hamilton, & Kean, 2014). In times of catastrophe, this means that DHS has to navigate 92 different committees to achieve the agency objectives.

**CONCLUSION**
Forensic accounting technology is beneficial when used in conjunction with the analysis tools of law enforcement agencies to predict and analyze future terrorist activity. Even though some of the tools in a forensic accountant’s arsenal are useful in tracking terrorist funds, the ability to identify conceivable terrorist threats is limited. To identify the future activities of terrorist groups, forensic accountants, and law enforcement agencies should cooperate with
one another by incorporating the analytical tools utilized by each agency. Agencies and government officials should become familiar with virtual currency like Bitcoins. Because of the anonymity and lack of regulatory oversight, virtual currency offers terrorist groups a useful means to finance illicit activities on an international level. A new government agency may be needed to tie together all of the financial forensics efforts of the different organizations so that information sharing is not compartmentalized.

REFERENCES


Dubinsky, B. G. (2001). Math formula fights fraud: Benford’s law plus technology can detect white collar crime. Legal Times, XXIV.


ANDREA PYON

Andrea Lynch Pyon is an auditor with the Office of Legislative Audits (OLA) in Maryland. Before joining OLA, she worked as a Fiscal Grants Specialist/Audit Coordinator with the Governor’s Office of Crime Control & Prevention. Mrs. Lynch Pyon has a B.S. in Accounting from the University of Maryland University College and is currently a student in the Masters of Forensics Studies – Accounting track at Stevenson University.
Eradicating Elder Financial Abuse
Cheryl A. Panattoni

By the year 2030, it is estimated that seniors over the age of 65 will comprise 72 million people (Reiser & Eisenkraft, 2013, p.1). When does the aging process begin to affect one’s mental capacity thus diminishing the ability to make sound financial decisions? As reported by the Alzheimer’s Association, once an individual attains the age of 65, diminished capacity may result. By the age of 90, fifty percent of seniors will experience some form of disability and/or mental deterioration that will require outside assistance to perform daily tasks (Alzheimer’s, n.d.). Who will supervise these individuals to ensure financing decisions remain in the best interest of the senior citizen? A process should be developed which protects individuals and their assets, decreases the opportunity for financial fraud, and prevents access by scrupulous parties.

Federal and state agencies have approached this concern by issuing grants, establishing coordination teams, and drafting legislation, i.e., the Affordable Care Act, Dodd-Frank Act, and California Elder Abuse Act. Building a coalition among private sector, nonprofits, federal and state agencies in order to develop a proactive approach could reduce and eventually eliminate elder financial abuse. This article explores the feasibility of creating a proactive model which combines the resources of federal and state agencies, private sector, nonprofits, healthcare professionals and legal experts. Investigating the feasibility of this proposal requires a clear definition of the problem, how it manifests, why this form of abuse is problematic, current costs to society, and applicability of current laws to solving the problem.

ELDER FINANCIAL ABUSE DEFINED

As noted in A Family Systems Perspective Of Elder Financial Abuse, “Financial abuse, or exploitation is limited to, the illegal or improper utilization of an elder’s funds, property, or assets.” The authors, Gibson and Qualls, discuss “undue influence” or the “ability of someone to misuse their power to exploit the trust of a weaker person’s decision-making” as important factors when defining this type of abuse. (2012, p. 26).

WHAT DOES ELDER FINANCIAL ABUSE REALLY LOOK LIKE?

A Family Systems Perspective Of Elder Financial Abuse defines the typical victims as “white, widowed females who are ages 70 to 89 years” (Gibson & Qualls, 2012, p. 26). Elder financial abuse assumes many forms and occurs across varied demographics. Famous personalities such as Mickey Rooney, Zsa Zsa Gabor, J. Howard Marshall (married to Anna Nichole Smith), and Liliane Bettencourt (heiress to the L’Oreal fortune), are victims of financial fraud (Peck, 2012). Sandra Timmermann, offers examples in her article Financial Gerontology. The first example discusses a caregiver who borrowed $80,000 over the course of several years and subsequently gambled away the money. The $80,000 loan was never repaid. Example two also implicates a caregiver. Hired by an elderly man to care for his wife who suffered from diminished mental capacity, the caregiver persuaded the elderly husband to sign over a general power of attorney allowing the perpetrator access to the couple’s financial resources, in the amount of $200,000, to obtain a mortgage on their home, and accrue tens of thousands of dollars in credit card debt (2009, p 23).

Personal interviews conducted by the author highlight additional instances of elder financial abuse. Phyllis Horsley, Enrolled Agent (who is allowed to represent individuals in front of the Internal Revenue Service and state agencies), and Lynn Ursiny, Senior Director of Risk Management within a Northern California acute care hospital, each shared stories of clients affected by elder financial abuse. Ursiny explained incidents of financial abuse, including, “Mismanaged social security checks, family or friends having access to patients’ personal assets and using them inappropriately, caregivers withholding care, and the insistence that a patient remain alive (despite a very poor expected outcome) simply to keep money coming into the family via social security or In Home Support Services funding” (2014).

A senior can become a victim under four different scenarios:

1. the senior is a “financial prisoner,” physically and perhaps psychologically dependent on a caregiver;
2. the senior is losing the ability to handle financial affairs because of physical or cognitive impairment, a “new best friend” gradually assumes the responsibility for handling the senior’s affairs and then abuses that trust;
3. a widow or widower does not know how to handle financial affairs that their deceased spouse used to take care of and is taken advantage of by someone offering assistance; and
4. a senior, perhaps out of fear or paranoia, refuses help or financial advice from reliable, responsible relatives or other individuals and instead turns to strangers” (Reiser & Eisenkraft, 2013, p. 2).

The incidents described above appear to match the scenarios listed by Reiser and Eisenkraft and confirm the need for a different approach to fighting elder financial abuse. Although the hospital where Lynn Ursiny works has mandatory reporting requirements to “appropriate authorities” or to a Medical Social Worker, initiating an assessment from a new centralized agency, might have provided better protections for the at-risk seniors (2014).

HOW IS ELDER FINANCIAL ABUSE CURRENTLY REPORTED?

Thomas L. Hafemeister, author of Financial Abuse of the Elderly in Domestic Setting, explains that most state agencies have mandatory or voluntary reporting requirements, but reporting and case processing requirements vary within each state. Most states have
a reporting requirement for the following professionals: police, social workers, public assistance and mental health workers, nursing home employees, and licensed health care providers. They are required to report possible incidenes to agencies and, as a result, an investigation commences within a prescribed period of time—normally 48 hours. If the agency processing the initial report is not a law enforcement entity, the agency will turn the case over to a law enforcement agency if it is believed a crime had been perpetrated (2003). There are reporting agencies within each state; however, there is no “one” cohesive centralized agency with the ability to immediately assess the senior’s situation and put processes in place to protect the senior’s assets.

Expanding the scope of professionals who must report should include: financial planners, accountants, bankers, funeral home directors, and church officials. Each would be in the position to assess how the individual is affected by life events. For example, a funeral home director helping a family bury an elderly parent might notice that the spouse is not sure of her financial situation or appears to have diminished mental capacity. If the employee of the funeral home was required to report an at-risk senior, the “opportunity” for those to take advantage of the senior may be diminished.

Jill Panattoni, a Marriage and Family Therapist, works extensively with seniors over the age of 60 (2014). Prior to becoming Program Director of an elder wellness program, she provided therapy, social rehabilitation, and case management services for adult patients. Panattoni explained how she and her staff are mandated to report possible instances of abuse and the process once an allegation is reported.

1. Every Adult Protective Services (APS) case starts with the initial abuse report. In order for the APS program to respond, a report must be filed with the Intake Unit. The mandatory reporting laws exist to ensure that victims of abuse get the help they need as quickly as possible.
2. California Law, under the Welfare & Institutions Code for Elder Abuse, mandates reporters to make a verbal report immediately or as soon as possible, followed by a written report within two working days.
3. A victim of abuse may refuse or withdraw consent to any investigation or provision of services, which are initiated as a result of the report, unless a violation of the Penal Code has been alleged.

Sheri L. Hoffman, Attorney at Law, explains that she has observed suspected elder abuse in her practice. Hoffman stated, “Yes, I have suspected this (elder financial abuse), but without the consent of my client to take any action, I am prohibited by the rules of ethics from calling any county services organization. All I can do is speak with the client independently, counsel the client about their concerns, and the options available” (2014). Additional study is required to identify a means to balance individual confidentiality against professionals seeking to protect at-risk seniors without creating an ethical dilemma.

WHY SHOULD SOCIETY CARE ABOUT THIS PROBLEM?

The fraudulent depletion of seniors’ resources places the burden of paying for elder care on the rest of the U.S. population. This may include imposing higher taxes to fund the gap of the social welfare agencies. With the recently enacted Affordable Care Act, new taxes have already been enacted, i.e., the 3.8% investment tax that applies to those citizens that hold investments and generate income of $200,000 or more (Obama Care, 2008, pp. 1-7). Over $5 million dollars within the Affordable Care Act has been set aside to establish a federal elder justice coordination team in an effort to further protect seniors (Fleck, 2012). Extended family members are also affected by the fraudulent depletion of a senior’s financial resources. These family members would experience the reduction of their own resources if forced to support the senior.

