5-2018

The role of forensic accounting in U.S. counterterrorism efforts

Madison Gaither
University of Tennessee at Chattanooga, xpq564@mocs.utc.edu

The Role of Forensic Accounting in U.S. Counterterrorism Efforts

Madison P. Gaither

Departmental Honors Thesis
The University of Tennessee at Chattanooga
Accounting

Examination Date: March 23, 2018

_____	_____
Amie L. Haun	Dr. Joanie Sompayrac
Lecturer in Accounting	UC Foundation Professor of Accounting
Thesis Director	Department Examiner

Abstract

The September 11th attacks on the World Trade Center directed international attention to the financial component of terrorist operations. The demand for forensic accounting specialists is increasing rapidly because of a growing intolerance for fraud and terrorist activity. This research paper argues that forensic accountants have and will continue to have a vital role in United States' counterterrorism efforts in the post-9/11 era by detecting acts of fraud and money laundering. Comprehensive review of relevant literature including books, peer-reviewed articles, government databases, court records and news media reveals that forensic accountants are equipped with special skills and analytical tools that make them valuable members of terrorism task forces. The soft skills of forensic accountants typically include attention to detail, self-motivation, professional communication, and integrity. Technical skills include broad industry knowledge, data gathering techniques, advanced financial statement interpretation, and ratio analysis.

Literature review also indicates that government organizations are relying more on financial analysts for gathering evidence and preparing summary reports for investigations, prosecutions, and court proceedings. Additionally, a demand exists for forensic accountants in private-sector companies to implement and monitor systems of internal control (e.g. fraud and enterprises risk management frameworks) and communicate threats to the FBI or Department of Homeland Security. While past research mainly includes retrospective analysis of terrorist financing, this paper will argue that forensic accounting will continue to be relevant due to technological change and shifting political, legal, and financial climates.

The Role of Forensic Accounting in U.S. Counterterrorism Efforts

Introduction

The National Commission on Terrorist Attacks upon the United States (2004) estimates that the September 11th attacks cost the organizers anywhere between $400,000 and $500,000 to perpetrate. The terrorists were able to successfully transfer these funds without raising suspicion of financial or government institutions, which resulted in one of the most devastating terror attacks on U.S. soil with approximately 3,000 deaths and billions of dollars in damages (Alexander, 2004). Governments, banks, and other institutions have since strived to implement controls to prevent and detect acts of terrorist financing. These efforts include utilizing the special skillset of forensic accountants in both public and private sectors to identify, prosecute, and aid in the eradication of terrorists and their sympathizers from the U.S. economy.

This study applied a qualitative approach to discover the role of forensic accounting in U.S. counterterrorism efforts in the post 9/11 era. Results emerged after careful reading of content and comprehensive review of relevant literature from both primary and secondary sources. Primary sources of high authority include U.S. District, Appellate, and Supreme Court rulings; transcripts from United Nation's International Convention for the Suppression of Financing Terrorism; and various publications from U.S. Executive Agencies including the Departments of Justice, Homeland Security, and Treasury. Other primary sources referenced include publications from the National Counterterrorism Center, publications from accounting professional organizations (e.g. AICPA), and interviews with forensic accountants and special agents within the FBI. Secondary sources referenced include textbooks, peer-reviewed articles in professional journals, and news articles. Qualitative analysis of relevant literature reveals that forensic accountants make valuable members of terrorism task forces due to their detailed

financial training and unique ability to detect nuances in cash flows. This paper attempts to contribute to our understanding of terrorist financing and the specific role that forensic accountants have in U.S. counterterrorism efforts.

Overview of Terrorist Financing

Defining Terrorism

This paper makes use of the terms "terrorism" and "terrorist financing" often; therefore, it is beneficial to discuss how they are used and understood in this analysis. Unfortunately, it is difficult and often counterproductive to have a globally agreed-upon definition of terrorism. First, terror is an abstract psychological response, and there are always exceptions to abstract definitions. Secondly, because terrorism is constantly evolving, it is almost impossible to create an all-inclusive definition. Dr. Walter Laqueur states that "no all-embracing definition will ever be found for the simple reason that there is not one terrorism, but there have been many terrorisms, greatly differing in time and space, in motivation, and in manifestations and aims" (2007). However, for the purpose of this paper we will use the definition of terrorism provided by Alex Schmid and Albert Jongman (1988):

> "Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi)clandestine individual, group, or state actors for idiosyncratic, criminal or political reasons, whereby- in contrast to assassination- the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population and serve as message generators" (p. 28).

The term "terrorist financing" refers to the funds obtained from both legal and illegal sources, transferred between parties, and used to advance the interests of terror groups or to fund specific

activities. The UN International Convention for the Suppression of the Financing of Terrorism defines funds related to terrorism as:

> "assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, traveler's checks, money orders, shares, securities, bonds, drafts, letters of credit" (The United Nations, 1999).

For example, the funds related to the 9/11 attacks included cash, traveler's checks, and debit and credit cards. These funds were sent and received through bank-to-bank transfers and were primarily used to finance flight training, living expenses, and travel (National Commission, 2004).

Financial Needs of Terrorists

Terry Davis, Secretary General of the Council of Europe, stated, "Terrorists seldom kill for money, but they always need money to kill" (2007). Terrorist organizations are essentially in the business of terrorizing, in which they incur substantial operational costs just like legitimate businesses (Gurulé, 2008). Perpetrating a terrorist attack of any scale requires the careful planning and controlling of vital resources including money, people, and materials. Terrorists fund their operations both legally and illegally with activities extending across the globe (Raphaeli, 2003). These funds are needed for obtaining false documents, explosive chemicals, transportation, communications, equipment, and weapons (Koh, 2006; Gurulé, 2008). Other costs incurred include general livelihood expenses (e.g. housing, food, uniforms), training facility maintenance, and compensation for soldiers and their families. For example, Al-Qaida supported approximately 70,000 soldiers in extensive training camp networks before the 9/11,

and reports in Palestine show that as much as $30,000 is given to the surviving relatives of suicide bombers (Koh, 2006, p.12-13).

Terrorists develop strong relationships with the nations or regions where they operate by financially supporting other militant groups with similar goals and soliciting the social and political cooperation of key leaders in their territories. For example, before the 9/11 attacks, Osama bin Laden repeatedly reached out to Taliban leader Mullah Mohamed Omar, "the most powerful man in Afghanistan at that time" for support (Curry, 2013, p.16-17). Additionally, terrorist organizations create safe havens by donating to charities or other public service organizations like schools and mosques to win the favor of local communities (Gurulé, 2008). Like any other business, substantial capital is critical for maintaining the organizational structure and growing the operations of a terrorist organization; however, the means and motives of obtaining and moving capital for terrorism are of a more sinister nature.

Obtaining and Laundering Funds

Terrorist financing can come from external sources such as individual donations, businesses, governments or banking systems, while activities that generate cash within terrorist organizations can include drug and human trafficking, kidnapping, ransom, blackmail or credit card fraud (Levitt, 2002; Koh, 2006). Abu Sayyaf, a radical Islamist sect in the Philippines, obtained nearly $5.5 million by kidnapping citizens and demanding ransoms; the sect was able to expand their ranks from 200 to 3,000 individuals in the early 2000s and became the largest employer in many poor areas of the Philippines (Koh, 2006, p.12). Additionally, a 2003 joint FBI-DEA investigation resulted in the arrests of sixteen Afghan and Pakistani individuals involved in an extensive heroin operation. These individuals smuggled drugs into the U.S., and

the profits were laundered by stateside businessmen who returned the funds to criminal counterparts in the Taliban and Al-Qaida (McCraw, 2003).

Money laundering. Terrorist organizations are often tasked with transforming proceeds from illegal activities into useable assets (Chong & Lopez-de-Silanes, 2015). This process is known as money laundering, or "disguising… the existence, nature, source, control, beneficial ownership, location, and disposition of property derived from criminal activity" (ACFE, 2016). According to Choo (2009), there are three stages of money laundering: placement, integration and layering. The individuals place the assets in use, disguise the funds with legitimate income, and reinvest or redistribute the funds. For example, dirty money from a drug or weapons operation can be used to purchase prepaid cards or layered with other income from a legitimate business. Then, this pool of "legitimate" funds can be used to purchase materials necessary to continue illegitimate operations.

While terrorist financing often involves money laundering, Koh (2006) argues that the final product of terrorist financing is distinguishable from other criminal activities as shown in Figure 1 below. Koh states that "money laundering begins with brushing off the audit trail and ends by achieving legitimization, while terrorist financing begins with money making and ends with distributing it" (2016, p. 27). While a drug lord might launder money through a restaurant to hide the illegal source of his income to appear as a legitimate businessman, a terrorist organization might launder money through a restaurant to later distribute it for its operations and expenses, not for personal profit or legitimate societal status.

