Accountants’ perceptions regarding fraud detection and prevention methods

James L. Bierstaker
Department of Accountancy, College of Commerce and Finance, Villanova University, Villanova, Pennsylvania, USA

Richard G. Brody
School of Business, University of South Florida, St Petersburg, Florida, USA, and

Carl Pacini
Department of Accounting and Finance, College of Business, Florida Gulf Coast University, Ft Myers, Florida, USA

Abstract

Purpose – The purpose of this study is to examine the extent to which accountants, internal auditors, and certified fraud examiners use fraud prevention and detection methods, and their perceptions regarding the effectiveness of these methods.

Design/methodology/approach – A survey was administered to 86 accountants, internal auditors and certified fraud examiners.

Findings – The results indicate that firewalls, virus and password protection, and internal control review and improvement are quite commonly used to combat fraud. However, discovery sampling, data mining, forensic accountants, and digital analysis software are not often used, despite receiving high ratings of effectiveness. In particular, organizational use of forensic accountants and digital analysis were the least often used of any anti-fraud method but had the highest mean effectiveness ratings. The lack of use of these highly effective methods may be driven by lack of firm resources.

Practical implications – Organizations should consider the cost/benefit tradeoff in investing in highly effective but potentially underutilized methods to prevent or detect fraud. While the costs may seem prohibitive for small organizations, substantial cost savings from reduced fraud losses may also be significant.

Originality/value – By identifying methods that work well for fraud detection and prevention, prescriptive information can be provided to accounting practitioners, internal auditors, and fraud examiners.

Keywords Internal auditing, Fraud, Accountants

Paper type Research paper

Introduction

Recent corporate financial accounting scandals (e.g. Enron, WorldCom, Global Crossing, Tyco, etc.) have increased concerns about fraud, wiped out billions of dollars of shareholder value, and led to the erosion of investor confidence in financial markets (Peterson and Buckhoff, 2004; Rezaee et al., 2004). Globally, the average estimated loss per organization from economic crimes is $2,199,930 over a two-year period (PriceWaterhouseCoopers (PWC), 2003). In the USA, the Association of Certified Fraud Examiners (ACFE) estimates that about six percent of firm revenues, or $660 billion, is
lost per year as the result of occupational fraud (Association of Certified Fraud Examiners, 2004).

Although larger businesses are more likely to experience economic crime, fraud may be more costly for small businesses (Thomas and Gibson, 2003; PriceWaterhouseCoopers (PWC), 2003). The average small business fraud amounted to $98,000 per occurrence compared to $105,500 per incident for large companies (Association of Certified Fraud Examiners, 2004). On a per employee basis, losses from fraud can be as much as 100 times greater at small firms than large firms (Association of Certified Fraud Examiners, 2004; Wells, 2003). In addition, the damage inflicted by fraud goes beyond direct monetary loss. Collateral damage may include harm to external business relationships, employee morale, firm reputation, and branding (PriceWaterhouseCoopers (PWC), 2003). In fact, some of the collateral effects of fraud, such as damage to firm reputation, can be long-term (PriceWaterhouseCoopers (PWC), 2003). Despite the increased incidence of fraud and enactment of new anti-fraud laws, many organizational anti-fraud efforts are not current and are somewhat superficial (Andersen, 2004). Hence, many entities are trying new and different steps to combat fraud (KPMG Forensic, 2003; PriceWaterhouseCoopers (PWC), 2003).

One reason that entities of all types are taking more and different steps to fight fraud is that the traditional red flags approach is not considered effective. The well-known red flags approach involves the use of a checklist of fraud indicators. The existence of red flags does not portend the presence of fraud but represents conditions associated with fraud; they are cues meant to alert an auditor to the possibility of fraudulent activity (Krambia-Kardis, 2002). Numerous commentators have cast doubt on the red flags approach as it suffers from two limitations:

1. red flags are associated with fraud, but the association is far from perfect, and
2. since it focuses attention on specific cues it might inhibit internal and external auditors from identifying other reasons that fraud could occur (Krambia-Kardis, 2002).

In fact, critics of SAS 99 – Consideration of Fraud in a Financial Statement Audit – point to its heavy reliance on the red flags approach (Kranacher and Stern, 2004).

A second reason that organizations are trying more and different ways to attack fraud is that most entities have used an impractical strategy of fraud detection (Wells, 2004). Fraud prevention is a more viable strategy since it is often difficult to recover fraud losses once they are detected (Wells, 2004). Many companies and their auditors deal with fraud on a case-by-case basis rather than implement a long-term plan. Also, recent legislation such as the Sarbanes-Oxley Act of 2002 (SOX) does not do much in terms of fraud prevention; instead, the law focuses on punishment and accountability (Andersen, 2004).