Hafemeister further notes that as a result of abuse, the senior’s life might also be cut short due to fear, depression, suicide, or hopelessness (2003). The cost of elder financial abuse may extend beyond the death of a victim, as it affects beneficiaries who would otherwise inherit the assets. The impact to the profitability and reputation of financial institutions that create products to help seniors sustain a better quality of life could be adversely affected—if elder financial abuse is not eliminated. For example, if the popular reverse mortgage product (a product allowing a senior to receive a tax-free payment each month that taps into the equity of their primary residence) were to be found “financially abusive, Congress could prevent its sale.”(Reiser & Eisenkraft, 2013).

WHAT LAWS HAVE BEEN ENACTED AND WHAT HAS BEEN THE IMPACT IN COMBATING ELDER FINANCIAL ABUSE?

Specific laws have been created by federal and state agencies in an effort to combat the growing problem of elder financial abuse. The Dodd-Frank Wall Street Reform and Protection Act contains the “senior-specific provision”—called the Senior Investment Protection Act of 2008. (Reiser & Eisenkraft, 2013, p. 1). This Act:

…protects older Americans from misleading and fraudulent marketing practices, with the goal of increasing retirement security through “grants” enabling states to investigate and prosecute those who sell financial products through “misleading and fraudulent marketing practices,” provide educational materials to help seniors avoid becoming a victim, “establish reporting requirements, application procedures, appropriate use of designations in the offer or sale of securities, investment advice, and the sale of insurance products” (2008, S.2794: pp. 2-10).
The Affordable Care Act authorized funds to create a “federal elder justice coordination team.” The team is charged with combining previously fragmented elder abuse initiatives across the federal government and determines what actions are needed to enhance protection efforts.” (Fleck, 2012). The Elder Justice Act directs the Department of Health and Human Services to develop this “coordination team” among other efforts to “focus on education, research, leadership and guidance in establishing programs to prevent elder abuse.” (USC, n.d.). Although Congress has authorized 125 million dollars for the directives of the Elder Justice Act, only $8 million was actually appropriated to the 2013 federal budget (NAPSA, n.d.).

The California Elder Abuse Act provides strong “remedies” for those affected by financial abuse to include: “the ability to recover damages for mental suffering, attorney fees, punitive damages and injunctive relief.” The Act punishes representatives (conservator, trustee, or representative of an estate) and businesses (real estate or other professionals) who perpetrate financial abuse against a senior. The Act also specifically mentions “additional protections” for those seniors who suffer from diminished mental capacity (Freni, 2011). California’s law appears strong, however, it remains reactionary in nature as the fraud must have already been committed. The other laws described above contain some preemptive provisions. Current funding, however, is insignificant thus providing minimal impact on elder financial abuse. Sheri Hoffman, Attorney at Law, explained, “The biggest problem I see is the enforcement of the laws. There are not enough funds available to properly enforce the laws that are put in place. Without a funding mechanism, the laws aren’t worth the paper they are written on” (2014). A better approach might be to encourage the private sector and nonprofits in partnership with federal and state agencies to develop a model that can be self-sufficient and not wholly dependent on governmental funding. The government can demand accountability through the drafting of laws, but the development, implementation, and monitoring should come from the private, nonprofit, legal, and law enforcement sectors.

EXPLORATION OF CREATING A CENTRALIZED AGENCY: A NEW MODEL

Federal and state agencies in partnership with law enforcement, nonprofits, the private sector, and the court system must work together to develop a new model to eradicate elder financial abuse. This new model’s primary concentration should be creating preemptive measures and processes to immediately protect the senior’s financial resources. University of California, Irvine-School of Medine-Center of Excellence in Elder Abuse and Neglect illustrates an example of a working collaboration in which they participate. The Elder Abuse Forensic Center of Orange County, California, has experts from legal, medical, social services, and law enforcement backgrounds. They have effectively changed the elder abuse investigation process. The Forensic Center members: perform case reviews; check in-home medical and mental status; conduct evidentiary investigations; tape victim interviews; educate; consult and do research. This collaborative approach results in a better understanding, identification and treatment of elder abuse cases. Results also include effective and successful prosecution of elder abuse cases, and prevention through awareness and education programs (UOCI, n.d.).

The Elder Abuse Forensic Center of Orange County model resolved the most difficult component of developing a new process – encouraging professionals from different sectors to work together to generate change. Building on this model could result in the creation of a central agency serving as the first contact to implement a proactive protection program. This central agency could handle the entire process: investigating, assigning professional teams, monitoring and compliance. This approach would remove the court system from the process of assessing a senior’s situation and assigning guardians.

For a new central agency to work, first and foremost, the current requirements for reporting and initiating an inquiry would need to be enhanced. Physicians and attorneys should not be bound by their profession’s ethics when they come in contact with a high-risk senior. If they suspect possible risk to a senior, they should be granted the ability to initiate an inquiry with this new agency. Mandatory reporting should be expanded to include life-altering events such as the death of a spouse, the diagnosis of dementia, or other forms of diminished mental capacity.

The initial contact with this new central agency would be an inquiry, not an investigation, thereby negating confidentiality issues and the ability of a senior (who may not possess the mental capability to fully realize what is happening) from refusing help. The central agency would open an inquiry within 48 hours of initial contact. Ms. Hoffman, as noted, “the county and state departments are so back-logged and overrun with complaints that it is difficult to investigate in a timely manner and in the manner that each case should be handled” (2014).

Adult Protective Services (APS), Medical Social Workers, Ombudsmen, and other state and local authorities, should be reinvited or absorbed into this new central agency. The agency could: eliminate duplicate processes, lengthy investigation times, broken communication streams, confidentiality and legal constraints, funding concerns, and losing track of an at-risk senior.

The agency should have the authority to interview those closest to the senior: family, friends, doctors, bankers, and others in close contact with the senior in order to determine the elder’s living arrangement, financial resources, and the potential for financial abuse. Once the situation has been fully assessed, a team of professionals, including a Certified Financial Planner, a Certified Public Accountant, and an attorney would be assigned. This team
would replace the court-appointed guardian used in the past. The state courts could concentrate their stretched resources on prosecuting perpetrators of financial fraud.

The central agency would monitor the recommended financial plan established by the team. The financial planner would ensure the financial resources of the at-risk senior were invested conservatively in accordance with standards previously determined. The accountant would be responsible for bill paying and cash account reconciliation on behalf of the senior and monthly reporting of income and expenses to the central agency, financial planner, attorney, and family. The attorney would be responsible for protecting the at-risk senior’s living at home or in the extended care facility, as well as monitoring real and personal property assets. The team’s assignment ends upon death of the senior and the distribution of the estate to the legal beneficiaries.

Developing several funding streams to support this central agency will be critical. According to National APS Resource Center (funded by the U.S. Administration on Aging) report, Adult Protective Services: In 2012: Increasingly Vulnerable, funding comes from a variety of sources but not from the federal government. Twenty-five states obtain their funding from the “Social Services Block Grant” program, while other states rely on the “Older Americans Act,” A few states use “targeted case management funds” from the Medicaid program. (n.d., p. 12). Additional research is required to consider whether these revenue streams would be a viable option if APS were to be absorbed into this new central agency.

Assessing the ability of high-risk seniors to fund their own costs must be explored. Reiser and Eisenkraft state, “As of 2007, seniors owned 80 percent of all the money in US savings and loan institutions, and 77% of all financial assets in the United States. As of 2009, it was estimated that US citizens aged 65 or older held $18 trillion of assets.” It would appear, based on these projections, many at-risk seniors may have the financial resources necessary to cover the cost of providing a team of professionals to manage their assets. It would be necessary, however, to compare statistics from data compiled from many sources, including the Association of American Retired Persons (AARP), the National APS Resource Center, American Society on Aging, and the National Center on Elder Abuse to discover the average amount each senior has in investments instead of generalizing. Detailed statistics could be obtained through the assessment process of the central agency to verify how many seniors hold the 18 trillion dollars.

Considering the feasibility of enhancing current or developing new insurance products to help defray the costs of managing the at-risk senior’s financial resources may be an option. A new product may act similar to a long-term health insurance plan. The policy would be actuated once the central agency’s services were deemed necessary. This “new” insurance policy would cover the costs of the team of professionals until the elder passed away and their estate settled.

Provisions might be included within already established health care insurance policies and included within the Affordable Health Care Act. Enhancements to supplement coverage as provided through AARP or other agencies should be considered.

Lastly, one must explore who would be more capable of handling this new central agency. Federal, state, and local agencies have assumed the responsibility for targeting elder financial abuse, however, these agencies cannot meet demand, lack funding, and have limited staffing resources. There are many successful leaders within the private and nonprofit sectors, yet accountability might be an issue. A balanced partnership between the agencies, nonprofits, and the private sector may be the best approach. The partnership model of The Elder Abuse Forensic Center is a good basis from which to grow and expand.

CONCLUSION

Elder financial abuse can only be eradicated if a preemptive approach is implemented. One must understand the history and growth of elder financial abuse, the government’s attempt to enact new laws, the current reactive process, and the cost to society, before brainstorming can commence to develop a better model. Only through a partnership between agencies, state and local authorities, private sectors, law enforcement, and nonprofits can one produce a central authority that could become the shield to protect the aging population from financial abuse.

REFERENCES


Data Analysis and Reliability in Predicting Fraud
Joseph T. Harris, CIA, CFE

INTRODUCTION

Background
Global Capital Markets rely on truth, accuracy and transparency in financial reporting. When financial statements are released by public companies the words and figures tell a story. The story is of particular interest to major stakeholders such as institutional investors, bankers, creditors, employees, and regulators. The speed and efficiency of the financial reporting system in the United States makes it convenient for stakeholders to sift through financial reports, analyze large volumes of data, and extract information relevant to their decisions regarding investment opportunities, emerging industry patterns, or global challenges impacting a specific country. However, over the past decade, a serious problem has surfaced: companies engaging in deceptive financial reporting. Equally disturbing is that, despite the intense scrutiny of public audits, massive fraud occurs and remains undetected for periods ranging from years to decades.