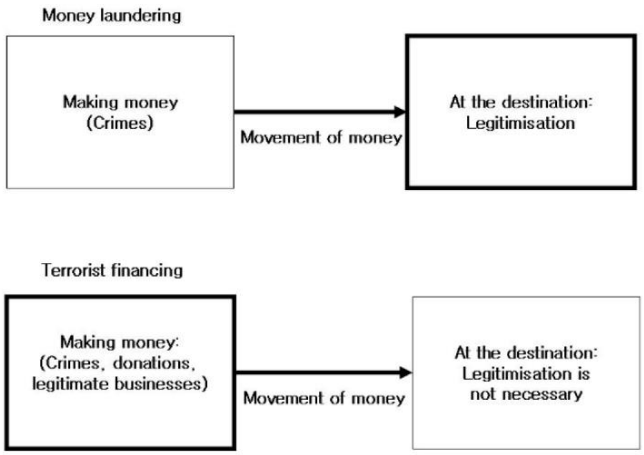

Figure 1. Disguising the funds related to a terrorist operation is means to an end, not the goal. Source: Koh, J. (2006).

Off-book financing allows a company to conceal revenues in accounts not listed in the financial statements, and businesses that deal heavily in cash are at a higher risk for fraud (Mantone, 2013; Messier, Glover & Prawitt, 2016). Terrorists often launder funds through companies such as bars, restaurants, waste paper brokers, laundry mats, car washes, check cashing, wire-transmitting services, and non-profits[1] (Dorrell & Gadawski, 2005; ACFE, 2016). These types of businesses are cash-intensive making it easier for criminals to disguise dirty money in pools of legitimate business income by contriving fictitious sales receipts or invoices (Reuter & Truman, 2004). For example, Abdirahman Isse and Abdillah Abdi operated a wire-transmitting service out of Virginia which became a subsidiary for a network headquartered in the United Arab Emirates. The business assisted customers who sent funds to Somalia, Ethiopia, Kenya, and Sudan from 1997 to 2001. Isse and Abdi routinely deposited and withdrew funds just below $10,000 and were found guilty of conspiracy to structure financial transactions to evade

[1] Osama bin Laden was known to have an extensive global network of companies in wood and paper industries, hospital equipment, fishing boats, and real estate (Koh, 2006).

reporting requirements.[2] The U.S. Department of Treasury was able to freeze the assets of the network with proof that the money-transmitting business was a channel for terrorist sympathizers to funnel cash to Al-Qaida cells in Africa and the Middle East (U.S. v. Isse, 2003).

Money trails nearly disappear with the use of prepaid products like "burner" phones or cash cards, which are not traceable to a specific individual or bank account. The advantages of prepaid cards include anonymity, convenience, affordability, and reduction of overdraft risk. The use of prepaid cards requires no face-to-face verification, and the cards can be hidden among other personal items to avoid detection by customs officials at international borders. These cards can be drained, reloaded instantly from anywhere in the world, and carried by mules to fund terrorist activities (Choo, 2009).

Forensic Accounting

Terrorist organizations, like legitimate businesses, need money to continue to fund their operations. "Follow the money" is a common phrase in accounting and investigative communities. The phrase is simple, but investigations are often complicated by factors including the use of prepaid cards, extensive laundering schemes, and carefully crafted transactions that fall just below mandatory financial institution reporting. If the intent to commit an act of terrorism can be proven, an individual can be prosecuted under U.S. laws without funds ever moving locations (Dorrell & Gadawski, 2005). However, intent is very difficult to prove in court because it occurs in the criminal's mind. Forensic accountants can utilize a wide array of technical skills to establish "a sufficient pattern of fraudulent transactions or activities" to provide evidence necessary for the prosecution of terrorists (Singleton & Singleton, 2010, p. 41).

[2] Under the Bank Secrecy Act, financial institutions are required to file Suspicious Activity Reports (SARs) to combat money laundering in the United States. The law requires any cash transactions exceeding $10,000 (daily aggregate amount) to be included in these reports. More information about the mandatory reporting requirements can be found at https://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html.

The Association of Chartered Certified Accountants defines forensic accounting as "the application of accountancy skills and knowledge in circumstances that have legal consequences" (ACCA, 2015). Forensic accounting is often confused with auditing, but inquiries conducted by forensic accountants are generally more in-depth and of a wider scope than audits (Bilbeisi & Brown, 2015). An anonymous agent within the FBI describes forensic accounting as a "360" of accounting; in other words, forensic accounting requires knowledge beyond foundational accounting. It is necessary to know not just how to report a transaction correctly, but how a transaction can be reported incorrectly and hidden or covered up. The agent states that forensic accounting involves reverse engineering, or taking events and transactions apart to see how they fit together. The agent states, "Investigators at the Bureau must continually ask themselves what the terrorists are thinking when they try to launder money" (FBI Forensic Accountant, personal communication, February 8, 2017). Due to this, there is a need for highly-specialized individuals who are trained in accounting to assist in terrorist investigations.

Soft Skills of Forensic Accountants

Literature review results indicate that accountants possess unique personality traits, communications skills, and strict ideals of integrity that empower them to detect financial crimes. According to Carl Jung (1971), there are eight personality types that dominate society; these traits can be divided into four dichotomous pairs: extraversion versus introversion, sensing versus intuition, thinking versus feeling, and judging versus perceiving. Jung argues that an individual has a dominate trait in each of the four pairs; this theory has been adapted into the Myers-Briggs Type Indicator (MBTI) as shown in Figure 2 below. Research indicates that while all MBIT personalities are represented in the accounting profession, a prevalent number of Sensors and Judgers are attracted to and retained in the industry (Schloemer, 2015; Swain &

Olsen, 2012; Kovar et al. 2003; Wheeler, 2001). By following 1,208 students throughout college and into their professional careers, Swain and Olsen (2012) found that Sensors and Judgers were respectively 9.48 and 1.59 times more likely than their pair counterparts to major in accounting (p. 30). Similar results were found in studies conducted by Oswick and Barber (1998), Ramsay et al. (2000), Bealing et al. (2006), and Garlick et al. (2013).

	Sensing		Intuitive		
Judging	**ISTJ** **The Inspector** Responsible, Organizer, Analytical, Private, Hardworking, Sound Practical Judgement 11.6%	**ISFJ** **The Protector** Warm, Considerate, Gentle, Responsible, Enjoys being helpful, Work behind the scenes 13.8%	**INFJ** **The Counselor** Reflective, Idealistic, Organized, Psychic, Quietly caring, Enjoy intellectual stimulation 1.5%	**INTJ** **The Mastermind** Innovative, Strategic, Logical, Reserved, Driven by own original ideas for improvement 2.1%	Introvert
Perceiving	**ISTP** **The Crafter** Action-oriented, Hands-on practicality, Enjoys adventure, Skilled at how things work 5.4%	**ISFP** **The Composer** Warm, Sensitive, Artistic, Nurturing, Realistic, In touch with self nature and creating environments 8.8%	**INFP** **The Healer** Sensitive, Creative, Idealistic, Perceptive, Value inner harmony, Focus on possibilities 4.4%	**INTP** **The Architect** Intellectual, Logical, Socially cautious, Imaginative thinkers, Enjoy creative problem solving 3.3%	
	ESTP **The Promoter** Unconventional, Fun, Lives for here and now, Good problem solver, Spontaneous 4.3%	**ESFP** **The Performer** Social, Spontaneous, Loves surprises, Juggles multiple projects, Quip master/ Witty 8.5%	**ENFP** **The Champion** Seeks harmony, Playful, Life of party, Optimistic, People oriented, Sees value in others 8.1%	**ENTP** **The Inventor** Objective, Enthusiastic, Versatile, Strategic, Enjoys new ideas and challenges, Tests limits 8.1%	Extrovert
Judging	**ESTJ** **The Supervisor** Efficient, Outgoing, Systematic, Analytical, Results driven, Traditional, Likes to run the show 8.7%	**ESFJ** **The Provider** Good interpersonal skills, Gracious, Eager to please, Practical, Harmonizing, Enjoys being active 12.3%	**ENFJ** **The Teacher** Charismatic, Idealistic, Persuasive talker, Organized, Values connection with people 2.5%	**ENTJ** **The Field Marshal** Visionary, Take change, Gregarious, Logical, Outgoing, Effective planners of people 1.8%	
	Thinking	Feeling		Thinking	

Figure 2. Accountants dominate Sensing and Judging personality types on the MBTI. Source: "Myers-Briggs Type Indicator Grid." KONA. (n.d.).