In the Fall 1997 issue of the Auditor’s Report, the American Accounting Association (AAA) encouraged research directed toward assisting auditors and investigators in preventing and detecting fraud. The growth in fraud cases indicates that a strong need exists for research approaches that better enable auditors and investigators to prevent and detect potential fraud. Thus, the purposes of this study are to analyze and understand accountants’ perceptions of the myriad techniques used to combat fraud, shed light on whether the techniques actually used by firms are considered the most
effective and offer suggestions to practitioners as to what prevention and detection techniques are the “best.” Organizational management attempting to comply with SOX and similar laws by launching new anti-fraud programs, as well as external and internal auditors, will benefit from this study’s findings, when considering which anti-fraud methods to pursue. The benefits consist of less time spent on the use of ineffective techniques and reduction of fraud risk through earlier implementation of more effective fraud prevention and detection techniques.

The remainder of this paper is organized as follows. The next section reviews past research addressing fraud detection and prevention methods. The third section discusses various techniques for combating fraud. The fourth section presents the design of the study. The fifth section analyzes the results and the last section concludes the paper.

Literature review

Much prior research addressing fraud prevention and detection methods has addressed “red flags.” For example, Albrecht and Romney (1986) found in a survey of practicing auditors that 31 flags related to internal control were considered better predictors of fraud. The survey contained a list of 87 red flags. Loebbecke and Willingham (1988) offered a model that considers the probability of material financial statement misstatement due to fraud as a function of three factors:

1. the degree to which those in authority in an entity have reason to commit management fraud;
2. the degree to which conditions allow management fraud to be committed; and
3. the extent to which those in authority have an attitude or set of ethical values that would facilitate their commission of fraud.

Loebbecke and Willingham (1989) used the red flags approach to develop another conceptual model to evaluate fraud probability. A survey instrument was used to query 277 audit partners of a big 6 firm. These researchers concluded that an auditor’s assessment of the client’s internal controls is significant in evaluating the probability of fraud. Pincus (1989) found that auditors who did not employ red flag checklists outperformed those who did in an experimental setting. In another study, auditors were found to hold different opinions concerning the degree of fraud risk indicated by various red flag indicators. Auditors with different client experience were found to possess different perceptions of the importance of a given red flag indicator (Hackenbrack, 1993).

Other researchers have investigated the effectiveness of various audit procedures in detecting fraud. Hylas and Ashton (1982) performed an empirical study of 281 errors requiring financial statement adjustments on 152 audits. These researchers found that analytical review procedures and discussions with clients predicted a large percentage of errors. Wright and Ashton (1989) investigated the fraud detection effectiveness of client inquiry, expectations based on prior years, and analytical reviews from a sample of 186 engagements involving 368 proposed audit adjustments. These researchers discovered that about half of the errors were signaled by the three procedures noted.

Blocher (1992) determined that only four out of 24 fraud cases were signaled by analytical procedures. Calderon and Green (1994) found that analytical procedures were the initial signal in 15 percent of 455 fraud cases. Kaminski and Wetzel (2004)
performed a longitudinal examination of various financial ratios on 30 matched pairs of firms. Using chaos theory methodology, metric tests were run to analyze the behavior of time-series data. These researchers found no differences in the dynamics between fraudulent and non-fraudulent firms providing evidence of the limited ability of financial ratios to detect fraud. Apostolou et al. (2001) surveyed 140 internal and external auditors on the fraud risk factors contained in SAS 82. They document management characteristics as the most significant predictor of fraud followed by client operating/financial stability features, and industry conditions. Chen and Sennetti (2005) apply a limited, industry-specific strategic systems auditing lens and a logistic regression model to a matched sample of 52 computer firms accused of fraudulent financial reporting by the SEC. The model achieved an overall prediction rate of 91 percent for fraud and non-fraud firms.

Moyes and Baker (2003) conducted a survey of practicing auditors concerning the fraud detection effectiveness of 218 standard audit procedures. Results indicate that 56 out of 218 procedures were considered more effective in detecting fraud. In general, the most effective procedures were those yielding evidence about the existence and/or the strength of internal controls.

**Methods to combat fraud**

Both fraudulent financial reporting and asset misappropriation have become major costs for many organizations. Numerous fraud prevention and detection techniques are now utilized to reduce the direct and indirect costs associated with all forms of fraud. These various techniques include but are not limited to: fraud policies, telephone hot lines, employee reference checks, fraud vulnerability reviews, vendor contract reviews and sanctions, analytical reviews (financial ratio analysis), password protection, firewalls, digital analysis and other forms of software technology, and discovery sampling (Carpenter and Mahoney, 2001; Thomas and Gibson, 2003). Organizations that have not been fraud victims tend to rely more on intangible prevention tools such as codes of conduct or fraud reporting policies while those that have suffered fraud have implemented more tangible measures such as whistle-blowing policies and fraud prevention and detection training (PriceWaterhouseCoopers (PWC), 2003).