In December 2008, reports of the $65 billion dollar fraud involving Madoff Investment Securities LLC were front page news (Frontline, 2009). This was considered the longest running Ponzi scheme in U.S. history. The mastermind behind the fraud, Bernie Madoff, misled investors for nearly eighteen years, however, it was preceded by the 2001 $74 billion dollar Enron fraud, the 2002 $11 billion dollar WorldCom fraud, and the 2003 $4.6 billion dollar HealthSouth fraud. (Crawford, 2005; Freudenheim, 2004; Weld, Bergevin, & Magrath, 2002)

The problem of financial reporting fraud is not exclusive to public corporations. In 2012, the collapse of Dewey & LeBoeuf, LLP was considered the largest bankruptcy ever filed by a law firm in the United States. The failure was the result of hidden financial concerns to include increasing debt and cash flow problems. In April 2012, the city of Dixon, Illinois discovered it was a victim of “the largest municipal embezzlement in U.S. history,” perpetrated by Rita Crundwell, the City Controller. By the time the fraud was discovered Crundwell had embezzled $54 million dollars over a twenty-two year period. (Katersky, 2014; McKenna, 2013)

Despite the Securities and Exchange Commission’s (SEC) ongoing efforts to fight fraud it is apparent that large scale financial statement fraud will continue to be a problem. Stakeholders must use more effective detection methods, and exercise vigilance in the pursuit of financial reporting fraud. One method commonly used by auditors to identify fraud is data analysis. Although, data analysis can be helpful in detecting fraud, the question remains if data analysis is reliable enough to consistently detect fraud in financial reporting. This question is worth examining since it could potentially translate into billions of dollars in cost savings over the next decade.

EXPLORING DATA ANALYSIS

Corporate financial reports can portray operational success, but unless the information is examined carefully it may prove to be an optical illusion created by highly paid executives as a means of bolstering their bank accounts. As companies pursue financial statement fraud schemes, a series of effective data analysis methods may help stakeholders to curtail these deceptive practices. Data analysis is defined as “the process of evaluating data using analytical and logical reasoning to examine each component of the data provided. This form of analysis is just one of the many steps that must be completed when conducting a research experiment. Data from various sources is gathered, reviewed, and then analyzed to form some sort of finding or conclusion. There are a variety of specific data analysis methods, some of which include data mining, text analytics, business intelligence, and data visualizations” (WebFinance). Data analysis is used by financial professionals, such as public accountants, internal auditors, securities analysts, bankers and industry regulators, however it is the type of analysis performed which determines overall effectiveness. To understand both the power and limitations of data analysis, it is necessary to identify practical examples where its application has succeeded in identifying financial reporting anomalies that could indicate fraudulent activities.

EXAMPLES

DSI Index
In his internet blog, convicted fraudster and former CFO of Crazy Eddie, Sam E. Antar, posted public statements about Nu Skin questioning the company’s growing inventory levels in relation to its sales trends. (Antar, July 22, 2014) Mr. Antar relied, in part, on an analysis he performed of the company’s inventory turnover measurement based on details cleaned from published financial reports. After posting comments on his blog, he continued following the company’s financial performance and provided periodic updates. It is interesting to note the timeline between comments posted by Mr. Antar and the subsequent public disclosures released by Nu Skin. On July 22, 2014, an initial observation was made by Sam Antar regarding the potential buildup of inventory at the company. Too much inventory buildup can be a significant development because the excess may be difficult to sell and ultimately lead to a write-down of inventory. On August 4, 2014, two days prior to Nu Skin releasing its second quarter operating results, Mr. Antar posted another blog urging the company to be truthful about its excess inventory problem (Antar, August 4, 2014). His suspicion of excess inventory buildup was confirmed two days later, on August 6, 2014, after Nu Skin released its second quarter results, which included a $50 million write-down of inventory (Nu skin enterprises reports second-quarter results, 2014). Despite the company’s inventory write-down, about a month later Mr. Antar continued to insist that based on his DSI analysis there could be more inventory surprises to come (Antar, September 8, 2014).
In the above example, the type of analysis performed studies the amount of time it takes a company to sell its inventory and evaluates that information against the company’s sales growth. To do this, a special ratio is used: Days-Sales-In-Inventory (DSI) Index, which estimates the number of days it takes for a company to convert its inventory into sales (Figure/Refers). In essence, the higher the ratio, the longer it takes to convert inventory to sales. As the trend gets further out of a company’s normal range it could point to concerns such as inventory mismanagement, overvaluation or obsolescence. The DSI analysis in this particular case employed horizontal analysis, whereby the analyst compares changes that occur between two periods for the same company.

**Figure 1**

\[
\text{Ending Inventory} \times \frac{\text{Number of Days in Period}}{\text{Cost of Goods Sold}} = \text{Days' Sales Inventory Index}
\]


In Mr. Antar’s initial blog post of July 22, 2014, he highlights the financial details, calculations and exhibits that show a growing trend of inventory buildup at Nu Skin based on its Days-Sales-In-Inventory measurement. Figure 2, below shows that in each quarter presented the “DSI Current Period” and “DSI Previous Period” is used to calculate the DSI “Change over Previous Year Period” (Antar, July 22, 2014). This calculation continued to increase in every quarter except June 30, 2012. As an example, the DSI “Change over Previous Year Period” was up 43.7% in March, 2012 and had risen to 132.3% by March, 2014 (Antar, July 22, 2014). In addition, inventory measured at the lower of cost or market had risen from 7% to 175.5% during the past several quarters (Antar, July 22, 2014). This meant that the increase in inventory was significantly higher than the increase in Cost of Goods Sold, during the same period of time. While inventory grew at a rate of 175.5%, in the first quarter 2014, the Cost of Goods Sold only grew 18.6% (Antar, July 22, 2014). Since this pattern was consistent in several previous quarters it pointed to the same conclusions as the DSI analysis according to Mr. Antar (Antar, July 22, 2014).

**DSR Index**

Calculating a company’s Days-Sales-in-Receivable (DSR) Index is another meaningful measure that can be used in financial data analysis. This analysis examines a company’s sales figures in relation to its receivables figures to assess overall financial health of receivables. The index determines the number of days it typically takes a company to convert its accounts receivable into cash. Since the DSR measure links sales and receivables figures together, a substantial increase in the index could be indicative of fictitious receivables and sales. See Figure 3 for DSR calculation.

**Figure 2**

<table>
<thead>
<tr>
<th>Quarter Ended</th>
<th>Revenue Guidance (Min.)</th>
<th>Revenue Guidance (Max.)</th>
<th>Reported Revenues</th>
<th>Excess Revenues over Maximum Revenue Guidance</th>
<th>Cost of Goods Sold</th>
<th>Change over Previous Period</th>
<th>Inventory at lower of cost or market</th>
<th>Change over Previous Year Period</th>
<th>DSI Current Period</th>
<th>DSI Previous Period</th>
<th>Change over Previous Year Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/31/14</td>
<td>$650</td>
<td>$670</td>
<td>$671.1</td>
<td>$1.1</td>
<td>$106.7</td>
<td>18.6%</td>
<td>$410.7</td>
<td>175.5%</td>
<td>346.4</td>
<td>149.1</td>
<td>132.3%</td>
</tr>
<tr>
<td>12/31/13</td>
<td>$1,020</td>
<td>$1,050</td>
<td>$1,055.8</td>
<td>$5.8</td>
<td>$164.7</td>
<td>73.2%</td>
<td>$339.7</td>
<td>150.0%</td>
<td>189.8</td>
<td>135.1</td>
<td>44.3%</td>
</tr>
<tr>
<td>9/30/13</td>
<td>$790</td>
<td>$810</td>
<td>$908.3</td>
<td>$98.3</td>
<td>$139.8</td>
<td>61.2%</td>
<td>$254.2</td>
<td>85.4%</td>
<td>167.3</td>
<td>145.5</td>
<td>15.0%</td>
</tr>
<tr>
<td>6/30/13</td>
<td>$570</td>
<td>$580</td>
<td>$671.3</td>
<td>$31.3</td>
<td>$90.0</td>
<td>18.7%</td>
<td>$149.1</td>
<td>23.5%</td>
<td>149.1</td>
<td>144.9</td>
<td>2.9%</td>
</tr>
<tr>
<td>3/31/13</td>
<td>$500</td>
<td>$510</td>
<td>$541.3</td>
<td>$31.5</td>
<td>$90.0</td>
<td>18.7%</td>
<td>$149.1</td>
<td>23.5%</td>
<td>149.1</td>
<td>144.9</td>
<td>2.9%</td>
</tr>
</tbody>
</table>

In the case fraudster Barry Minkow, founder of ZZZZ Best Carpet Cleaning Company, he used fictitious receivables to present to banks whenever he needed to borrow money. During an interview with the President, Association of Certified Fraud Examiners, Joseph T. Wells, Minkow described his thought process as he committed one dishonest act after another. Minkow described how easy it was for him to use receivables to borrow money from the bank because not only could he show the bank a receivable but also fictitious revenue since the two accounts were offsetting (GAAPquest, 2010). If any of the company's accountants, bankers, or stock analysts had applied the DSR index to ZZZZ, Best Carpet Cleaning Company's 1985 and 1986 financial statement information it would have revealed that its DSR was over 177,622 (Wells, 2001). This DSR index would have been a significant red flag indicating that something about the company's receivables and sales looked unusual.