According to the MBIT, Sensors are typically more concerned with facts; these individuals are logical, realistic, and bottom line-oriented. In contrast to Intuitors, Sensors rely more on their own experiences rather than information given. Furthermore, Judgers enjoy making lists and staying on task. In contrast to perceivers, Judgers are less flexible with deadlines and prefer to streamline decision-making (Martin, 1997). Because Sensing and Judging

personality types are prevalent in the profession, abilities such as attention to detail, organization and self-motivation dominate a typical accountant's skillset. For example, an anonymous special agent within the Financial Crimes Unit of the FBI describes his background in public accounting as an advantage over other agents in the same investigative field. He states that in his experience, the accounting mind is trained to work differently and approaches tasks with specificity (FBI Agent & Forensic Accountant, personal communication, November 20, 2017).

Communication and professional client interaction is a key skill required in the accounting industry. Alan Anderson (2012) lists "people skills" and "superior communication skills" as two qualities that a good accountant must possess. Individuals with a background in auditing are trained to communicate their findings both orally and in writing. Similarly, tax specialists are trained to explain complicated legal codes and other tax laws to clients. Expert witness testimony is a large professional role of fraud consultants and forensic accountants. These individuals must possess the ability to condense in-depth findings and communicate them in a way that is understandable to lawyers, juries, and judges (Dorrell & Gadawski, 2005). With the rise of technology, face-to-face interaction is a fading phenomenon; however, successful accountants are trained to maintain effective communication and professionalism at all times and through a multitude of mediums (Anderson, 2012).

Accountants have historically been associated with integrity and honesty, and these ideals are communicated to accounting students in classrooms and throughout the professional careers of CPA's (Bougen, 1994; AICPA, 2017). A CPA who is a member of the AICPA must comply with the organization's Code of Professional Conduct.[3] The Code's policy on integrity states, "In

[3] While the AICPA can only require its members to comply with the Code of Professional Conduct, U.S. state and federal courts have consistently held all CPAs to the principles outlined in the Code. As of 2016, twenty-three states have adopted the AICPA Code of Professional Conduct as their ethical and conduct standards (Messier, et al., 2016).

the performance of any professional service, a member shall maintain objectivity and integrity, shall be free of conflicts of interest, and shall not knowingly misrepresent facts or subordinate his or her judgment to others" (2017, p. 30). Messier, Glover, and Prawitt (2016) describe the profession's dedication to integrity in their textbook on auditing and assurance services:

> "Certified public accountants have been charged with providing audit services because of their traditional reputation of competence, independence, objectivity, and concern for the public interest. As a result, they are able to add credibility to information produced and reported by management to outside parties" (p. 8).

Integrity, transparency, and objectivity dominate industry conduct expectations, which are demonstrated by the core values of the Big Four[4] accounting firms:

> **Ernst & Young**: "Who we are- People who demonstrate integrity… who build relationships based on doing the right thing."
> **Deloitte**: "We believe that nothing is more important than our reputation, and behaving with the highest levels of integrity is fundamental to who we are."
> **PwC**: "Act with integrity. In everything we do… we speak up for what is right, even when it's the harder option."
> **KPMG**: "Above all, we act with integrity – constantly striving to uphold the highest professional standards, provide sound advice, and rigorously maintain our independence."

Thus, accountants are familiar with the personal and professional expectation to adhere to the highest ethical standards, a sought-out quality among numerous government organizations including the Federal Bureau of Investigation and Central Intelligence Agency.[5]

---

4 The listed core values of the Big Four accounting firms were obtained from each firm's website at the time of writing.

5 Integrity is included in the core values of both the CIA and FBI listed on the organizations' respective websites at the time of writing. The CIA states, "We uphold the highest standards of conduct. We seek and speak the truth - to our colleagues and to our customers." Similarly, the FBI's core values include a dedication to "uncompromising personal integrity and institutional integrity."

Technical Skills of Forensic Accountants

Terrorists have basic financial needs that must be fulfilled in order to maintain operations and execute attacks. Forensic accountants are equipped with the technical skills necessary to examine cash flows across a variety of mediums to assist in gathering evidence and creating financial profiles (Bilbeisi & Brown, 2015). Botha (2009) describes a forensic investigation as "an in-depth, more detailed investigation into finances and financial matters undertaken for court or law purposes and is similar in character to a criminal investigation. It utilizes specialized skills, expert knowledge, and scientific methods" (p.115). The technical skills of forensic accountants include broad industry knowledge, advanced financial statement interpretation, data gathering, and analysis techniques.

Forensic accountants often have various backgrounds in auditing, taxes, litigation, consulting, and banking; therefore, these individuals have the industry knowledge of what financial statements should look like and the attention to detail to detect anomalies and/or misinformation. For example, a forensic accountant might recognize when the fees for a certain transaction look too high or too low, or when the expenses claimed by a charity are higher than the industry norm (FBI Forensic Accountant, personal communication, February 8, 2017). Forensic expert Pam Mantone states in her book on financial statement analysis that "abnormal growth in days sales in receivables [Accounts receivables ÷ Total credit sales per day] when compared to benchmarks of similar companies" and "the growth in profit margins [Net income ÷ net sales] that are in excess of industry standards" are early warning signs of fraud (2013, p.20). Therefore, a forensic accountant's industry knowledge can expedite the investigative process by gathering data and examining financial statements for manipulation. Marc Curry (2013) describes the importance of forensic accounting in gathering data for financial investigations:

> "Using their basic accounting and auditing skills, forensic accountants also utilize their understanding of economic theory and data gathering when analyzing, interpreting and summarizing their findings when they conduct their audits… The forensic accountant picks apart every receipt and financial statement they are reviewing and in a way work backwards to calculate any patterns within the money trail" (p.200).

If the forensic expert expects that fraud is being committed by examining data, a more thorough investigation can be conducted.

Forensic accountants typically have a background in public accounting, are comfortable around financial statements, and are familiar with the nuances of money flow. Coupled with necessary industry knowledge, forensic accountants are more likely to detect when an individual or company has committed fraud. A common financial crime is the overstatement of assets and revenues or understatement of expenses and liabilities in financial reporting (Crumbley et al., 2007). For example, Sunbeam Corporation began using "bill and hold sales" to manipulate earnings in 1997. The company offered buyers lower prices for purchase orders well in advance of needed items and maintained custody of the goods until delivery was requested. The SEC described the scheme as "little more than projected orders disguised as sales" (2001). Additionally, companies can omit proper disclosures or engage in fraudulent related-party transactions to disguise unfavorable information from financial statements, as was the case in the 1990s with Enron's special-purpose entities (SPEs)[6] (Crumbley et al., 2007). Considering frauds such as this, forensic accountants developed a wide array of data analytics and ratio functions that are powerful tools in detecting abnormalities in financial data.

[6] Enron CFO, Andy Fastow, sold company stock to special-purpose entities and fraudulently recorded the promissory note as an addition, rather than reduction, of equity (Crumbley, et al., 2007).

Net Worth Method. Forensic accountants and investigators can directly trace cash flows through various accounting and financial records. However, in the instance that a financial records statement crime is being committed, the perpetrator takes precautions to cover his trail, and these documents are often not available (Botha, 2009). If investigators identify a suspect that is living unexplainably lavish, the Net Worth Method can be used to indirectly calculate an estimate of income to compare to the amount on an individual's tax returns. Investigators calculate the individual's net worth (assets less liabilities) and account for explainable differences, such as nontaxable income. Any significant differences that cannot be accounted for are red flags (Crumbley et al., 2007). The Net Worth Method does not tell investigators where the unaccounted income comes from and cannot be used as direct proof of a crime, but the method can lead investigators to dig further into the financial records of the suspected criminal (Botha, 2009).

Percentage analysis. Forensic investigators can quickly spot red flags in financial data by converting statement amounts into percentages of assets or revenue totals. Horizontal analysis examines financial data from year-to-year, and unexpected changes in the percentages over time can be examined further (Crumbley et al, 2007). For example, HealthSouth Corporation underwent federal investigation for fraudulent misrepresentation of financial data and insider trading in 2003 (Tie, 2010). The FBI suspected HealthSouth of inflating income and assets in its financial statements; specifically, agents discovered the use of overvalued intangible assets to reduce expenses over a period of several years as shown in Table 1 below.