**Maintain a fraud policy**

Every organization should create and maintain a fraud policy for guiding employees. A corporate fraud policy should be separate and distinct from a corporate code of conduct or ethics policy. A model or sample fraud policy is available from the ACFE. Such a fraud policy should be clearly communicated to employees. Various avenues of communication include use in orientation of new hires, employee training seminars, and annual performance evaluations. Written acknowledgment by each employee that the policy has been read and understood should be required.

**Establish a telephone hotline**

A rather novel fraud approach that is becoming more common is the use of anonymous telephone hotlines (Holtfreter, 2004). It is a very cost effective means for detecting occupational fraud and abuse. A hotline allows employees to provide confidential, inside information without the fear of reprisal that accompanies being a whistleblower (Pergola and Sprung, 2005).
Hotlines may be supported in-house or provided by a third party. An example of a third-party hotline is a subscription service offered by the ACFE. The annual subscription rate may be quite modest. The results of all calls are provided to the client within two or three days. A hotline is not only an effective detection tool but it also enhances deterrence. Potential perpetrators will likely have second thoughts when considering the risks of being caught.

**Employee reference checks**

Organizations should conduct employee reference checks prior to employment. An employee with a history of perpetration of fraud schemes may move from one organization to another. When employee references are not checked, a dishonest person may be hired. A dishonest employee can defraud an unsuspecting organization of thousands of dollars and move on to a new job before the fraud is discovered. Resumes should be scrutinized and information verified to determine that the information provided is legitimate. An organization should not rely on the telephone numbers listed on the resume for prior employers, as they may be false. Employer phone numbers should be obtained by the organization independently.

Organizations should conduct a second reference check six months after an employee starts work. The reason for a dishonest employee’s recent dismissal from a previous job may not have had time to become part of the employee’s record during the initial search. This may be discovered by a second check.

**Fraud vulnerability reviews**

A fraud vulnerability review that investigates the organization’s exposure to fraud should be performed. This includes an assessment of what assets are held and how they could be misappropriated. For those organizations involved in electronic commerce, a vulnerability review should also include an assessment of exposure to employee misappropriation or destruction of such “non-balance” sheet items as confidential customer data and financial information. The purpose of such a review is to “outsmart the crooks.” A vulnerability review can help to direct an internal audit plan and, in particular, to highlight the most vulnerable assets. The review is considered a proactive step in fraud prevention and detection. Consideration of each class of asset and the evaluation of the exposure to loss helps the auditor or accountant to see what the thief sees. Steps then should be taken to eliminate, minimize, or at least control the exposures.

**Perform vendor contract reviews**

Review of company contracts and agreements can provide an indication of possible contract fraud, including kickbacks, bribery, or conflicts of interest by an organization’s employees. Contract fraud can occur when a trade supplier fraudulently takes advantage of a contract to make illegal profits. Contract fraud may involve a conspiracy between entity personnel and a trade supplier or conspiracy among two or more vendors.

Analyzing contract files for the same contractor routinely bidding last, bidding lowest, or obtaining the contract may detect this type of contract fraud. Awarded contracts may also be scrutinized for evidence of a supplier regularly being awarded contracts without indication of a legitimate reason for the constant receipt of contract.
awards. Such a review may reveal that bribes or kickbacks are the reason for the awards. A review of various public records may reveal whether an employee has a covert ownership interest in the contractor.

Use analytical review
Fraud can affect financial statement trends and ratios. Accounts that are manipulated to conceal a fraud may manifest unusual relationships with other accounts that are not manipulated. Also, erratic patterns in periodic account balances may occur because the fraudster may engage only sporadically in fraudulent activity. Financial analysis conducted by an accountant or investigator may reveal existing relationships that are not expected or the absence of relationships that are expected to be present.

It may behoove the accountant or investigator to analyze several years of financial statement data using different techniques to obtain a clear picture of the financial impact of any fraud scheme. Various analytical review techniques which the accountant or investigator may employ include: trend (horizontal) analysis, ratio analysis (vertical analysis or common size statements), budgetary comparisons, comparisons with industry averages, and review of general ledger and journal entries. Unusual items should be pursued to determine if fraud could be the cause of an aberration.

Password protection
The growth of the internet and e-commerce has led to a rise in the number of dial-in ports to computer networks thus increasing the exposure to fraud. Accountants and investigators should assure that only legitimate users have access to the computer network and associated data. Although passwords are the oldest line of computer defense, they still constitute the most effective and efficient method of controlling access.