Apparently, no such analysis occurred as a significant number of sales and receivables were fictitious. In 1982, ZZZZ Best began operations as a legitimate carpet cleaning business. However, as the company became less successful, Barry Minkow used deceit and lies to hide the truth behind the company's lack of success (Akst, 1087). The deceit continued as his company went public in January, 1986 and Minkow lied to auditors, regulators and the public about the true nature of the company's operations (Akst). He said the company's core business had changed from carpet cleaning, (20%) to building registration (80%) thus increasing earnings (Akst). Minko had to create a plausible explanation for the overall rise in earnings, revenue, and profit. In 1984, ZZZZ Best earned $1.3 million, which was generated through its carpet cleaning services. However, by July 1986, the company's sales had grown to $5.4 million (Akst). The restoration business was used as a front to explain the company's strong sales growth and allow Minkow to continue borrowing money (Akst).

The deceit continued as his company went public in January, 1986 and Minkow lied to auditors, regulators and the public about the true nature of the company's operations (Akst). He said the company's core business had changed from carpet cleaning, (20%) to building registration (80%) thus increasing earnings (Akst). Minko had to create a plausible explanation for the overall rise in earnings, revenue, and profit. In 1984, ZZZZ Best earned $1.3 million, which was generated through its carpet cleaning services. However, by July 1986, the company's sales had grown to $5.4 million (Akst). The restoration business was used as a front to explain the company's strong sales growth and allow Minkow to continue borrowing money (Akst).

In 1998 the cash flow to net income ratio of HealthSouth jumped from 1.3 the previous year to 14.95. The next year it dropped somewhat but was still way above average at 9.21. In fact, the subsequent investigation revealed that management had been misclassifying the provision for doubtful accounts by adding to it in rich earnings years and debiting it to increase earnings in flat years (ACFE, 2007).

In 1968, the Z-Score was developed by Edward Altman, Assistant Professor of Finance at New York University. Although the model was initially developed as a way of measuring a company's financial health, it can also be useful when analyzing companies for potential fraud. The Z-Score is limited in scope in that it only applies to manufacturing companies, and cannot be applied across a broad spectrum of organizations. Overall, the model provided a high rate of accuracy. In fact, “In its initial test, the Altman Z-Score was found to be 72% accurate in predicting bankruptcy two years prior to the event. In subsequent tests over 31 years up until 1999, the model was...
found to be 80-90% accurate in predicting bankruptcy one year prior to the event” (The Altman Z-Score, 2011).

The Z-Score calculation for public companies incorporates five individual ratios, which are weighted and combined into one index. The calculation assesses working capital to total assets (T1), retained earnings to total assets (T2), earnings before interest and taxes to total assets (T3), market value of equity to book value of total liabilities (T4) and sales to total assets (T5) (The Altman Z-Score). The Z-Score calculation appears as follows:

\[ M = -0.104 + 0.92^*DSRI + 0.528^*GMI + 0.404^*AQI + 0.892^*SGI + 0.115^*DEPI - 0.172^*SGAI + 4.679^*TATA - 0.327^*LVGI \] (The Beneish M-score, 2011).

M-Score

While the Z-Score can be used as one measure of financial health, other models have been developed to identify companies that might be engaging in earnings manipulation. One such model is the M-Score. The M-Score is a mathematical model developed in 1999 by Messod Daniel Beneish, Professor of Accounting at Kelly School of Business, Indiana University. The model consists of eight individual ratios which are weighted and then combined into one index. The index is then used as a performance measure to evaluate the subject company for potential earnings manipulation. A calculated index that exceeds -2.22 is considered a strong indicator of earnings manipulation. If the index is less than -2.22 the company is not considered to be an earnings manipulator. The individual ratios comprising the index are Days’ Sales in Receivable Index (DSRI), Gross Margin Index (GMI), Asset Quality Index (AQI), Sales Growth Index (SGI), Depreciation Index (DEPI), Sales, General and Administrative Expenses Index (SGAI), Total Accruals to Total Assets Index (TATI) and Leverage Index (LVGI) (The Beneish M-score, 2011; The Trustees of Indiana University, 2014; Jun, 2014; ACFE Like A Laser, 2013). The M-Score calculation appears as follows:

\[ M = -4.84 + 1.2^*T1 + 1.4^*T2 + 3.3^*T3 + 0.6^*T4 + 1.0^*T5 \] (The Altman Z-Score, 2011).

F-Score

The Fraud Score (F-Score) is another model that is used to assess companies for potential fraud. This model is not as popular as the M-Score in the business or academic community, but some consider it useful as an initial filter for predicting fraud. The model was actually created to use as a screening tool to help identify potential companies capable of outperforming the stock market. The F-Score was developed by Joseph Piotroski when he was an Associate Professor of Accounting at the University of Chicago’s School of Business. Piotroski is now an Accounting Professor at Stanford University’s Graduate School of Business (Joseph D. Piotroski, n.d.). The model analyzes nine variables within three categories; (1) Profitability, (2) Leverage, Liquidity and Source of Funds, and (3) Operating Efficiency (Croft, 2011). The highest possible score is nine (Lipton, 2009).

Under the Profitability category the analysis is focused on reviewing the quality of Net Income, Operating Cash Flow, Return on Assets and Quality of Earnings. Generally, the score assigned to variables within the profitability increase if they are positive, or outperform prior year results. For example, the Net Income variable and Operating Cash flow variable only require positive results in the current year to be assigned a score of one whereas, both the Return on Assets and Quality of Earnings variables need to exceed prior year figures to be assigned a score of one. Under the Leverage, Liquidity and Source of Funds category the F-Score model analyzes the extent of decreases in leverage and increases in liquidity from current to prior year. Lower leverage and higher liquidity from prior to current signals a relatively healthier company. Therefore, each of the two variables would be assigned a score of one if current year results outperformed prior year results. This category also assesses the extent of dilution from current to prior year. For this variable, less dilution is better than higher dilution. Therefore, a score of one is assigned to companies that issue no new equity. Under the Operating Efficiency category, the analysis involves reviewing the company’s gross margin and asset turnover. Each one of these metrics are assigned a score of one if the current year performance exceeds the prior year performance. For the overall F-Score Model, under each category, the score assigned to each variable is combined into an overall score (Croft, 2011).

The F-Score model requires direct access to the company’s books and records otherwise it is difficult to use this data analysis to make meaningful assessments about the company’s true financial condition. However, “for publicly-traded companies, you can get access to a company’s publicly-reported financial statements, such as their annual reports or the 10-K statements they file with the United States Securities and Exchange Commission (SEC). And with that
information, you can calculate a company’s ‘fraud score’ or ‘F-Score’, which can provide a pretty good indication of whether or not the people inside the company might be manipulating their accounting.” (A tool for average investors to detect public company accounting fraud, 2012).

Accounting Quality Model
In July 2013, the SEC announced plans to develop an automated data analysis tool to assist in the detection of financial reporting fraud i.e. the Accounting Quality Model (AQM), but it was nicknamed RoboCop by a reporter in a news article printed in The Financial Times newspaper. The AQM tool combines computer automation and data analysis to scan through corporate financial reports filed with the SEC. Since all public companies are now required to submit their financial reports using the eXtensible Business Reporting Language (XBRL) filings format it makes corporate data easier to work with and analyze using the AQM (XBRL.SEC.gov, n.d.).

The AQM tool searches the SEC’s Electronic Data Gathering Retrieval (EDGAR) database to locate financial statements filed by companies. It then analyzes the financial statements for relationship anomalies among the data, either within the company itself, or as compared to its peer group, and flags the company for closer scrutiny by an SEC Examiner. To help determine which companies receive closer attention, and which do not, the AQM tool assigns risk scores to companies based, in part, on its comparison of discretionary and nondiscretionary expense data that appear in the financial reports (A look inside the SEC’s accounting quality model, 2014).

FALSE POSITIVES
The preceding indexes, ratios and models offer focused guidance but no guarantees that observed anomalies are in fact synonymous with fraudulent financial reporting. Identifying the presence of material fraud in financial reporting is more of an art than a science and there is no sure pathway to prevent or detect this type of fraud. The reason for this is because the environment in which companies operate is both volatile and dynamic. While this creates legitimate deviations from normal business operating results, it also provides opportunities to manipulate financial reporting. The peaks and troughs of the U.S. economy distorts business operations which might impact some industries more than others. The adoption of new accounting rules impacts year-over-year changes in financial reporting. SEC regulations change over time, especially in response to major corporate scandals, and these changes impact the quality and quantity of information reported to the public. Finally, there are certain areas in accounting which are subject to management estimates, interpretation and future projected which are subject to either legitimate change or false manipulation. The challenge for the forensic analysis is to differentiate truth from fiction.

To avoid rushing to judgment with respect to the integrity of management’s financial reporting, the forensic analyst must consider the totality of circumstances when evaluating changes in the results of key indexes, ratios or models. When assessing the probability of fraud, company specific information included in financial reports should not be evaluated in isolation. External information, such as overall industry growth, should be incorporated in the analysis to help distinguish industry anomalies from company anomalies.

USING COMPUTER TECHNOLOGY AND AUTOMATION
There are dozens of tools available to assist individuals in performing data analysis. Some of these tools range from basic software programs such as Microsoft Access and Excel, to more advanced programs such as Audit Command Language (ACL), IDEA, and Monarch. Regardless of the program selected, introducing automation into a data analysis routine can enhance accuracy, efficiency, timeliness and completeness. Many auditors use technology to review one hundred percent of a transaction file. This allows conclusions to be reached quickly and with greater confidence. Computer technology also allows forensic accountants to create scripts, a set of predefined automated procedures. The scripts are then applied in a consistent manner to data files, when analyzing quarterly and annual financial reporting data. Ideally, scripts should be designed to assist in the periodic review of key metrics that point to anomalies in financial reports. These exception reports are designed to alert the forensic accountant or data analyst of potential problems which may require a more focused review.