HealthSouth Corp.	CYE 1996 (in $000)	CYE 1997 (in $000)	1996-1997 $ Change	1996-1997 % Change	CYE 1998 (in $000)	1996-1998 $ Change	1996-1998 % Change
Intangible Assets	$1,094,421	$2,243,372	$1,148,951	105%	$2,959,910	$1,865,489	170%

Table 1. Horizontal analysis can be used to spot fraud in financial statements. Source: Tie, R. (2010).

The SEC reported that HealthSouth Corporations' assets were overstated by $800 million by the third quarter of 2002 (Litigation Release No. 18044, 2003).

Similarly, investigators can use vertical analysis to display data amounts as a percentage of a total amount on a statement. For example, these percentages can be compared with other accounts within the same company's statement or with percentages from industry averages and individual competitors. Forensic expert, Pam Mantone describes an example of the usefulness of vertical analysis when examining accounts in a company's statements:

> "If sales are decreasing, accounts receivable is decreasing, and accounts payable is increasing while expenses are decreasing, then it is reasonable for cash to be increasing. If cash was decreasing in this scenario, a forensic examiner would spot the red flag by conducting a simple vertical analysis" (2013, p.40).

In the same 2003 HealthSouth Corp. case discussed above, the FBI used vertical analysis to compare HealthSouth to Tenet HealthCare Corp., a major competitor in the industry. Agents discovered that HealthSouth's intangible assets as a percentage of total assets were materially greater than leading competition as shown in Table 2 below.

	Health South Corp. CYE 1997 (in $000)	**Tenet HealthCare Corp. FYE 5/31/1998 (in $000)**
Intangible Assets	$2,243,372	$3,417,000
Total Assets	$5,401,053	$12,833,000
Intangible Assets as % of Total Assets	42%	27%

Table 2. Vertical analysis can be used to spot fraud in financial statements. Taken from: Tie, R. (2010).

In addition to percentage analysis, various ratio analyses can be performed to examine relationships between accounts that can assist investigators in assessing a company's liquidity, solvency, asset management, profitability, market performance, and cash flow (Trussel, 2017). Additionally, Edward Altman's model[7] (1983) and Messod Beneish's model[8] (1997) can assist investigators in making judgements related to bankruptcy predictions and likelihood of earnings manipulation respectively. It is outside the scope of this paper to discuss all ratio analysis functions available, but a more inclusive list can be found in the appendix of this paper. An abnormality in a single ratio alone is not enough to suspect a company or individual of illegal activity. Rather, forensic accountants can utilize qualitative review of financial statements with quantitative percentage and ratio analysis to establish a better understanding of a company's financial environment and likelihood of fraud.

Other analytical measures. The overwhelming amount of data involved in a fraud or money laundering case is a complicating factor for investigators. However, several additional measures are at the disposal of forensic accountants including digital analysis and other data

[7] More information on the Altman model can be found in *Corporate financial distress: a complete guide to predicting, avoiding, and dealing with bankruptcy*. New York: Wiley.

[8] More information on the Beneish Model can be found in "Detecting GAAP violation: Implications for assessing earnings management among firms with extreme financial performance." *Journal of Accounting and Public Policy,* 16 (3), 271-309/ doi: 10.1016/S0278-4254(97)00023-9.

filtering techniques. Physicist Frank Benford discovered in the 1920s that low digit numbers occur more frequently in the world, a phenomenon that also applies to accounting records and transactions (Nigrini, 1999). Benford found that data sets follow a "predictable pattern," and deviance from the expected pattern might suggest "artificial or contrived numbers" (Dorrell & Gadawski, 2005, p. 3). Forensic accountants can apply Benford's law to large data sets (e.g. invoices or stock exchange data) to highlight irregularities. Dr. Mark J. Nigrini lists several other practical applications of Benford's law and digital analysis in examining financial data related to accounts payable, multilocation inventory, processing inefficiencies, new selling price combinations, and customer refunds (1999, p. 81). Generally, daily accounting records by a company are recorded to the cent and consist of a higher percentage of small transactions rather than large transactions. Therefore, a high volume of large or rounded transactions should be scrutinized. Additional digital analysis techniques search for excessive duplicated data and transactions that fall between the $8,000-9,000 range to avoid mandatory reporting (Dorrell & Gadawski, 2005). These digital techniques filter a huge population of transactions into a manageable pool of transactions for the forensic accountants to examine manually for indications of wrongdoing (Ibid).

The Net Worth Method, percentage analysis, Benford's law, digital analysis, and other technical measures are powerful tools used by analysts to investigate financial crimes. However, the use of these techniques requires an understanding of mathematics, statistical modeling, and numeric sequencing, but more importantly, the ability to interpret and further investigate the results. With a background in public accounting, forensic accountants are typically comfortable with large data sets and can apply these analytical techniques to filter data using Microsoft Excel and other advanced software (Collins, 2017). Combined with industry experience and attention

to detail, forensic accountants are uniquely equipped with the technical skillset to help attorneys and juries visualize and understand unusual or fraudulent accounting patterns in terrorist investigations.

Civil Strategies Used by Forensic Accountants

Forensic accountants can be vital legal resources in civil and criminal investigation and prosecution of suspected terrorists. However, prosecutions under criminal laws can be time-consuming, labor intensive and require a higher burden of proof to convict (Smith & Cooper, 2009). Fortunately, there are a variety of civil statutes that are available to law enforcement and investigators (Dorrell & Gadawski, 2005). Notably, Title 18 of the United States Code Section 2333(a) provides the legal basis to prosecute terrorists and terrorist sympathizers under civil proceedings. Section 2333(a) was passed as a part of the Anti-Terrorism Act of 1992 as a derivative of the criminal provisions provided in 18 U.S.C. §2339B[9] and 18 U.S.C. §2339C[10] (Smith & Cooper, 2009). Section 2333(a) states:

> "Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney's fees."

In 2008, the U.S. Court of Appeals of the Seventh Circuit affirmed a $156 million award to the family of David Boim, a U.S. citizen who was murdered in Israel by members of Hamas. The

[9] 18 U.S.C. §2339B prohibits knowingly providing (or conspiring to provide) support to a foreign terrorist organization. To read the full statute, visit https://www.law.cornell.edu/uscode/text/18/2339B.

[10] 18 U.S.C. §2339C prohibits providing or collecting funds intended to cause death or injury to a civilian. To read the full statute, visit https://www.law.cornell.edu/uscode/text/18/2339C.

Washington Legal Foundation filed the suit under the Anti-Terrorism Act of 1992 against the Holy Land Foundation and other defendants "for providing financial and other support to Hamas" (WLF, 2008). *Boim v. Holy Land Foundation* is a landmark case that "appears to have cleared away the major obstacles complicating the use of section 2333(a)" and other civil statutory measures in prosecuting terrorist financing (Smith & Cooper, 2009, p. 75).

In addition to U.S. Code Section 2333(a), courts have the ability to apply the doctrine of alter ego; this allows courts to pierce the corporate veil and hold individuals responsible for the wrongdoings of corporations that are otherwise treated as separate legal entities (Dorrell & Gadawski, 2005). In *Dietel v. Day* (1972), the doctrine of alter ego is defined as follows:

> "The corporate fiction will be disregarded when the corporation is the alter ego or business conduit of a person…The alter-ego status is said to exist when there is such unity of interest and ownership that the separate personalities of the corporation and owners cease to exist" (16 Ariz. Ct. App., 492 P.2d 455).

The alter ego doctrine gives courts the power to prosecute individuals involved in organizations that are directly linked to terrorists. Additionally, The Antiterrorism and Effective Death Penalty Act of 1996 gives the U.S. Secretary of State the power to designate organizations and their aliases as a Foreign Terrorist Organization (FTO). As described in *National Council of Resistance of Iran v. Department of State* (2004), "Alias status is established… when one organization so dominates and controls another that the latter can no longer be considered meaningfully independent from the former." The ramifications of this designation 1) makes it illegal to knowingly support a designated FTO, 2) bars FTO representatives and members from the U.S., and 3) allows banks to freeze the funds of a designated FTO (U.S. Department of State). The alter ego doctrine and the FTO designation are powerful tools that are increasingly

utilized to pressure terrorists and affiliated organizations "to get out of the terrorism business" (Ibid).

The statutory measures discussed above are only a few of the civil strategies used to prosecute financial crimes. These cases generate demand for skilled forensic accountants to collect evidence and perform data analysis functions to expedite the investigative process. Law firms can hire forensic accountants as consultants or expert witnesses, and courts can appoint forensic accountants as masters or special masters in specific financial cases (Crumbley et al., 2007). Forensic accountants use their industry knowledge and skills to orally communicate complex financial concepts and analyses to lawyers, judges, and juries (Curry, 2013; ACCA, 2015). As mentioned previously, if the *intent* to commit an act of terrorism can be proven, an individual can be prosecuted under U.S. laws without funds ever moving locations (Dorrell & Gadawski, 2005). Forensic accountants can provide expert testimony or interpretation of financial analyses performed to help prove to the court that the defendant intended to commit a crime. Extensive anti-terrorism statutes exist in U.S. civil and criminal law; combined with the legal expertise of investigators and the financial expertise of forensic accountants, terrorists are facing their hardest battle yet.