The difficulty with passwords is that there is an inverse relationship between making the password effective and usable. If password requirements are too complex, users will write the password down, placing it at risk (Gerard et al., 2004). Therefore, every organization needs to evaluate the tradeoffs. Passwords should be six to eight characters long with a mix of letters, numbers and special symbols. Users should be required to change their password often, for example, every 30-60 days. Additionally, users should have to cycle through 6-12 different passwords before being allowed to reuse a password (Gerard et al., 2004). Also, employees should not be allowed to display their passwords in any location where unauthorized individuals may see them. Lockout procedures should be implemented if a user fails to input a correct password after three attempts.

Technology has advanced to create new forms of password protection using biological features of the user (i.e. biometrics) such as voiceprints, fingerprints, retina patterns, and digital signatures. New forms of password protection are likely to become cost effective in the near future.

Firewall protection
One necessary technique for controlling unauthorized access is the use of firewalls. Firewalls can be used at the software or hardware level. At the software level, there are specific programs (e.g. ZoneAlarm from zonelabs.com) that can be coordinated with internet-related software programs (browsers, e-mail, etc.) to protect the data being
Hardware firewalls/routers basically prevent people from finding an organization’s connection to the internet. The internet connection is known as an IP address. The hardware firewall/router basically hides the IP address so that hackers cannot find and access it (Gerard et al., 2004).

**Digital analysis**

Digital analysis, which is based on Benford’s Law, tests for fraudulent transactions based on whether digits appear in certain places in numbers in the expected proportion. A significant deviation from expectations occurs usually under two conditions. The first condition is that a person has added observations on a basis that does not conform to a benford distribution. The second condition is that someone has deleted observations from a data set that does not adhere to a benford distribution (Durtschi et al., 2004).

Tax cheats, check forgers, and embezzlers simply cannot consciously generate random numbers. Forensic accountants and auditors have depended on this human quirk for years and various types of digital analysis software, including DATAS, have proven themselves capable of pinpointing this habit (Lanza, 2000). A list of examples of data sets where digital analysis software may be used includes investment sales/purchases, check registers, sales and price histories, 401 (k) contributions, inventory unit costs, expense accounts, wire transfer information, life insurance policy values, bad debt expenses, and asset/liability accounts.

Other types of fraud exist that cannot be detected by digital analysis because the data sets under examination are not appropriate for such analysis. For example, duplicate addresses or bank accounts cannot be uncovered, yet two employees with similar addresses might signal a shell company. Digital analysis will not detect such frauds as contract rigging, defective deliveries, or defective shipments.

**Discovery sampling**

Discovery sampling is a form of attribute sampling. The latter is a statistical means of estimating the percentage of a population that possesses a particular characteristic or attribute. Discovery sampling is based on an expected error rate of zero. It is employed when the accountant needs to know whether a population contains any error indicative of fraud. If a single case of significant error or fraud is found in a sample, the sampling process is stopped and the error or fraud is investigated.

Let us consider an example. An account should not include any payments made out to a vendor name that is known to be fictitious unless there is that type of fraud in the account. If there is no such fraud in the account, there should be no payments to fictitious vendors. If an auditor were to test some of the payments in an account and were to find a payment made out to a fictitious vendor, the auditors would know that fraud existed but would not know the extent of the fraud. Conversely, if an accountant examined some account payments and did not find any illegitimate payments, he or she would not conclude that no fictitious payments existed in the account.

We now turn to a discussion of the study’s participants.

**Study participants**

The participants of this study consist of 86 accountants, internal auditors and certified fraud examiners with a mean (standard deviation) of 13.94 (10.97) years of experience[1].
In an attempt to obtain as many responses as possible, multiple methods were used to collect the information. Of the 86 usable responses, approximately 40 percent were received via a mail survey sent to practicing accountants in the USA, 15 percent were obtained from individuals in an executive MBA program at a New England university, 15 percent were completed by volunteers recruited from the IIA and ACFE websites and 30 percent were collected from two participating IIA chapters[2]. Sixty-eight percent of the participants are male, 32 percent are female. Sixty-two percent hold a bachelor’s degree, thirty-four percent have a master’s degree, and four percent have education beyond a master’s degree. Twenty-nine percent of the participants are certified public accountants, 22 percent are certified internal auditors, 16 percent are certified fraud examiners, 8 percent are certified managerial accountants and eight percent are certified information systems auditors. The remaining participants did not provide their certification, if any. Forty percent of the accountants work at firms whose revenues exceed one billion dollars, about 28 percent work at firms with revenues between 250 million and one billion dollars, 22 percent work at firms with revenues below 250 million dollars, and 10 percent did not respond. Participants come from a wide range of industries including: insurance (13 percent), health care (7 percent), banking (5 percent), retail (5 percent), utilities (5 percent), manufacturing (5 percent), government (5 percent), pharmaceuticals (5 percent) financial services (4 percent), education (4 percent) and many others. None of the participants worked at a CPA firm.