Computer technology can also be used to analyze non-financial data such as the text in financial statement footnotes or management discussions and analysis. Some fraud experts believe that analyzing words can be an effective way of identifying deception on the part of management. In fact, on April 25, 2011, the SEC posted a request for information (RFI) on its Federal Business Opportunities website, seeking information about text mining software that it could use to potentially predict financial statement fraud. A partial excerpt of the request reads:

“The U.S. Securities & Exchange Commission (SEC) seeks information about data and text mining software applications that assess the probability of financial statement fraud occurring at a given public company. Such application should utilize textual analysis to identify such things as word patterns and frequency of usage that may be correlated with financial fraud...” (SEC seeks information on data and text mining software applications to analyze financial statements, 2011).

Although text mining is still relatively new and evolving, computer programs such as RapidMiner and StatSoft allow text mining to be performed with relative ease.
WORD OF CAUTION

Fraud is hidden and red flags are usually not obvious to the casual observer. Even professionals whose job it is to sift through financial data every day sometimes overlook critical anomalies. One of the most infamous examples of this is the SEC’s mishandling of the tips provided by Harry Markopolos in the Madoff Ponzi Scheme. Unfortunately, mistakes like this allow small frauds to grow into massive frauds until eventually uncovered years later. By this time the financial loss sustained is more difficult to recover. Although the Madoff scenario is an extreme case of failure, the reality is that many cases are not obvious examples of fraudulent activities. The reason is that some businesses and industries are more complicated than others and many accounting rules provide room for judgment and estimates. Using Data Analysis cannot replace individual judgment and expertise.

A Washington Post article that discusses recent legal defeats suffered by the SEC shows that, despite using its Robocup tool to bring actions against companies for fraud, more persuasive evidence was required by the SEC to support allegations of actual financial reporting fraud. The article illustrates why data analysis must be used in conjunction with professional judgment and expertise; especially when developing cases for trial. According to the article, in December 2014:

“the SEC suffered a jury trial defeat in SEC v. Kovzan, a civil fraud action alleging that the CFO of NIC Inc. failed to disclose more than $1 million in perquisites to the company’s former CEO. The SEC alleged that the CFO knew or was reckless in not knowing that the perquisites were not disclosed accurately. Not only did the Kansas jury acquit the CFO on all 12 charges, they found in his favor on every question on the jury verdict form” (Morgan, Nicolas, & Jennifer Feldman, 2014).

The article continues by explaining that this SEC defeat:

“was followed by another adverse ruling in December, in SEC v. Jensen. In that case, the SEC charged two former executives of Basin Water Inc. with accounting fraud for improperly recognizing revenue for six transactions, purportedly to disguise the company’s financial performance. The judge found that the SEC failed to demonstrate fraud, as there were no documents or witnesses to support the allegation that these transactions were shams. Further, the judge found there was no direct evidence of scienter or recklessness. While the SEC’s case was premised on allegations of improper accounting, the only evidence of such improprieties was unconvincing witness testimony, according to the court” (Morgan, Nicolas, & Jennifer Feldman, 2014).

As the article implies, direct evidence is stronger than circumstantial evidence and data analysis is circumstantial at best; assuming the court would consider it evidence at all. Data analysis alone cannot conclusively prove who did it, what was done, when it was done, why it was done and whether alleged fraudster’s actions were accidental or intentional.

TRAINING

Organizations strive for success in fighting fraud must be proactive: anticipate financial results, and then measure actual results against those anticipated results. The right combination of training, education and skills will improve the odds that red flags are detected in a timely manner so as to identify fraud during its early stages. However, caution must be exercised when leveling accusations of fraud, because the determination that fraud is present is a legal and factual distinction involving specific elements that must be proven in a court of law. Conclusions reached should be supported by extensive analysis and investigative work. Making premature conclusions or direct accusations of fraud against persons or organizations, whether verbal or written, should be strictly avoided by forensic analyst.

CONCLUSION

The temptation to engage in financial reporting fraud is unlikely to go away any time soon. Strong internal controls, pervasive ethics training and increased regulatory scrutiny are all important considerations that help manage the risk of financial reporting fraud. However, in order to stay two steps ahead of the fraudsters, old methods of fighting fraud must be constantly refined and replaced with new innovative techniques. Without question, data analysis is reliable, but fraud is so complicated that no full proof method exists capable of predicting it on a consistent basis. Any fraud detection method requires the application of judgment, experience and specialized knowledge in order to truly be effective.

REFERENCES


Association of Certified Fraud Examiners. (2007). How to detect and prevent financial statement fraud (2nd ed.). Austin, TX: ACFE.


Morgan, Nicolas, and Jennifer Feldman. (2014, January 2) “No More Mr. Nice Guys:


JOSEPH HARRIS

Mr. Harris has worked as an Internal Auditor for the past 14 years. He is currently a Senior Internal Auditor at ePlus, inc. (Herndon, VA). Joe has extensive experience performing financial, operational, compliance, and Sarbanes-Oxley (SOX) audits, in a variety of industries. He is currently pursuing a Master’s degree in Forensic Accounting at Stevenson University. Mr. Harris completed his undergraduate work at William Paterson College (Wayne, NJ), where he received a B.S., in Accounting. He also holds Certified Internal Auditor (CIA) and Certified Fraud Examiner (CFE) designations.
Medicaid and Medicare Fraud, Waste and Abuse
Lindsay M. Wheatley

The Medicaid and Medicare programs were initially created as part of President Lyndon B. Johnson and the 89th United States Congress's passage of the Social Security Act of 1965 (Stevens & Stevens, 2003, p. 48). The non-partisan Congressional Budget Office approximates that federal spending for healthcare totals nearly $1 trillion each year, thus representing one of the single largest federal budget expenditures (Smith, Gifford, & Meyer, 2013, p. 1). Individually, Medicaid expenditures totaled $428 billion in fiscal year 2011, with Medicare expenditures reaching $565 billion within the same time period (Government Accountability Office, 2012, p. 1). Before the Affordable Care Act of 2010, an average of 52 million senior citizens and permanently disabled adults received Medicare-related healthcare coverage. 60 million needy citizens received Medicaid benefits, and about 9 million citizens received benefits from both programs (Wilson, Dilulio, & Bose, 2013, p. 524).

While various types of healthcare, food and other essential-needs welfare programs existed before Medicare and Medicaid were created, the programs together have grown to encompass the care of a very large portion of U.S. citizens and are funded with trillions of tax payer dollars. Within this wide-reaching coverage and flux of large sums of money lies the potential for fraudulent, wasteful or abusive appropriations of program money. This ill- or mis-intentioned diversion of program funding can occur at the hands of numerous individuals and organizations including beneficiaries, providers, hospitals, clinics, surgical centers, dental offices, nursing homes, pharmaceutical companies, laboratory operations, hospice and palliative care facilities, and various other entities. Over time this inadvertent or purposeful fraud, waste and abuse siphons off huge sums of taxpayer monies intended for the healthcare of those truly needy, aged or disadvantaged individuals. While the true total of all program fraud, waste and abuse is unknown, estimates indicate that it could be 20% or greater of total Medicare and Medicaid expenditures (Berwick & Hackbarth, 2012, p. 1).

Compounded in many ways by the structure and inconsistencies of Federal and state policy, efforts against program waste also depend upon this legislation to provide detection, prevention and education tools. While Medicaid and Medicare fraud, waste and abuse seem like the most egregious of program exploitations, incidental and accidental waste also affects funds appropriation. Complexity of the programs and their ever-changing policies on both the Federal and state levels contribute to huge sums of misdirected program monies. As state program policy varies, so does state program spending. States such as Maine, West Virginia and Mississippi, for example, spend one of every five dollars of state gross domestic product on healthcare while Wyoming spends less than 9 percent on average (Saving & Goodman, 2013). The percentage that states contribute to the initial federal funding of Medicaid and Medicare programs also varies.

These regulation intricacies and inconsistent standards weaken program efficiencies and create opportunities for beneficiaries, providers and national healthcare as a whole to waste significant amounts of money. Funds are squandered on unneeded, unwanted, accidental, incorrectly billed, miscoded and misunderstood services and care. In 2010 alone Medicare expended $48 billion dollars in improper payments comprised of coding errors, calculation mistakes and other non-fraudulent service and billing issues (Gibson & Singh, 2013, p. 55).

Today, policy and regulation focus on creating and funding programs tasked with discovering these intentional and accidental misuses of program dollars. Not only is the healthcare community held to a higher standard of program integrity compliance, they are also more frequently policed by programs, requirements and structures that are designed to detect their fraudulent or wasteful behavior.

While these detection efforts are responsible for recouping large amounts of fraudulent and improper dollars for return to the state and Federal programs, new fraud schemes and habitual improper payment patterns are created each year. The Centers for Medicaid and Medicare Services (CMS) has devoted resources i.e. Fraud Prevention System to help counteract these new schemes and patterns, but the approach to combating program fraud, waste and abuse remains reactive in nature (Salinger, 2013, p. 429). The future of program integrity efforts lies in developing more comprehensive tools and perfecting those already in use to predict and prevent fraud, waste and abuse before it occurs.