Forensic Accounting and Counterterrorism

Unfortunately, as counterterror task forces become more efficient and technology advances, so do the terrorists. In his analysis, André Botha discusses the convoluted nature of financial crimes and the inability of any classroom to adequately prepare investigators with *all* necessary skills:

> "The fight against financial crime is fraught with difficulties. It takes place in the global sphere, in an extremely complex, sophisticated, and worldwide distribution, in a highly

> technological environment… What the expectations of the community and authorities are asking from investigators in the field of preventing and combating financial crime make up a kind of knowledge which no existing discipline provides ready-made" (2009, p. 24).

The knowledge needed to combat financial crimes and terrorist financing cannot be learned in a single setting, through a single academic discipline, or by a single individual. Rather, the knowledge and skills are developed over individual careers and are best utilized when individuals from various professions are brought together in counterterror teams. The information gathered in this paper suggests that individuals who are trained in accounting and pursued careers in banking, finance, or other financial sectors are advantageously prepared to participate in forensic investigations due to the nature and expectations of their profession.

Forensic accountants in the FBI

Accounting has been an integral part of the FBI since its creation in 1908, but substantial waves of accounting employees within the Bureau occurred 1) during the 1920s due to Prohibition and mobsters like Al Capone,[11] and 2) during the 1940s as a result of WWII investigations involving the Surplus Property Act, Contract Settlement Act, and War Fraud Claims (Bilbeisi & Brown, 2015; Crumbley et al., 2007). Demand for forensic accountants in the FBI also increased in the early 2000s due to corporate scandals such as Enron and WorldCom (Crumbley et al., 2007). Approximately 15 percent of FBI employees today are qualified special agent accountants with a variety of certifications and specialties; these individuals must meet high qualification standards and go through rigorous training (Curry, 2013, p. 200; Bilbeisi &

[11] The FBI pursued many mobsters during the 1920s, but the Bureau's initial participation in the Al Capone case was limited until he was suspected of a federal crime. Capone's takedown is ultimately attributable to the forensic accounting work of the U.S. Treasury Department. Capone was indicted and found guilty of tax evasion and prohibition charges in October 1931 (Beebe, 2016; "Solving Scarface," 2005).

Brown, 2015). Forensic accountants are located in FBI offices across the nation and play an important role in the Bureau and other governmental agencies as they investigate cases across a wide criminal spectrum. Special agents often go into the field to collect evidence and conduct surveillance and interviews. The agents then update the case files, and forensic accountants are responsible for reviewing the evidence and identifying any red flags that may suggest a financial crime is being committed (FBI Agent & Forensic Accountant, personal communication, November 20, 2017).

After the September 11th attacks, the FBI created the Terrorist Financing Operating Section (TFOS) to direct more attention to the financial aspect of counterterrorism (Terror Financing, 2013). John Pistole, Assistant Director of the FBI's Counterterrorism Division, stated:

> "TFOS has developed tactical and strategic, time sensitive, financial investigative methodologies enabling the FBI to be recognized worldwide as the leader in this area. TFOS has evolved into a broader strategy to identify, investigate, prosecute, disrupt and dismantle incrementally all terrorist related financial and fundraising activities (2003)."

TFOS consists of special agents, analysts, forensic accountants, and other professionals that jointly gather intelligence and follow money trails of suspected terrorists (Terror Financing, 2013). Additionally, white-collar crime divisions exist within many of the FBI's 56 field offices and typically investigate financial crimes such as insider trading, health care fraud, and bank fraud. However, their accounting and finance expertise can be tapped into by the TFOS and other joint task forces during times of crisis. For example, special agent accountants and forensic accountants in white-collar divisions across the country were called upon to assist with the 9/11 terrorism investigation. Recently, the white-collar divisions in Tennessee were contacted to assist with the investigation of the July 2015 terrorist attack on a Chattanooga military facility that

killed four U.S. Marines and one U.S. Navy officer (FBI Agent & Forensic Accountant, personal communication, November 20, 2017; Rayman, 2015).

Outside of the FBI, other government organizations, notably the CIA and Department of Homeland Security, employ accountants in various analyst positions in intelligence, counterterrorism, and cyber threat divisions (CIA, 2017; DHS, 2017). These analysts participate in high-profile investigations by gathering evidence, preparing support documents (e.g. warrants), compiling findings in investigative reports, and meeting with prosecutors (Bilbeisi & Brown, 2015). Identifying patterns and red flags in large sets of data takes a trained eye and years of specialized experience. The FBI estimates that the Oklahoma City bombing cost approximately $4,000 to execute, the attack on the USS Cole about $10,000, and the London subway bombings around $14,000 (Terror financing, 2013). It is not uncommon that the dollar amounts involved in executing terror attacks are very low, so the expertise that forensic accountants and analysts possess is critical to national security. Organizations like the FBI and DHS spend extensive advertising dollars on public campaigns such as "If You See Something, Say Something[12]," and strive to maintain open lines of communication with private institutions who are often the true "first responders" of terrorist financing (Bures, 2013).

The Value of Public-Private Partnerships

It is a common misconception that fighting terrorism is the sole responsibility of the government. Parker and Taylor (2010) argue that we are experiencing "a new security paradigm in which financial borders and parameters are best understood as a 'complex assemblage' in which private financial institutions are in effect, authorized to make security decisions" (p. 459)

[12] "If You see Something, Say Something" is the Department of Homeland Security's campaign to encourage citizens to report suspicious activity (e.g. signs of terrorist activity or human trafficking) to local law enforcement. More information can be found at https://www.dhs.gov/see-something-say-something.

The National Commission of Terrorist Attacks Upon the U.S. (2004) estimates that the private sector controls approximately 85 percent of the country's critical infrastructure, which in turn makes many private U.S. companies a target for attack. Therefore, the private sector has the opportunity, and arguably the responsibility, to contribute to counterterrorism efforts (Bures, 2013). The U.S. DHS describes critical infrastructure as "the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on." Homeland Security has identified sixteen major infrastructure sectors[13] that the department works closely with to share information and monitor threats, but is this enough?

While a massive infrastructure breach has not yet occurred in the United States, other countries around the world have experienced devastating attacks. Notably, three distribution centers of a Ukrainian electricity company were remotely accessed by foreign hackers within thirty minutes of each other leaving approximately 225,000 Ukrainians without power for several hours on December 23, 2015. (ICS-CERT, 2016). The Electricity Information Sharing and Analysis Center (2016) described this incident as the first cyber-attack of its kind that "targeted solely civilian infrastructure," through which the hackers demonstrated "an escalation from past destructive attacks that impacted general-purpose computers and servers" (p. 20). This incident should catch the attention of not only companies in charge of critical infrastructure, but companies in all industries and should demonstrate how important public-partnerships are to protecting company assets and civilian lives.

[13] A full list of The U.S. Department of Homeland Security's Critical Infrastructure Sector Partners can be found at https://www.dhs.gov/critical-infrastructure-sector-partnerships.

The Corporate Stake. According to the Institute for Economics and Peace (2017), the global economic impact of terrorism was $84 billion in 2016. Terrorism has a direct impact on businesses in all industries in the U.S. and abroad, and attacks have the potential to disrupt supply chains, affect available employees, and dissuade investors (Rosand & Millar, 2017). For example, Air France-KLM claimed the company lost $76 million in revenue as the result of the November 2015 attacks in Paris (Landauro, 2016). Yet, many U.S. industries are still hesitant to directly involve themselves in counterterrorism efforts. (Rosand & Millar, 2017). Bures (2013) argues that while private institutions have the ability to play a large role in counterterrorism efforts, the inherent emphasis that these institutions place on generating profits rivals public interest and national security. For instance, a bank may place so much value on maintaining customer relationships that employees are less likely to raise security concerns or question the authenticity of documents (Mantone, 2017). Other companies distance themselves from the politically charged environment surrounding terrorism to satisfy "sensitive" investors or are overwhelmed by bureaucratic red tape and federal reporting mechanisms (Rosand & Millar, 2017). Despite the rationale for inaction, there is a need for transparent communication between the private sector and government organizations if terrorist financing is to be combatted on all fronts.