In terms of the entities’ scope of operations, 34 percent of survey participants are from local organizations, 22 percent are from national organizations, and 41 percent are from international organizations, and 3 percent did not indicate the scope of operations. Fifty-three percent of participants are from publicly held companies (44 percent listed on the New York Stock Exchange), while 47 percent work at privately held companies. About 4 percent of survey participants come from companies without an internal audit department, 47 percent have an internal audit department with 1-8 members, 20 percent have an internal audit department with 10-19 internal auditors, and 29 percent have departments with 20 or more internal auditors. Overall, participants are diverse in terms of their years of experience, certifications held, industry background, scope of operations, and internal audit department size. A summary of these results is contained in Table I.

### Results

**Fraud victimization and funding for prevention**

About 56 percent of the survey participants indicated their company had been a victim of fraud, with 24 percent indicating their company had not been a victim of fraud and 20 percent indicating they did not know whether or not their company was a fraud victim. Fifty-two percent of participants expected fraud to increase in the future, while 30 percent did not expect fraud to increase and 18 percent did not know.

Forty-eight percent of participants indicated funding for fraud prevention training had increased over the last three years, while 45 percent said it remained the same and only 8 percent said it decreased. Similarly, 56 percent indicated funding for the internal audit department had increased over the past three years, while 39 percent indicated internal audit funding had remained the same and only five percent stated it had decreased.
Use and effectiveness of fraud prevention methods and software

Based on a review of the fraud literature for types of fraud procedures (Carpenter and Mahoney, 2001; Coderre, 1999; KPMG, 1998; Albrecht et al., 2002), auditors were asked to indicate whether their firms used the following fraud prevention and detection procedures and software: corporate code of conduct/ethics policy, internal control review, reference checks, employment contracts, fraud auditing, fraud reporting policy, fraud vulnerability reviews, fraud hotline, whistle-blowing policy, operational audits, forensic accountants, fraud prevention training, ethics training, surveillance equipment, increased attention of management, code of sanctions against suppliers, increased role of audit committee, surveillance of electronic correspondence, staff rotation, security department, employee counseling programs, cash reviews, inventory observation, bank reconciliations, ethics officer, discovery sampling, data mining, digital analysis, continuous auditing, financial ratios, virus protection, password protection, firewalls, and filtering software (Appendix 1). In addition, auditors were asked to rate the effectiveness of anti-fraud procedures and software used in their organization on a scale from 1 (completely ineffective) to 7 (completely effective).

As shown in Table II, fraud procedures and software are ranked from the most frequently used (virus protection, firewalls, password protection, internal control review, and improvement) to the least frequently used (forensic accountants, digital analysis, staff rotation, employment contracts, data mining). Differences clearly exist between the use of fraud procedures and software. Firewalls, virus protection, password protection, and internal control review are the most common (97-99 percent) and organizational use of forensic accountants is the least common (14 percent). Differences also exist for participants’ ratings of effectiveness. Organizational use of forensic accountants received the highest mean rating (5.86) while staff rotation received the lowest mean rating (3.84). It is interesting to note that organizational use of forensic accountants was the least often used method to combat fraud (14 percent), but received the highest rating of effectiveness (5.86). These findings suggest that firms
may wish to consider investing in forensic accountants in the future if they have not already done so.

In addition, other methods of combating fraud that involve software, such as discovery sampling, data mining, continuous auditing, and digital analysis were not commonly used. Mean effectiveness ratings, however, were relatively high, ranging from 4.96 for discovery sampling to 5.37 for data mining. While none of these fraud software applications were used by the majority of the participants’ organizations, three of them ranked in the top ten for effectiveness (digital analysis, continuous auditing, and data mining) and a fourth ranked in the top fifteen (discovery sampling). Therefore, while firms may be reluctant to invest in anti-fraud technology, the perceived benefits of the software may outweigh the cost given their apparent effectiveness.

Table II.