MEDICAID AND MEDICARE: A BRIEF HISTORY

Before the Medicare and Medicaid programs were created, states developed various assistance plans for similar groups of people: the aged, disabled and underfed children. Before the 1930s, this type of assistance was assumed by local towns and communities and was postured more as charity relief than entitled aid. By 1934, 28 states passed laws that, while rudimentary, provided assistance to the aged, disabled and underfed. With the Social Security Act of 1935 national legislated government aid for citizens unable to work, feed and care for themselves became law (Stevens & Stevens, 2003, p. 6).

Although assistance programs did exist before the Social Security Act of 1965, there were still large numbers of people excluded from, but in need of those benefits. Generally, Medicare was designed to finance healthcare services for the elderly who were ineligible for previously offered assistance. At the onset, it was thought Medicare would blanket most of the neediest of the U.S. population, and that Medicaid would be the safety net for those individuals not eligible for Medicare but in need of assistance (Marmor & Marmor, 1973, p. 24).

Today, Medicaid enrollment numbers surpass those of Medicare by approximately 13 million recipients (Meyer, 2013, p. 2).
Medicare was considered a continuation of previous assistance programs but Medicaid was a new aid concept, thus states were given until December 1969 to develop a plan outlining how they would provide the services and meet the Medicaid program financial and policy requirements. While several states initially rebuffed their forced participation in the Medicaid and Medicare programs, by 1970 all states except Alaska and Arizona implemented the programs. The Medicaid program created the most trepidation for states, especially those with high unemployment rates, because of the perceived burden of funding healthcare for so many more individuals than were originally aided prior to the programs’ passage. When Alaska failed to develop a plan and implement the Medicaid program, the state argued that because virtually all indigenous Eskimos and Indians would be eligible under program eligibility requirements, the potential costs to their state would be unbearably high (R. Stevens, 2007, p. 124).

Not only did Medicaid expand eligibility requirements to cover even more citizens, the program expanded services to cover a minimum of five different types: laboratory and X-ray, skilled home nursing, outpatient hospital, inpatient hospital and physician. States were also given the freedom to cover additional services for Medicaid recipients including dental, private nursing, home health and other types of care. While the standard categories of Medicaid-eligible recipients included needy women and children and disabled adults, the policy also offered provisions for those, “noncategorically [sic] related medically needy,” individuals to receive Medicaid services if the state so chose (R. Stevens, 2007, p. 124).

Throughout the years, Medicaid has experienced significant changes due to state reaction to the additional financial burden created by so many additional eligible citizens. As a result, policy related to eligibility requirements has undergone several transformations to include and/or exclude various groups of “needy” individuals. The first Congressional expansion of Medicaid occurred in 1972 with the next occurring in the early 1980s. The 1981 and 1982 program expansions extended Medicaid eligibility from solely covering institutionalized disabled children to covering those receiving at-home care as well. This expansion and another offering eligibility to pregnant women for prenatal care quickly caused program costs to surge even higher than the already-underestimated expectations. As an example, during its first full year of operation, The Department of Health, Education, and Welfare estimated that the Medicaid program would cost the Federal Government an additional $238 million. In 1966, the Federal share of vendor payments totaled exactly that amount, however, only six states were operating Medicaid programs at the time (Gilman, 1998, p. 22).

With state and Federal Medicaid and Medicare expenditures on the rise, even more money was being paid to various service providers within the healthcare community. This influx of money combined with ever-expanding and changing eligibility requirements helped create an environment from which fraudulent and improper program claims began to emerge. Concurrently, policies regulating these providers and claims also underwent many changes and fund exploitation firmly established itself as a bane to the aid and assistance offered by the programs.

**FRAUD SCHEMES**

Abuses of the Medicaid and Medicare programs exist in myriad shapes and sizes and continue to evolve each fiscal year. While Medicaid and Medicare fraud, waste and abuse appear to be the most egregious program issues, incidental and accidental waste also threaten program integrity, similar to outright criminal exploitation of expenditures. Altogether, these overpayments of Medicaid and Medicare dollars represent the largest portion of misused government money, accounting for 59 percent of the $102.2 billion government improperly distributed among all agencies in 2013 (Davis, n.d., p. 1). These exorbitantly expensive improper payment issues can be attributed, in part, to the complexities of the programs and their ever-changing policies among states.

While Medicaid and Medicare are considered universal programs, each state is able to operate its own version of the healthcare programs autonomously and independent of any collective standard. This autonomy creates wide-ranging policy inconsistencies due to the differences among states, which in many ways also parallels the ideals of American federalism (Patel & Rushefsky, 2014, p. 108). How states administer programs like Medicaid and Medicare is largely influenced by the type of bureaucratic style employed by the state legislature (Sparer, 1996, p. 67). These variations and inconsistencies can facilitate inaccuracies and misunderstandings in every aspect of both programs, from recipient eligibility, billing protocols, coding standards and licensure requirements. Doctors offering Medicaid or Medicare services are not easily able to transfer their practices from one state to another without first exploring expectations and requirements of the new state. These hard state boundaries create the potential for provider, beneficiary and administrative confusion, which ultimately equates to billions of program dollars misappropriated each year.

Beyond the innocent misappropriation of program dollars are the much more incendiary and egregious problems with the Medicaid and Medicare programs occurring in the form of illicit and purposeful fraud, waste and abuse by individuals, providers and larger healthcare establishments. Medicaid and Medicare identity theft, much like general identify theft, has continually resurfaced as a bane since the programs’ inception. It is estimated that three percent of $50 billion of the nation’s annual identity theft losses is associated with some type of medical identity theft. Because of their propensity to being enrolled in government-facilitated insurance programs like Medicare
or Medicaid, individuals aged 50 or older are most likely to fall victim to this type of identity theft (Salinger, 2013, p. 452). Fraudsters steal these identities to access services, such as prescriptions for drugs with high black-market value i.e. OxyContin, Fentanyl and Morphine intended for legally enrolled, authorized recipients. Once the prescription is obtained, the thieves sell the drugs for cash or abuse them.

A similar identity theft scheme infiltrates the sale of durable medical equipment prescribed to recipients. By stealing a beneficiary’s Medicaid or Medicare number, the perpetrator can place orders for equipment i.e. slings or braces, all paid for through program dollars, and re-sell online or via newspaper classifieds for cash. In January of 2012, a former owner of a Texas medical supply company was indicted on charges of conspiracy to commit healthcare fraud for her participation in a nearly $10 million Medicare scam related to fraudulent bills submitted to the program for various medical supplies (KWXT RSS, 2014). Additionally, those individuals attempting to defraud the programs through medical identity theft may use a beneficiary’s information to bill for healthcare services or goods that were not actually provided or received in order to collect cash pay-outs (Beik, 2011, p. 139). Medicaid and Medicare provider identifiers can also be stolen or misused to fraudulently bill the programs. In 2012, a nurse employed by a Medicaid provider in the state of Iowa was indicted by a Federal grand jury for healthcare fraud and money laundering. A Department of Justice investigation found that the nurse coordinated a fraudulent billing scheme that billed Medicaid in conjunction with three other private insurance companies more than 6,000 times for services using the names and national provider identification numbers of various doctors who did not work for the center. Altogether, this fraudulent billing scheme generated $1 million in fictitious bills to Medicaid (Ocker, 2014). Physicians participating in the Medicaid and Medicare programs also have access to a wide range of possible fraud, waste and abuse schemes. Double billing is a common provider fraud scheme that involves the submission of duplicate claims to Medicaid or Medicare in an attempt to receive double the amount of payment for services that were only provided once (Olson, 2010, p. 17). Those physicians wise to the high detectability of billing duplicate claims to either program via simple data analysis will also often send one bill to a private insurance company and a duplicate bill to Medicaid or Medicare so that the duplication does not appear within one data set (Sells, 2000, p. 423).

Other fraud schemes include upcoding bills to Medicare or Medicaid to represent more complex, lengthy or in-depth procedures when a simpler or lower-level service was actually provided or performed. Usually, complex procedures are paid at a higher dollar amount than their simpler counterparts, which leads providers to be paid more money than what they actually earned during the office visit or procedure. This fraud scheme takes advantage of small but specific variations in the current procedural terminology (CPT) coding system standardized for both Medicaid and Medicare coverage (Leap, 2011, p. 71). In September 2014, a Nevada Medicaid provider pleaded guilty and was sentenced to 200 days in jail and 100 hours of community service for submitting false documentation for reimbursement of services provided to Medicaid mental health recipients. During the nine month fraudulent billing cycle, the Medicaid provider padded medical documentation to represent more hours than were actually worked, totaling approximately $7,500 in overpayments (Bowers, 2014). Similar to upcoding is the fraudulent unbundling of CPT codes billed as individual entities that per regulation should be grouped together and billed under one umbrella code. Usually, the umbrella code pays a discounted rate for all the services combined. Each individual code gets paid an amount that, when totaled together, equal more than what the umbrella code pays (Leap, 2011, p. 73). Dishonest Medicaid and Medicare providers also bill for services that are not medically necessary. In this scheme, providers perform and bill for services and/or testing beyond what patient needs require. Under this scheme, hospital stays are lengthened, additional diagnostic testing is ordered, entitled hospice enrollment is invoked too early, and equipment and tools are wasted for beneficiaries who really require less care and fewer services. This fraud scheme not only wastes program dollars but also strains other areas of the general healthcare system by introducing and allowing individuals to linger thus monopolizing unnecessary services and care that could be better applied to other more needy beneficiaries. In September of 2014, a California woman was found guilty of conspiracy to commit healthcare fraud after an investigation revealed she fraudulently billed more than $7 million to Medicare for medically unnecessary power wheelchairs for program beneficiaries who were reportedly often recruited from the street. Altogether, four other employees of her company, Adelco Medical Distributors Inc., were convicted of healthcare fraud crimes related to this fraud scheme (City News Service, 2014). While Federal regulation does not contain a definition of medical necessity, states are granted authority to develop and apply medical necessity criteria as they see fit (Rosenbaum, Silver, & Wehr, 1997, p. 15). Providing and billing for services beyond the needs required of the beneficiary may be intentional and fraudulent, but because of differing state criteria, instances where unnecessary services are provided and billed may also be accidental or well-intentioned. Medical identity theft, double billing, upcoding, unbundling and billing for services not medically necessary represent only a portion of the known problems and schemes that weaken the Medicaid and Medicare programs. There are many other types of program fraud, waste and abuse occurring on a daily basis that have yet to be discovered. In the past 27 years the Federal government has recovered approximately $24 billion in settlements or judgments.
against individuals and organizations who committed both accidental and purposeful healthcare fraud, waste and abuse (Meyer, 2013, p. 2). On a state level, another $15 billion has been recouped from criminal fines and civil settlements resulting from the prosecution of healthcare fraudsters.