Potential Solutions. A strong counterterrorism task force and educational initiatives are potential solutions to the lack of information flow between the private sector and U.S. governmental agencies. Rosand and Millar (2017) suggest that President Trump utilize his vast network of business connections to gather Fortune500 CEOs to discuss how the private sector can be harnessed to combat terrorism. If companies were made aware of how terrorism has the potential to negatively affect profits, they may be more inclined to protect themselves.

Additionally, the FBI should be encouraging key private-sector company members to join local InfraGard chapters. The mission of the FBI's InfraGard is to increase "public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure" (2018). InfraGard members have the benefits of chapter meetings to discuss best company practices, online access to information about cyber threats, and an open line of communication with the FBI.[14]

This collaboration between the public and private sector could create an incentive for companies in key targeted industries (e.g. financial institutions, airlines, and cybersecurity) to recruit and train forensic accountants and other analysts to closely monitor financial security threats and communicate any concerns back to the organization. Within these critical infrastructure sectors, forensic accountants could assist with the structure of internal controls that prevent, detect, and correct threats to company assets. Within government agencies including the FBI and Homeland Security, forensic accountants could track the dirty money coming into the cities to thwart attacks. Because terrorism has the ability to disrupt almost all industries in the U.S., security is a national concern that should be on the forefront of agendas in both government and private sectors. Financial expertise, open lines of communication, and shared responsibility are strong weapons in the United States' War on Terror.

Emerging Trends and Challenges

Terrorists will adapt their financial strategies to maintain operations in constantly evolving political, legal, and financial environments; simultaneously, counterterror taskforces

[14] More information about InfraGard and membership opportunities can be found at https://www.infragard.org/.

must predict and effectively respond to these changes and adaptations. Due to a multitude of technological innovations, it is outside the scope of this paper to examine all trends and challenges emerging in the counterterrorism environment. However, the following discussion attempts to illustrate key developments that impact the role of forensic accounting in counterterrorism efforts.

Terrorist Access to Information

With a quick internet search, anyone from anywhere in the world can access an abundance of information from a computer or mobile device. Terrorists' ease of access to legal and procedural information in the United States poses a threat to law enforcement. Normal is the new deviant, meaning terrorists can often complete their mission while blending in and following U.S laws. Terrorists are becoming more aware of financial regulations and reporting requirements, so they commit seemingly routine transactions that involve small sums of money to avoid detection. These transactions are disguised as normal business operational activities, which make fraud and laundering that much harder for officials to detect (FBI Forensic Accountant, personal communication, February 8, 2017). As a result, forensic accountants will continue to be needed in financial institutions to maintain a strong system of internal controls and in government organizations such as the IRS and SEC to filter and investigate private-sector reports.

The Rise of Virtual Currency

The rise of internet-based exchange is taking the global economy by storm, and financial technology, or "fintech," is changing the way business is conducted around the world (Ducas & Wilner, 2017). Companies like PayPal and M-Pesa have already cashed in on facilitating online

purchases and transfers, but these internet-based markets have yielded the creation of a new and uncertain phenomena: virtual currencies (He et al., 2016). The European Central Bank defines virtual currency "as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" ("Virtual Currency Schemes 2012, p. 5). Bitcoin, the most popular virtual currency, was created in 2009 but only recently received international attention when the currency reached a peak price equivalent to $19,783.21 in December 2017 (Higgins, 2017). Benefits of Bitcoin and others include anonymity, timeliness, and lower transaction costs; however, the opportunity exists for criminals to exploit the use of virtual currency in committing fraud, laundering money, and financing terrorism (He et al., 2016).

Individuals can obtain Bitcoins by accepting them as payment for goods or services, mining them through online networks, or purchasing them on an online exchange (Volastro, 2014). Virtual currencies are not regulated by any governing body, which opens the door for terrorists and terrorist sympathizers to circumvent U.S. money laundering laws (Ward, 2018). Both ISIS and the Mujahideen Shura Council announced the acceptance of Bitcoin donations in 2017 leading to an increase in virtual currency schemes globally (Ward, 2018). Additionally, Zoobia Shahnaz, a 27-year-old U.S. citizen born in Pakistan, was arrested in New York before boarding a plane to Syria in July 2017. She was charged with bank fraud and money laundering for allegedly using fraudulent credit cards to purchase Bitcoins to transfer to ISIS (Reuters Staff, 2017). If Shahnaz had obtained the virtual currency through legitimate means and then laundered those funds to ISIS, the crime would have been exponentially difficult for law enforcement to detect.

The United States, United Kingdom, and the European Union are investigating and implementing policies to "crack down on… cryptocurrency" transactions (Ward, 2018). In May 2017, U.S. representatives Rice and Kilmer introduced HR2433, a bill that calls for a threat assessment by the Department of Homeland Security on virtual currencies and associated risks (Terletska, 2018). While the FBI recognizes the legality of Bitcoin transactions, agents have made numerous arrests for fraudulent transfers and unregistered users ("Virtual Ticket," 2017). Still, the decentralized and anonymous nature of virtual currencies presents legal and technological challenges for the FBI, IRS, and DHS moving forward (He et al., 2016).

The Dark Web

Virtual currency donations that terrorists receive through their fundraising campaigns can be easily used to execute illegal transactions. In fact, Bitcoin and other virtual currencies have become the preferred payment method used on the dark web to purchase items including weapons, materials, and passports (Ward, 2018). For example, German authorities believe that Ali David Sonboly, the man responsible for the July 2016 shooting in Munich that killed nine civilians, obtained the firearm from Slovakia through the "dark net" (Bender & Alessi, 2016). While authorities determined Sonboly was acting alone in his attack, the organized efforts of groups like ISIS and Hamas could produce catastrophic destruction with resources obtained through untraceable purchases made on the dark web. Terrorism has also infiltrated social media and other legal websites leaving companies like Facebook, Twitter, and Google in an uncomfortable position between prioritizing the protection of users' civil rights and national security concerns.

The Impact on Forensic Accounting and Counterterrorism

A major challenge facing the counterterrorism environment is the inability of the FBI and other government agencies to keep up with technological advancements like virtual currency transactions. James Comey, former Director of the FBI, stated, "Unfortunately, there is a real and growing gap between law enforcement's legal authority to access digital information and its technical ability to do so. The FBI refers to this growing challenge as "Going Dark," and it affects the spectrum of our work" (DOJ, 2017, p.2). Comey explains that criminals "who hide their crimes and identities behind layers of anonymizing technologies… [and] use virtual currencies to obscure their transactions" seriously limit the scope of FBI investigations (Ibid). This information gap within the Bureau necessitates 1) recruiting and retaining top global talent and 2) sharing information with other government agencies and private-sector businesses. Further research may be necessary to examine the integration of government databases into a single inter-agency data hub to exchange financial crime information.

With rapid technological innovation, the United States will need forensic accountants more than ever. The automation of many accounting systems will increase demand for individuals trained in both accounting and computer science. While numerous data processing software exist to independently perform advanced financial analyses, forensic accountants will be needed to monitor these systems and interpret the results. Accountants understand the concepts and theories related to the underlying processes of accounting information systems and are more familiar with the nuances of cash flows. With financial industry knowledge, in addition to the soft and technical skills previously discussed, accountants can detect and correct errors in the information systems more quickly than non-accounting personnel.

It is not feasible to examine every transaction, so forensic accountants will be needed to perform analytical functions to identify patterns and red flags in data sets (FBI Forensic Accountant, personal communication, February 8, 2017). It is often difficult to determine a materiality threshold when investigating terrorist financing; investigators cannot label everything as important, because then nothing is important (FBI Forensic Accountant, personal communication, February 8, 2017). Materiality is a matter of professional judgment and requires specific training and experience (Messier, Glover & Prawitt, 2016). While many processes like manufacturing, dining, and even grocery shopping have the ability to be automated, professional judgment driven by years of skill and experience cannot be programmed into an algorithm.

Limitations and Conclusion

Terrorism is a global issue that affects all aspects of society. This paper contributes to scholarly understanding of the environment in which terrorists operate and the unique opportunity of forensic accounting to disrupt that environment. One limitation is that this study was restricted to qualitative analysis only; quantitative analysis might provide more specific feedback related to forensic accountant involvement in counterterrorism on a case-by-case basis. This paper references two separate personal communications with a FBI forensic accountant and a forensic accountant-special agent team. The connection between forensic accounting and counterterrorism could be strengthened by conducting additional interviews with accountants in other government bodies and within the private sector.