<table>
<thead>
<tr>
<th>Fraud procedure</th>
<th>Percentage</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Virus protection</td>
<td>99</td>
<td>5.66 (2)</td>
</tr>
<tr>
<td>2. Firewalls</td>
<td>97</td>
<td>5.63 (3)</td>
</tr>
<tr>
<td>3. Password protection</td>
<td>97</td>
<td>5.35 (6)</td>
</tr>
<tr>
<td>4. Internal control review and improvement</td>
<td>97</td>
<td>4.96 (13)</td>
</tr>
<tr>
<td>5. Operational audits</td>
<td>94</td>
<td>4.83 (17)</td>
</tr>
<tr>
<td>6. Corporate code of conduct/ethics policy</td>
<td>94</td>
<td>4.83 (18)</td>
</tr>
<tr>
<td>7. Reference checks on employees</td>
<td>85</td>
<td>4.75 (23)</td>
</tr>
<tr>
<td>8. Bank reconciliations</td>
<td>84</td>
<td>5.22 (9)</td>
</tr>
<tr>
<td>9. Increased attention of senior management</td>
<td>79</td>
<td>4.85 (16)</td>
</tr>
<tr>
<td>10. Filtering software</td>
<td>78</td>
<td>5.38 (4)</td>
</tr>
<tr>
<td>11. Fraud hotline</td>
<td>75</td>
<td>4.63 (26)</td>
</tr>
<tr>
<td>12. Cash reviews</td>
<td>74</td>
<td>4.83 (19)</td>
</tr>
<tr>
<td>13. Whistle-blowing policy</td>
<td>73</td>
<td>4.58 (28)</td>
</tr>
<tr>
<td>14. Fraud reporting policy</td>
<td>72</td>
<td>4.73 (24)</td>
</tr>
<tr>
<td>15. Employee counseling programs</td>
<td>70</td>
<td>4.00 (32)</td>
</tr>
<tr>
<td>16. Increased role of audit committee</td>
<td>70</td>
<td>4.98 (12)</td>
</tr>
<tr>
<td>17. Ethics training</td>
<td>69</td>
<td>4.76 (22)</td>
</tr>
<tr>
<td>18. Inventory observation</td>
<td>66</td>
<td>4.68 (25)</td>
</tr>
<tr>
<td>19. Security department</td>
<td>65</td>
<td>4.26 (30)</td>
</tr>
<tr>
<td>20. Fraud auditing</td>
<td>64</td>
<td>5.28 (8)</td>
</tr>
<tr>
<td>21. Surveillance of electronic correspondence</td>
<td>62</td>
<td>4.52 (29)</td>
</tr>
<tr>
<td>22. Financial ratios</td>
<td>57</td>
<td>4.81 (20)</td>
</tr>
<tr>
<td>23. Continuous auditing</td>
<td>52</td>
<td>5.35 (7)</td>
</tr>
<tr>
<td>24. Fraud prevention and detection training</td>
<td>52</td>
<td>4.92 (15)</td>
</tr>
<tr>
<td>25. Fraud vulnerability reviews</td>
<td>50</td>
<td>4.59 (27)</td>
</tr>
<tr>
<td>26. Surveillance equipment</td>
<td>48</td>
<td>4.78 (21)</td>
</tr>
<tr>
<td>27. Code of sanctions against suppliers/contractors</td>
<td>43</td>
<td>5.08 (11)</td>
</tr>
<tr>
<td>28. Ethics officer</td>
<td>42</td>
<td>3.90 (33)</td>
</tr>
<tr>
<td>29. Discovery sampling</td>
<td>42</td>
<td>4.96 (14)</td>
</tr>
<tr>
<td>30. Data mining</td>
<td>41</td>
<td>5.37 (5)</td>
</tr>
<tr>
<td>31. Employment contracts</td>
<td>37</td>
<td>4.23 (31)</td>
</tr>
<tr>
<td>32. Staff rotation policy</td>
<td>32</td>
<td>3.84 (34)</td>
</tr>
<tr>
<td>33. Digital analysis</td>
<td>23</td>
<td>5.22 (10)</td>
</tr>
<tr>
<td>34. Organizational use of forensic accountants</td>
<td>14</td>
<td>5.86 (1)</td>
</tr>
</tbody>
</table>

Note: Software in italic
Accountants’ use of effective but infrequently used anti-fraud methods was also analyzed based on the amount of firm revenues. It was expected that firms with greater revenues would have more resources to devote to technology and fraud prevention, thus accountants’ use of these methods should be greater at larger firms. As shown in Table III, one clear pattern that emerges is that accountants at firms with revenues of more than $1 billion did use discovery sampling, data mining, digital analysis, continuous auditing, and forensic accountants more than smaller firms. These results support the notion that smaller companies are reluctant to invest in anti-fraud technology because of concerns about cost. Nevertheless, smaller entities may be the most in need of fraud detection and prevention technology, since fraud may be more costly for small businesses than large ones (Thomas and Gibson, 2003; Association of Certified Fraud Examiners, 2002; Wells, 2003).