While the $39 billion in recovered overpayments from the last 27 years is only enough to cover a small percentage of one year’s program costs, the amount of overpayment dollars recovered each year by the Federal and state governments is growing exponentially. On average only about $1.4 billion in overpayments was recovered during that time period. However, in 2012 alone, $3.1 billion in healthcare fraud judgments and settlements was recovered by the Federal government (Meyer, 2013, p. 3). As Medicaid and Medicare fraud, waste and abuse schemes and problems become more prevalent and their financial toll increases, Federal and state governments are also detecting and reclaiming money back on a larger scale. This increase can be attributed to developments in policy created to prevent and identify fraud, increased investigative and program integrity funding, and technological improvements to fraud detection programs, databases and software.

PROGRAM INTEGRITY

Because U.S. healthcare expenditures comprise such a large portion of the country’s budget, the wasteful and fraudulent squandering of those funds has captured the attention of the media, public and legislative bodies, particularly in regard to the Medicaid and Medicare programs. Since their inception, congressional and state legislative bodies and representatives are consistently tasked fighting such program waste. In their answer to this ever-present problem, lawmakers, politicians and Federal and state governments have created and enacted volumes of policy and regulation to squelch program abuse and create solutions for fraud and waste detection and mitigation. Trends in these policies and regulations have ebbed and flowed as changes in the healthcare industry and the country’s economic posture influenced public and political perceptions of Medicaid and Medicare and the healthcare environment as a whole.

Prior to the 1970s, Federal healthcare policy was shaped by three assumptions: the healthcare system did not possess enough care facilities and services; major financial barriers stood between many needy individuals and the few resources that did exist; and the healthcare industry could not find success in competitive markets and regulatory strategies (Patel & Rushefsky, 2014, p. 37). These assumptions proved faulty as the market soon became saturated while testing and treatment trends grew excessively due to the unconstrained supply of hospitals and physicians, resulting in increased healthcare costs. The 1970 loan guarantee expansion of the Hospital Survey and Construction Act of 1946, known as the Hill-Burton program, encouraged new not-for-profit government-run hospital growth, creating a surplus of care facilities (U.S. Congress, 2001, p. 119). Simultaneously, the creation of the Medicaid and Medicare programs helped break down many pre-1965 financial barriers to healthcare while participating care providers were deliberately and generously reimbursed by the Federal government to garner political support of the programs. These factors contributed to the near tripling of national healthcare expenditures, from $27.1 billion in 1960, to $74.3 billion in 1970 (Patel & Rushefsky, 2014, p. 37).

Almost immediately, the rampant and widespread fraud and abuse within both programs became obvious. Public hearings held in the mid-1970s represented a growing disdain for the programs because of the waste and abuse associated with funding and expenditures. It was at these hearings that the pervasive practice of kickback payments within the healthcare industry – especially in the Medicaid and Medicare programs – was first exposed on a national level (Teplitzky & Holden, 1990, p. 788). Kickbacks had a long-standing presence before the creation of Medicare and Medicaid and were often referred to as fee splitting or commission drumming. Their existence was not limited to the healthcare field, but appeared throughout various other professions, including the funeral home industry whose undertakers would sometimes pay out commissions to physicians who referred their post-life services to families of the recently deceased. Before Medicaid and Medicare were created, kickbacks were shunned mainly because they created a black market of sorts where a patient’s needs were exploited and over-served by the auctioning off of their referral by their primary doctor to the highest bidding surgeon, physician, pharmacist or medical supplier for next-level care. These exacerbated healthcare costs for services that were often not needed were mostly paid out of pocket, however, so only the patient’s checkbook was affected (Rodwin, 1993, p. 22). With the creation of Medicaid and Medicare, kickbacks no longer targeted the beneficiary’s money to pay for the unneeded or excessive referred services but taxpayer dollars were appropriated instead.

As a result of the outrage and growing waste due to unethical kickbacks, Congress passed the Medicare and Medicaid Anti-Fraud and Abuse Amendments of 1977. The amendments offered several updates to previous anti-kickback provisions, including the upgrade of criminal charges for such offenses to the programs from misdemeanors to felony indictments. The new amendments also required individuals to disclose ownership or control of healthcare entities in an effort to curb conflicts of interest. More substantial than the anti-kickback amendments was the creation of the Office of the Inspector General (OIG) of the Department of Health and Human Services (HHS) via legislation in 1976. Prior to the creation of HHS OIG, the Federal Bureau of Investigation and United States Postal Service were primarily tasked with any investigation of violations against Medicaid or Medicare antifraud abuse statues. While the OIG is also tasked with other responsibilities including the oversight,
supervision, auditing and security maintenance of other departments and programs, their primary responsibility lies with overseeing and monitoring the Medicaid and Medicare programs and policing any associated internal or external fraud, waste and abuse (Teplitzky & Holden, 1990, p. 789).

Within the decade after the creation of HHS and OIG and the passage of anti-kickback updates, very few kickback-related cases were prosecuted by the Federal government because any instances other than the most classic or egregious models of kickbacks were difficult to prove and the Federal government was stretched thin over other priorities. Due to this absence of successful prosecution and conviction, kickbacks remained a firm presence within the Medicaid and Medicare programs. It wasn’t until 1989 when a stricter regulatory climate combined with OIG’s issuance of a heightened fraud alert that providers became more conservative with their use and involvement in kickback schemes (Rodwin, 1993, p. 121).

While the anti-kickback updates were less than successful at curbing any worthwhile amount of program waste and abuse, other legislation and regulations have been better situated to address past and present issues with the programs and continue to evolve present-day. Both the civil False Claims Act (FCA) and the Health Insurance Portability and Accountability Act (HIPAA) are older pieces of legislation that continue to undergo newer interpretations and development to bring them into modern-day healthcare fraud combat. The FCA was first enacted in 1863 after President Abraham Lincoln urged Congress to create a solution to deter individuals from fraudulently billing the U.S. government for supplies during the Civil War (Truelson, 2001, p. 414). Today, the FCA is most known for its qui tam provision that allows individuals to serve as whistleblowers – on behalf of the government – who bring to light acts of fraud against the government. Within 15 years of several 1986 amendments to the FCA that updated protections for whistleblowers, $1.8 billion was recovered by the U.S. Treasury due to whistleblowers (2001, p. 407). The largest ever whistleblower recovery of Federal dollars came after a small, independent pharmacy in Florida notified officials of over $2.2 billion Medicaid and Medicare dollars spent on drugs with artificially inflated purchase prices sold by a group of pharmaceutical manufacturers. A portion of the money recovered was awarded to the Florida pharmacy responsible for bringing the inflated reimbursement scheme to the attention of the government (Rollins & Petri, 2014, p. 173). What makes the policy so effective at detecting fraud is the whistleblower’s right to a percentage of the money recovered thus incentivizing whistleblowers to alert authorities on potential fraud schemes they have discovered.

In 1996, Title 11 of the Social Security Act was expanded by the enactment of HIPAA to include requirements and standards for the electronic transmission and dissemination of health information. HIPAA language was crafted to improve upon the efficiency and effectiveness of healthcare systems while simultaneously reducing fraud and waste within healthcare by making it easier to detect. The ultimate goal was to protect the sensitive nature of healthcare documentation while reducing administrative costs and wasted expenditures (Chaikind, 2004, p. 3). One of HIPAA’s most well-known functions is its Health Care Fraud and Abuse Control (HCFAC) program, which apportions money to fund HHS, Department of Justice (DOJ) and OIG healthcare fraud research, detection and mitigation. Money recovered from health care fraud cases funds the HCFAC program and the multi-agency participation helps facilitate multi-directional and strength-in-numbers approaches to combating healthcare fraud. In its first year alone, the HCFAC program was earmarked to receive approximately $65 million in fraud recovery monies. Even larger than the HCFAC program was HIPAA’s establishment of the Medicare Integrity Program that allocates funds and grants authority to CMS to contract with private entities to perform financial audits and medical reviews as well as provide regulation and policy education to healthcare providers participating in the Medicare program. In its first year, the Medicare Integrity Program was earmarked to receive approximately $450 million to operate (Swendimen & O’Sullivan, 2002, p. 95).