If we had the technology and laws in place in 2001 that we do today, could we have prevented the September 11th attacks? With predictive analytics and innovative scientific knowledge, can we determine when the next foreign terrorist attack on U.S. soil will occur? These are important questions that government organizations and investigators should be asking

themselves. Michael Scheurer, one of the CIA intelligence analysts responsible for tracking Osama bin Laden, stated, “One of the great intellectual failures of the American intelligence community, and especially the counterterrorism community, is to assume if someone hasn't attacked us, it's because he can't or because we've defeated him” (Leung, 2004). Terrorism is a genuine threat that the United States must take a proactive, rather than reactive, stance in combatting. Committing any act of terrorism involves some combination of planning and allocating financial resources, and as long as terrorists need money, the United States needs forensic accountants. Changes in political and technological climates across the globe present many challenges to combatting terrorism, but the solution remains the same: Follow the money.

References

Alexander, D. C. (2004). *Business confronts terrorism: Risks and responses*. Madison: University of Wisconsin Press.

Altman, E. (1983). *Corporate financial distress: A complete guide to predicting, avoiding, and dealing with bankruptcy*. New York: Wiley.

Anderson, A. (2012). The characteristics of a successful auditor. Kansas Society of Certified Public Accountants. Retrieved from https://www.kscpa.org/writable/files/Self-Study/AAE/12._aae_self-study.pdf

The Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214, codified as amended at 28 U.S.C.A. §§241-2266.

The Association of Certified Fraud Examiners (ACFE). (2016). Law: The civil justice system [Microsoft PowerPoint file]. Retrieved from http://www.acfe.com/uploadedFiles/ACFE_Website/Content/review/examreview/09-Law-Civil-Securities-Money.pdf

The Association of Chartered Certified Accountants (ACCA). (n.d.). Forensic accounting. Retrieved from http://www.accaglobal.com/za/en/student/exam-support-resources/professional-exams-study-resources/p7/technical-articles/forensic-accounting0.html

Bealing, W. E., Staley, A. B., & Russo, C. J. (2006). Personality: What it takes to be an accountant. *The Accounting Educators' Journal,* XVI, 119-128.

Beebe, L. R. (2016, October 13). Gotcha! How forensic accounting brought about the downfall of Al Capone. Bond Beebe Accountants & Advisors. Retrieved from

http://www.bbcpa.com/gotcha-how-forensic-accounting-brought-about-the-downfall-of-al-capone/

Bender, R. & Alessi, C. (2016, July 25). Munich shooter likely bought gun on 'dark net.' *The Wall Street Journal.* Retrieved from the ProQuest Central database.

Beneish, M. D. (1997). Detecting GAAP violation: Implications for assessing earnings management among firms with extreme financial performance. *Journal of Accounting and Public Policy,* 16 (3), 271-309/ doi: 10.1016/S0278-4254(97)00023-9

Bilbeisi, K. M. & Brown, R. T. (2015). How forensic accounting is used to combat terrorism in the United States. *The Forensic Examiner.* Retrieved from http://www.theforensicexaminer.com/2015/Bilbeisi_Brown_777.php

Boim v. Holy Land Foundation, 549 F.3d 685 (7th Cir., 2008).

Botha, A. E. (2009). The net worth method as technique to quantify income during investigation of financial crime [Master's dissertation]. Retrieved from http://uir.unisa.ac.za/bitstream/handle/10500/3305/dissertation_botha_a.pdf?sequence=1

Bures, O. (2013). Public-private partnerships in the fight against terrorism? *Crime, Law and Social Change,* 60, 429-455. doi: 10.1007/s10611-013-9457-7

Central Intelligence Agency. (n.d.). Careers & internships. Retrieved from https://www.cia.gov/careers/opportunities/analytical

Choo, K. K. R. (2009). Money laundering and terrorism financing risks of prepaid cards instruments? *Asian Criminology,* 4, 11-30. doi: 10.1007/s11417-008-9051-6

Chong, A. & Lopez-de-Silanes, F. (2015). Money laundering and its regulation. *Economics & Politics,* 27(1), 78-123. doi: 10.1111/ecpo.12051

Collins, J. C. (2017). Using Excel and Benford's law to detect fraud. *Journal of Accountancy.* Retrieved from https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html.

Crumbley, D. L., Heitger, L. E., & Smith, G. S. (2007). *Forensic and investigative accounting* (3rd ed.). Chicago, IL: CCH.

Curry, M. (2013). Forensic accounting and terrorism. *African Journal of Accounting, Auditing and Finance,* 2(3), 199-208.

Deloitte. (n.d.). Vision, values and strategy. Retrieved from https://www2.deloitte.com/az/en/pages/about-deloitte/articles/vision-values-strategy.html

Department of Homeland Security. (n.d.). How to turn your education and experience into a career with DHS. Retrieved from https://www.dhs.gov/homeland-security-careers/turning-education-and-experience-career

Department of Justice. (2017, May 2). Statement of James B. Comey, Director, Federal Bureau of Investigation before the Committee on the Judiciary, United States Senate [Transcript]. Retrieved from https://www.judiciary.senate.gov/imo/media/doc/05-03-17%20Comey%20Testimony.pdf

Dietel v. Day, 492 P.2d 455 (16 Ariz. App. 206, 1972).

Dorrell, D. D., & Gadawski, G. A. (2005). Financial forensics II. *The United States Attorneys' Bulletin,* 53(3), p. 1-16, 49-64.

Ducas, E. & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal,* 72(4), 538-562.

Electricity Information Sharing and Analysis Center (E-ISAC). (2016, March 18). Analysis of the cyber attack on the Ukrainian power grid. Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

European Central Bank. (2012). *Virtual currency schemes*. Retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

EY. (n.d.). Our values. Retrieved from http://www.ey.com/us/en/about-us/our-values/2020-vision_our-values culture/our-values.html

Garlick, J., Shurden, S. & Shurden, M. (2013). Can the dominant trait indicator predict success in a financial accounting principles course? *Journal of Modern Accounting and Auditing.* 9(5), 602-608.

Gurulé, J. (2008). *Unfunding terror: The legal response to the financing of terror.* Northampton, MA: Edward Elgar Publishing, Inc.

Higgins, S. (2017, December 30). From $900 to $20,000: Bitcoin's historic 2017 price run revisited. *Coindesk.com*. Retrieved from https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited/

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., …Verdugo,Yepes, C. (2016, January). *Virtual currencies and beyond: Initial considerations.* IMF Discussion Note. Retrieved from https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Virtual-Currencies-and-Beyond-Initial-Considerations-43618

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). (2016, February 25). Alert (IR-ALERT-H-16-056-01): Cyber-attack against Ukrainian critical infrastructure. Retrieved from https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Institute for Economics & Peace. (2017). *Global terrorism index*. Retrieved from http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf

International Convention for the Suppression of the Financing of Terrorism, Article I, paragraph 1. The United Nations (1999).

Jung, C. G. (1971). *Psychological Types.* Princeton, NJ: Princeton University Press.

Koh, J. (2006). *Suppressing terrorist financing and money laundering.* New York: Springer.

Kovar, S. E., Ott, R. L. & Fisher, D. G. (2003). Personality preferences of accounting students: A longitudinal case study. *Journal of Accounting Education*, 21, 75-94.

KPMG. (n.d.). Our values. Retrieved from https://home.kpmg.com/ca/en/home/about/values-culture/our-values.html

Landauro, I. (2016, January 11). Air France-KLM says Paris attacks cost $76 million in lost revenue. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/air-france-klm-puts-cost-of-nov-paris-attacks-at-76-million-1452500645

Laqueur, W. (2007). Terrorism: A brief history. *Foreign Policy Agenda,* 12(5), 20-23.

Leung, R. (2004, November 12). Bin Laden expert steps forward. *CBS News.* Retrieved from https://www.cbsnews.com/news/bin-laden-expert-steps-forward-12-11-2004/

Levitt, M. A. (2002). The political economy of Middle East terrorism. *Middle East Review of International Affairs,* 6(4), 49-65.

Mantone, P. S. (2013). *Using analytics to detect possible fraud.* Hoboken, NJ: John Wiley & Sons Inc.

Mantone, P. S. (2017). *The importance of professional skepticism* [Microsoft PowerPoint Presentation], Knoxville, TN.

Martin, C. R. (1997). *Looking at Type: The Fundamentals.* Gainesville, FL: Center for Application of Psychological Type, Inc.