An alternative explanation is that larger firms are more likely to be publicly held and may be investing more to combat fraud in response to Sarbanes-Oxley. While it is true that the majority of firms with revenues over $1 billion are publicly held (80 percent), the majority of firms with revenues between $250 million and 1 billion are also publicly held (57 percent), yet their use of discovery sampling, digital analysis, continuous auditing, and forensic accountants was quite similar to smaller firms. Therefore, it would appear that firm resources appears to be the primary driver behind investments in highly effective anti-fraud methods such as organizational use of forensic accountants and digital analysis.

### Conclusion

This study investigated the extent to which accountants, internal auditors, and certified fraud examiners use various fraud prevention and detection methods and software, as well as their perceptions about the effectiveness of those techniques. The results suggest that firewalls, virus and password protection, and internal control review and improvement are quite commonly used to combat fraud. However, continuous auditing, discovery sampling, data mining, forensic accountants, and digital analysis software are less often used, despite receiving the high ratings of effectiveness. In particular, organizational use of forensic accountants was the least often used of any anti-fraud method but had the highest mean effectiveness rating. Smaller firms (less than $1 billion in revenues) appear to be the most reluctant to invest in fraud prevention and detection methodology. This may be due to concerns about

<table>
<thead>
<tr>
<th>Fraud tool</th>
<th>Overall use percentage (percent)</th>
<th>Revenues &gt; $1 billion (percent)</th>
<th>Revenues between $250 million and 1 billion (percent)</th>
<th>Revenues &lt; $250 million (percent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous auditing</td>
<td>52</td>
<td>71</td>
<td>39</td>
<td>36</td>
</tr>
<tr>
<td>Discovery sampling</td>
<td>42</td>
<td>68</td>
<td>27</td>
<td>31</td>
</tr>
<tr>
<td>Data mining</td>
<td>41</td>
<td>72</td>
<td>31</td>
<td>8</td>
</tr>
<tr>
<td>Digital analysis</td>
<td>23</td>
<td>41</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Forensic accountants</td>
<td>14</td>
<td>20</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

**Table III.** Percentage of accountants who use anti-fraud methods by firm revenues
cost, even though a fraud occurrence may be more costly for small businesses than
does not occur (Thomas and Gibson, 2003; Association of Certified Fraud Examiners, 2002;
Wells, 2003). The results indicate that even at larger firms, anti-fraud methods and
software may by under-utilized.

This study has practical implications for accounting practitioners, internal auditors,
and fraud examiners. It provides prescriptive information on what fraud detection and
prevention methods work best, and suggests that many of the most effective methods are
often not being used. Accounting practitioners and management may wish to consider
investing in these methods in order to prevent costly frauds in their organizations and
respond to the demands of regulatory agencies and legal requirements such as those
imposed by the Sarbanes-Oxley Act of 2002. Regulators may also find these results of
interest. For example, codes of conduct and whistleblower programs are now required by
SOX. The cost/benefit tradeoff in mandating organizational use of forensic accountants
may be an issue worthy of consideration by regulators.

Future research could explore the use of fraud prevention and detection methods by
other members of the accounting profession such as external auditors and tax
practitioners. In addition, future research could gather data on practitioners’ suggestions
for improving the usefulness of fraud prevention and detection methods, and the reasons
why firms are reluctant to invest in anti-fraud technology and forensic accountants. For
example, firms may be concerned about the costs of these methods, but may underestimate
the potential benefits in terms of cost savings from reduced losses related to fraud.

Notes
1. Participants level of experience was not correlated with the results of interest.
2. The method of data collection did not affect the statistical significance of the results at
   conventional levels.

References
or suffer the consequences”, Journal of Accountancy, April, pp. 30-34.
Corporate Legal Times, April, pp. 1-6.
Association of Certified Fraud Examiners (2002) Report to the Nation: Occupational Fraud and
Abuse, Austin, TX.
Association of Certified Fraud Examiners (2004) Report to the Nation: Occupational Fraud and
Abuse, Austin, TX.
Blocher, E. (1992), The Role of Analytical Procedures in Detecting Management Fraud, Institute of
Management Accountants, Montvale, NJ.
Calderon, T.G. and Green, B.P. (1994), “Signaling fraud by using analytical procedures”, Ohio
April, pp. 33-38.


KPMG Forensic (2003), *Fraud Survey 2003*, Montvale, NJ.


Appendix 1. Fraud questionnaire

Purpose
The purpose of this survey is to gather data relating to the use of fraud detection and prevention techniques. It should take approximately 10 minutes to complete. Thank you in advance for your voluntary participation. It indicates your willingness to contribute to the enhancement of our profession. All responses you provide are confidential and will be published only in summary, statistical form. You or your firm will not be identified in any way. Accordingly, there are no foreseeable risks to you or your firm.