The Medicare Integrity Program is one of several entities to use both government and privately contracted resources to increase Medicaid and Medicare provider oversight and compliance. Similar to Medicare Integrity contractors are Recovery Audit Contractors (RACs) who are hired and provided with Medicare provider and beneficiary data from the government to mine for potential paid claims errors. The contractors utilize algorithms to detect potential errors or fraud and are then paid a percentage of the money they recover from providers. The RAC program was mandated in 2003 as part of the Medicare Prescription Drug, Improvement, and Modernization Act. When the RAC program was created, Medicare was processing over 1.2 billion annual claims submitted by over one million healthcare providers (Green & Rowell, 2006, p. 119). Zone Program Integrity Contractors work with the government to obtain claims data associated with Medicare providers who submit more claims or bill at a higher rate than most other Medicare providers within their community or area. The contractors also explore Medicare drug claims for potential overpayment, fraudulent activity or drug diversion schemes. A similar program exists to measure improper payments within the Medicare fee-for-service program that uses calculated error rates to identify billing areas the OIG may want to target and explore (Fordney & French, 2002, p. 44).

While Medicare received the most fraud prevention attention from government regulation and legislation prior to the 2000s, fast-growing Medicaid fraud, waste and abuse resulted in concentrated action. Because the Federal government was typically paying for a larger portion of Medicaid expenses than individual states and
due to the rampant uptick in Medicaid fraud far surpassing other types of federally-funded waste, it was imperative for legislators to create solutions similar to those designed for Medicare (Secunda, 2009, p. 495). In 2005, Congress enacted the Deficit Reduction Act (DRA) which, in part, mandated the creation of the Medicaid Integrity Program. Very similar to the Medicare Integrity Program, the Medicaid Integrity Program granted CMS the authority to contract with private entities to combat Medicaid fraud, waste and abuse through claims review, audits, overpayment determinations, and provider education regarding program integrity and care quality standards.

At its creation and to date, the Medicaid Integrity Program operates on several foundational principles. To successfully combat Medicaid fraud, program partners, called Medicaid Integrity Contractors (MICs) must be accountable for their fraud, waste and abuse discovery operations while maintaining ongoing collaborations with other internal and external partners and stakeholders to include: Federal contacts, State Medicaid programs and the mining entities responsible for providing the contract with pertinent provider and beneficiary data. MICs must also have access to national leadership associated with program integrity, such as HHS, OIG, DOJ and CMS, and must be flexible to accommodate the ever-changing healthcare arena and to combat continuously evolving Medicaid fraud, waste and abuse (Green & Rowell, 2006, p. 119).

While state Medicare and Medicaid policy and regulation varies widely across the country, one standard for all states exists: responsibility to report their program data and statistics to the State and Federal programs. This information details the number of state program recipients, each beneficiary’s demographic information, detailed accounts of the services received, and services billed to and paid by Medicaid or Medicare. Essentially, if a beneficiary receives even one dollar of Medicaid or Medicare services in the form of prescription drugs, hospital or doctor visits or durable medical equipment, every aspect of that service is recorded by the provider and given to the state. This information includes the dates of service, what types of services were provided, the doctor who provided the services, any codes the doctor used to bill the services, the amount the doctor or facility billed to the program and the amount the program paid back to the provider for their services. This information is then converted into complex data sheets collected and stored by the states and shared with the Federal government. Both the states and the Federal government relay this information to Medicaid or Medicare Program Integrity partners (Thompson & Dilullo, 1998, p. 288).

Under the direction of the Medicaid Integrity Program are three types of MICs review, audit, and education, each with a distinct role within the program. The MICs also simultaneously rely on the other entities for necessary operational support. Review MICs work with the large sets of claims data provided by states and the Federal government to identify and analyze areas where fraud has or potentially will occur. When target areas of claims with potential or probable fraud, waste and abuse are discovered, Audit MICs are responsible for auditing and reviewing the medical and financial documentation and information associated with the claims. They report their findings, including any overpayments, and refer fraud cases to the OIG. Education MICs are tasked with summarizing the fraud, waste or abuse issues determined by the Review and Audit MICs to educate Medicaid program participants i.e. providers, medical supply companies, hospitals and pharmacies regarding payment, program integrity and care quality issues, expectations and requirements (Belk, 2011, p. 126).

Since their enactment, HCFAC and the DRA have successfully recovered and saved the Federal government large amounts of program monies. Approximately $1.50 is saved or recovered for every $1 spent on fraud and waste detection, control and prevention efforts. As more money is saved or recovered, more money is available for redistribution to programs i.e. the Medicaid and Medicare Integrity Contracts to combat fraud, waste and abuse (Executive Office, 2014, p. 118). However, Medicaid costs are expected to grow an average rate of 6 percent annually for the next several years and will balloon much larger after the Affordable Health Care Act expands population enrollments (Bowman & Kearney, 1990, p. 475). If the cost of Medicaid program integrity efforts remains as is, coupled with projected increases in fraudulent spending, states and the Federal government will experience an even greater financial burden. While this reactive approach to discovering past Medicaid and Medicare fraud, waste and abuse has undoubtedly recovered and saved Federal and state governments large and valuable amounts of program dollars, only preventative solutions can provide the type of fiscal stability needed for these programs.

**CONCLUSION: THE FUTURE OF PROGRAM INTEGRITY**

Not all potential fraud can be conceived and prevented before motivated criminals find ways to infiltrate and exploit the system, so data analysis of past fraud can be helpful in identifying those areas most susceptible to future abuse. Reactive policy creation does have advantages because, “with reactive policy, one gets the benefit of observing the policy issues over time, and vetting the policy concerns, before making changes,” similar to retrospective fraud identification (Fiore, 2014, p. 1). However, predictive and preventative solutions do have the ability to view fraud, waste and abuse as outdated and exceptional characteristics of the Medicaid and Medicare programs rather than the norm.

A first step in bolstering fraud prevention is to make it harder for those with a propensity or history of committing fraud or creating or participating in deceitful financial schemes to obtain access to the Medicaid and Medicare programs. Currently, CMS utilizes the National Supplier Clearinghouse (NSC) to vet various types of
providers and facilities desiring operational identification numbers and legitimacy needed to bill services to the programs. The NSC collects data from application forms and uses it to perform various types of information verification for individuals or entities seeking provider status (Rozovsky, 1998, p. 211). The process is generally administrative and while it does utilize databases to corroborate provided documentation, a more investigative approach would yield more refined and verifiable results. Checks spanning financial, judicial, licensure, partnership, educational and residential levels would expose any existing areas susceptible or potentially susceptible to fraud, waste or abuse. Full business, billing and payment plans and models as well as planned internal controls submitted by the potential provider could reveal essential administrative flaws or weaknesses that could attract fraudulent or wasteful billing of the programs.

In recognition of prior industry weaknesses, a main focus of the AHA of 2010 was increased transparency and accountability among providers and payers, while pre-existing public healthcare entities such as the Medicaid and Medicare programs could greatly benefit from similar updates (Cimasi, 2014, p. 664). Within the past decade, hospitals and other healthcare facilities have adapted similar transparency efforts in response to lowered patient satisfaction reports. By updating business models to allow readily available and easy to understand dissemination of accurate and up-to-date wait and referral times, care costs, available services, and concise and time-effective care plans, these facilities reported improved patient satisfaction equating to not only higher revenue, but larger profits sustained over time (M. Stevens, 2007, p. 5). Utilizing a similar transparency strategy with the publicly-funded sector of Medicaid and Medicare services and provider membership would not only help protect against fraud but would strengthen beneficiary care and the healthcare industry as a whole.

While raising the standard for participating providers and increasing program transparency, a rigorous pursuit of ongoing Medicaid and Medicare fraud, waste and abuse should engage simultaneously on the largest and most public scale seen by the programs to date. Although HHS, OIG, DOJ and CMS do collaborate to exchange information and resources pertinent to program integrity, a partnership bolstered by additional funding and reenergized by open and purposeful communication between entities would send a very powerful message of zero tolerance. Ongoing audit and recovery efforts would be strengthened and expedited and the recouped expenditures would be reinvested into the expanded detection effort at a faster and larger rate. State legislature and Medicaid and Medicare programs would also play a vital role in working to prevent future expenditure exploitation by making commitments to solidify the areas of program policy that are weak or susceptible to fraud and/or unclear or contradictory regarding policy and regulation expectations. Since their inception, the Medicaid and Medicare programs have been susceptible to cyclical and systematic fraud, waste and abuse due in large part to policy and regulation weaknesses, gaps, ambiguity and lack of transparency. Some of the very issues the programs were created to address are the reasons program costs and the exorbitant waste of remunerate funding continue to expand and over-burden Federal and state treasuries, budgets and taxpayer responsibilities.

While current program integrity efforts work to reactively police the inadvertent and purposeful deficiencies and exploitations of the publicly-funded healthcare system, new proactive and unified approaches are needed to end the consistent leaching of taxpayer monies intended for the healthcare necessities of aged, disabled and disadvantaged citizens. Transparency, committed amalgamation of resources, and state and Federal dedication to policy and regulation clarity and consistency will enable the Medicaid and Medicare programs to successfully fulfill the needs for which they were originally created long into the future.

REFERENCES


Fiore, M. (2014, August 21). Deputy Program Director, Health Integrity, LLC – LMW. [Personal interview by the author].


**LINDSAY WHEATLEY**

Ms. Wheatley is a graduate of James Madison University and is currently enrolled in Stevenson University’s Forensic Investigation Master’s Program. She is employed by a Medicaid Integrity Contractor (MIC) as a health claims auditor. The MIC operates under the direction of the Centers for Medicaid and Medicare services and in conjunction with state Medicaid programs to investigate and audit Medicaid provider fraud, waste and abuse.