McCraw, S. C. (2003). Testimony before the Senate Judiciary Committee [Transcript]. The Federal Bureau of Investigation. Retrieved from https://archives.fbi.gov/archives/news/testimony/international-drug-trafficking-and-terrorism

Messier, W. F., Glover, S. M., & Prawitt, D. F. (2017). *Auditing and assurance services: A systematic approach (10th ed.).* New York: McGraw-Hill Education

"Myers-Briggs Type Indicator Grid." KONA. (n.d.). Retrieved from https://www.kona.com.au/myer-briggs-type-indicator-mbti/

National Commission on Terrorist Attacks upon the United States. (2004). Appendix A: The financing of the 9/11 plot. *Terrorist Financing Staff Monograph.* Retrieved from https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_App.pdf

National Council of Resistance of Iran v. Department of State, 373 F.3d 152, 157-58 (D.C.Cir.2004).

Nigrini, M. (1999). I've got your number. (CPA use of Benford's law of mathematics in discovering fraud). *Journal of Accountancy,* 187(5).

Oswick, C. & Barber, P. (1998). Personality type and performance in an introductory accounting course. *Accounting Education,* 7(3), 249-254.

Parker, M. & Taylor, M. (2010). Financial intelligence: A price worth paying? *Studies in Conflict & Terrorism*, 33(11).

Pistole, J. S. (2003). *Before the House Committee on Financial Service Subcommittee on Oversight and Investigations* [Transcript]. Retrieved from

https://archives.fbi.gov/archives/news/testimony/the-terrorist-financing-operations-section.

PwC. (n.d.). Our Purpose. Retrieved from https://www.pwc.com/us/en/about-us/purpose-and-values.html

Ramsay, A., Hanlon, D. & Smith, D. (2000). The association between cognitive style and accounting students' preference for cooperative learning: An empirical investigation. *Journal of Accounting Education,* 18, 215-228.

Raphaeli, N. (2003). Financing of terrorism: Sources, methods, and channels. *Terrorism and Political Violence,* 15(4), 59-82. doi: 10.1080/09546550390449881

Rayman, G. (2015, December 16). Chattanooga rampage was a terrorist attack, FBI says. *New York Daily News.* Retrieved from http://www.nydailynews.com/news/crime/chattanooga-rampage-terrorist-attack-fbi-article-1.2467954

Reuter, P. & Truman, E. M. (2004). *Chasing dirty money: The fight against money laundering.* Washington D.C.: The Institute for International Economics.

Reuters Staff. (2017, December 14). Prosecutors say Long Island woman tried to use bitcoin to aid Islamic State. *Reuters.* Retrieved from https://www.reuters.com/article/us-usa-arrest-new-york-bitcoin/prosecutors-say-long-island-woman-tried-to-use-bitcoin-to-aid-islamic-state-idUSKBN1E83DI

Rosand, E. & Millar, A. (2017, January 31). How the private sector can be harnessed to stop violent extremism. *Brookings.* Retrieved from https://www.brookings.edu/blog/order-from-chaos/2017/01/31/how-the-private-sector-can-be-harnessed-to-stop-violent-extremism/

"Solving scarface." (2005, March 28). *FBI Stories.* Retrieved from https://archives.fbi.gov/archives/news/stories/2005/march/capone_032805

Schloemer, P. G. (2015). Personality preferences and success in introductory accounting. *Academy of Business Disciplines Journal,* 7(1), 53-62.

Schmid, A. & Jongman, A. (1988). *Political terrorism: A new guide to actors, authors, concepts, data bases, theories, and literature.* Amsterdam: North Holland Publishing Co.

Singleton, T. W. & Singleton, A. J. (2010). *Fraud accounting and forensic accounting.* Hoboken, NJ: John Wiley & Sons. Inc.

Smith, J., & Cooper, G. (2009). Disrupting terrorist financing with civil litigation. (The World Conference on Combating Terrorist Financing). *Case Western Reserve Journal of International Law*, 41(1).

Swain, M. R. & Olsen, K. J. (2012). From student to accounting professional: A longitudinal study of the filtering process. *Issues in Accounting Education*, 27 (1), 17-52. doi: 10.2308/iace-50076

Terletska, R. (2018, February 12). US Senate reviewing bill calling for assessment of cryptocurrency terror threat. *Cryptocurrency News.* Retrieved from https://www.ccn.com/us-senate-reviewing-bill-calling-for-assessment-of-cryptocurrency-terror-threat/

Terror financing: Tracking the money trails. (2013, July 5). *FBI News.* Retrieved from https://www.fbi.gov/news/stories/terror-financing-tracking-the-money-trails1

Tie, R. (2010). Sniffing for cooked books. *Fraud Magazine.* Association of Certified Fraud Examiners. Retrieved from http://www.fraud-magazine.com/article.aspx?id=4294968446

Trussel, J.M. (2017). *ProFound: In-depth Financial Analysis* [Microsoft Excel Workbook].

United States Department of State. (n.d.). Foreign terrorist organizations. Retrieved from https://www.state.gov/j/ct/rls/other/des/123085.htm

U.S. v. Abdirahman Sheikh-ali Isse, 342F.3d 313 (4th Cir. 2003)

U.S. Securities Exchange Commission. (2003, March 20). Litigation Release No. 18044. SEC Charges HealthSouth Corp., CEO Richard Scrushy with $1.4 Billion Accounting Fraud. Retrieved from https://www.sec.gov/litigation/litreleases/lr18044.htm

U.S. Securities Exchange Commission. (2001, May 15). Securities Act 1933 Release No. 7976. Retrieved from https://www.sec.gov/litigation/admin/33-7976.htm.

Virtual ticket to prison. (2017, May 3). *FBI News.* Retrieved from https://www.fbi.gov/news/stories/fraud-scheme-leads-to-illegal-bitcoin-exchange

Volastro, A. (2014, January 23). CNBC explains: How to mine bitcoins on your own. *CNBC News.* Retrieved from https://www.cnbc.com/2014/01/23/cnbc-explains-how-to-mine-bitcoins-on-your-own.html

Ward, A. (2018, January 22). Bitcoin and the dark web: The new terrorist threat? *Rand Corporation*. Retrieved from https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html

Appendix

Table 1. Ratios assist forensic accountants in evaluating and identifying red flags in financial statement data. A summary of significant ratio analysis functions can be found below. This is an adapted list from J.M. Trussel's *ProFound: In-depth Financial Analysis* ©2017.

Liquidity Ratios	
Current Ratio	Current Assets ÷ Current Liabilities
Quick Ratio	(Cash + Cash Equivalents + Marketable Securities + Accounts Receivable) ÷ Current Liabilities.
Cash Ratio	Cash and Cash Equivalents ÷ Current Liabilities
Average Collection Period	365 ÷ Accounts Receivable Turnover
Days' Inventory on Hand	365 ÷ Average Inventory
Operating Cycle	Average Collection Period + Days' Inventory on Hand
Asset Management (Activity)	
Accts. Receivables Turnover	Net Sales ÷ Average Accounts Receivable
Inventory Turnover	Cost of Goods Sold ÷ Average Inventory
Payables Turnover	Net Sales ÷ Average Accounts Payable
Working Capital Turnover	Net Sales ÷ Average Working Capital
Fixed Asset Turnover	Net Sales ÷ Average Fixed Assets
Total Asset Turnover	Net Sales ÷ Average Total Assets
Profitability Ratios	
Gross Profit Margin	Gross Profit ÷ Net Sales
Return on Sales	Operating Profit ÷ Net Sales
Return on Assets	Net Income ÷ Average Total Assets
Pretax Return on Assets	Net Operating Income Before Income Taxes ÷ Average Total Assets
Return on Equity	Net Income ÷ Average Total Shareholder's Equity
Dividend Payout	Dividends Paid ÷ Net Income
Leverage/Solvency Ratios	
Debt to Equity	Total Liabilities ÷ Total Shareholder's Equity
Debt to Assets	Total Liabilities ÷ Total Assets
Interest Coverage	Income Before Income Taxes and Interest Expense ÷ Interest Expense
LT Debt to Equity	Long-term Liabilities ÷ Total Shareholder's Equity
Debt to Market Equity	Total Liabilities ÷ (Market Value per Share * Average Shares)
Market Ratios	
Price-Earnings Ratio	Market Value per Share ÷ Diluted Earnings per Share
Book Value per Share	Total Shareholder's Equity ÷ Average Shares
Market to Book Ratio	Market Value per Share ÷ Book Value Per Share
Dividend Yield	(Dividends Paid ÷ Average Shares) ÷ Market Value per Share
Sales to Market Value	Net Sales ÷ (Market Value per Share * Average Shares)
Cash Flow Ratios	
CFO to Income	Net Cash from Operating Activities ÷ Net Income
CFO to Liabilities	Net Cash from Operating Activities ÷ Total Liabilities
CFO per Share	Net Cash from Operating Activities ÷ Average Shares
Cash Flow Adequacy	Net Cash from Operating Activities ÷ Net Cash Required for Investing Activities