Respondent profile
Job Title ____________________________________________
Gender __________ Age __________
Highest educational level obtained: Bachelor Degree__ Masters Degree__ Coursework beyond Masters ________
Years of accounting experience________
Certification: ________ ________ ________ ________ ________ ________ ________ ________ ________ ________
   CIA CPA CISA CMA CFE CFP Other
Number of Auditors in Internal Audit Department:________
Primary Industry ____________________________
Revenue for 2002: < 250 mm______ > 250 mm-1 billion______ > billion ______
Operations: Local_____ National_____ International_____
Is your company publicly held? Yes______ No______
If yes, which of the following exchanges is your company listed on? NYSE__ AMEX__ NASDAQ__ OTC__ Other__ (please identify__).

Fraud questions: Please answer the questions below to the best of your ability. All answers will be held in confidence.
1. Do you expect fraud to increase in the future? Yes______ No______ Don’t know______
If so, why?
2. Has your firm been a victim of fraud? Yes______ No______ Don’t know______
If so, for how long? ______years What were the amount of the damages? $________
3. If you have an internal audit department, whom do they report to? __Board of Directors
   __Controller __CFO __CEO __Other (Please identify__) Don’t know__
4. Is management at your firm accountable to the same fraud standards as non-management employees? __Yes __No __Don’t know__
5. How important would you say your external auditors are for fraud detection?
   1 2 3 4 5 6 7
Not very important Somewhat important Very important
6. How much pressure would you say is placed on employees at your organization to meet firm objectives?
   1 2 3 4 5 6 7
Little Some A great deal
7. If you have an internal audit department, how has the funding for this department changed over the past three years?
   1 2 3 4 5 6 7
Decreased Same Increased
8. How has the funding for fraud prevention training changed over the past three years?

1 2 3 4 5 6 7
Decreased  Same  Increased

9. How would you assess the likelihood of fraud in your organization? ______ percent.

10. How many times does your audit committee meet per year? ______ Don’t know______

**Fraud detection techniques.** Please indicate below what steps you have taken to reduce the possibility of fraud in your organization and the perceived effectiveness of each step for preventing/detecting fraud from 1 (completely ineffective) to 7 (completely effective).

**Fraud detection techniques (continued).** Please indicate below what steps you have taken to reduce the possibility of fraud in your organization and the perceived effectiveness of each step for preventing/detecting fraud from 1 (completely ineffective) to 7 (completely effective).

**Fraud technology:** Please indicate below what technology you use to reduce the possibility of fraud in your organization and the perceived effectiveness of each application for preventing/detecting fraud from 1 (completely ineffective) to 7 (completely effective). In the case of software, indicate the name of the software and whether it was internally or externally developed.

Thank you!

<table>
<thead>
<tr>
<th>Fraud procedure</th>
<th>Yes/No</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate code of conduct/ethics policy</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Internal control review and improvement</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Reference checks on employees</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Employment contracts</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Fraud auditing</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Fraud reporting policy</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Fraud vulnerability reviews</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Fraud hotline</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Whistle-blowing policy</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Operational audits</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Organizational use of forensic accountants</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Fraud prevention and detection training</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Ethics training</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Surveillance equipment</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Increased attention of senior management</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Code of sanctions against suppliers/contractors</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Increased role of audit committee</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
</tbody>
</table>

**Table AI.**

<table>
<thead>
<tr>
<th>Fraud procedure</th>
<th>Yes/No</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surveillance of electronic correspondence</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Staff rotation policy</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Security department</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Employee counseling programs</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Cash reviews</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Inventory observation</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Bank reconciliations</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Ethics officer</td>
<td>Yes/No</td>
<td>1 2 3 4 5 6 7</td>
</tr>
</tbody>
</table>

**Table AII.**
<table>
<thead>
<tr>
<th>Fraud software</th>
<th>Yes/No</th>
<th>Internally or externally developed</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery sampling</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Data mining</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Digital analysis</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Continuous auditing</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Financial ratios</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Virus protection</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Password protection</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Firewalls</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Filtering software</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Other (Please identify other audit applications that are completed with a software package)</td>
<td>Yes/No</td>
<td>Internal</td>
<td>1 2 3 4 5 6 7</td>
</tr>
</tbody>
</table>

Table AIII.

**Corresponding author**
James L. Bierstaker can be contacted at: James.Bierstaker@villanova.edu
This article has been cited by:

2. Sawsan Saadi Halbouni. 2015. The Role of Auditors in Preventing, Detecting, and Reporting Fraud: The Case of the United Arab Emirates (UAE). *International Journal of Auditing* n/a. [CrossRef]