

Fraud in US Organisations: An Examination of Control Mechanisms

Kristy Holtfreter

INTRODUCTION

According to estimates from a recent US survey, approximately 6 per cent of 2002 revenues were lost through fraud committed by employees.¹ When considered in the context of the US gross domestic product (GDP), this figure translates to nearly \$600bn in losses. These alarming statistics underscore the need for a thorough assessment of methods that organisations can utilise to detect and prevent fraud from within. This study focuses on a form of white-collar/occupational crime, occupational fraud, defined as: 'The deliberate misuse of one's occupation for personal enrichment through the misapplication of the employing organisation's resources or assets.'² Consistent with prior white-collar crime research, occupational fraud is conceptualised as an act that violates trust.³

Using data from 663 occupational fraud cases in four US organisational settings (ie government agencies, non-profit agencies, private businesses, and publicly traded companies), the study evaluates whether the presence of internal control mechanisms impacts organisations' median dollar losses from fraud. Implications for future research and fraud prevention in organisations are discussed.

LITERATURE REVIEW

A variety of offences referred to as 'white-collar crime' occur in organisations. One such offence is fraud. Fraud may take the form of 'corporate crime', which directly benefits the organisation and may have a wide variety of victims, or 'occupational crime', which benefits the individual perpetrator and victimises the employing organisation.⁴ In the USA, fraud studies have focused disproportionately on corporate crime. Because of difficulties in obtaining white-collar crime data, studies of occupational crime (eg fraud) are often restricted to a single organisation.

One exception in which researchers included data from multiple organisations is the series of studies on fraud in the US savings and loan industry during the 1990s.⁵ While little is known about how fraud varies in other US organisational settings, the literature

suggests that certain organisations may be more vulnerable to fraud. For example, a recent study revealed that fraud by managers occurred more often in 'transportation, communication and publishing, retail and wholesale, and gaming, tourism and recreational services', while fraud by employees was more common in financing and insurance businesses as well as property and construction.⁶ Clearly, research focusing on occupational fraud in a variety of settings has important implications for fraud control and prevention.

Controlling and preventing fraud

To prevent and detect fraud by employees, US organisations may use a number of methods. Control mechanisms generally take one of two forms: (1) those that are implemented at the pre-employment stage to screen out potentially questionable applicants, and (2) methods that take place during the course of employment to prevent fraud from occurring or to detect fraud in progress.⁷

One common, early stage strategy is the background check.⁸ Depending on the organisation and the particular job for which a person applies, the type of background check performed can vary considerably. For instance, if the employee interviews well and appears acceptable 'on paper', the check may consist solely of a verbal (ie phone call) investigation of reported prior employment history. Organisations may ask previous employers about the applicant's reasons for leaving the former job to determine whether he or she was suspected of fraud. Some organisations may take a stricter stance, and perform checks that also include criminal history information. This technique can reveal whether the applicant has previous criminal or civil fraud-related convictions, signalling a possible problem. A limitation of this technique is that, unlike offenders who commit violent crimes, the majority of fraudsters are 'first time' offenders with no criminal history. Although they may have committed fraud, many individuals either were not caught for their crimes, or were fired by a previous employer; in both situations, there would be no official criminal record.⁹ As Riddle describes, some organisations that regularly require employees to handle and

account for cash (eg banks) also perform financial credit history checks on applicants. This strategy may reveal whether the potential employee is experiencing serious financial hardship, another sign that engaging in fraud is more likely. Research suggests that in addition to the pre-employment screening phase, organisations would also benefit from conducting regular checks (eg criminal and credit) during the course of employment to determine whether current employees exhibit new behaviour indicative of occupational fraud.¹⁰

The audit function is also a widely used organisational defence against fraud.¹¹ According to Hemraj's research, 'the audit is not intended to target the existence of fraud' but by design, it is capable of detecting irregularities and assuring they are not the product of fraudulent transactions.¹² Depending on the organisation, audits can be performed internally (eg by an accounting or audit department) or externally (eg by an outside consultant or firm). Organisations regularly conduct audits through the course of standard operating procedures, but may also do so in response to suspicions of fraud. Like other control mechanisms, the effectiveness of audits varies based on several factors. For instance, in a recent case study of employee thefts in a large department store, long-term audits of three months' duration allowed management to clearly identify theft patterns that were previously unrecognisable when daily reports (eg cash register tapes and end-of-shift records) were examined.¹³ This study also revealed that increasing the number of regular audits at locations throughout the store's separate departments was beneficial in documenting 'normal' activity as a means of detecting subsequent 'abnormal' activity more easily.

In addition to background checks and audits, a rather novel fraud control approach that is becoming more common in the USA is the use of anonymous reporting to encourage employees to turn in co-workers who commit fraud.¹⁴ Through procedures such as toll-free, off site 'hotlines', employees can provide confidential, inside information without the fear of retaliation that often accompanies the prospective whistleblower. Other potentially devastating consequences for whistleblowers include the possibility of legal action for slander.¹⁵ Given the many negative outcomes for whistleblowers, anonymous reporting mechanisms provide a protective barrier with the goal of encouraging and ultimately increasing reports of fraud. Since anonymous reporting mechanisms are a fairly new form of control, little is

known about their success in detecting fraud. However, existing research suggests that, if accompanied by positive support from management, hotlines can be an effective deterrent.¹⁶

Although there has been a substantial amount of research on the mechanisms used to prevent and detect occupational fraud, no studies have compared multiple control mechanisms. Prior research is often limited to describing a control mechanism (eg the audit) and then determining its effectiveness. Previous studies on control mechanisms tend to be restricted to a single organisational setting, resulting in no knowledge of how the effectiveness of specific mechanisms differs based on the type of organisation. To bridge the gap in the literature, the present study examines four types of control mechanisms (ie anonymous reporting, background checks, internal audits and external audits) in four US organisational settings (ie government agencies, non-profit agencies, private businesses and publicly traded companies). The organisations ranged in size from less than 100 to 10,000 or more employees. The analysis considers the effect of each control mechanism on median fraud losses in each setting.

METHODOLOGY

This study uses data originally collected by the Association of Certified Fraud Examiners (ACFE). The ACFE is a professional organisation focused on the prevention of white-collar crime, specifically occupational fraud. ACFE uses information from four areas: criminology and ethics, financial transactions, fraud investigation, and legal elements of fraud to provide training and assistance to over 30,000 members worldwide.

Sample and procedures

The sample was drawn from occupational fraud cases that were investigated by Certified Fraud Examiners (CFEs) who responded to a 2001–02 survey. In an earlier, exploratory study, ACFE established baseline measures of fraud, and developed a system for classifying occupational fraud cases. All respondents were CFEs, and were employed in three main industries: government, business, and public accounting. Respondents' primary occupations included: auditor (37 per cent), fraud investigator (27 per cent), accountant (23 per cent) and law enforcement (13 per cent). They had an average of approximately 19 years of work experience in fraud investigation.

Data collection began in April 2001 and ran through February 2002. A six-page questionnaire was distributed by mail to randomly selected CFEs. The sample was restricted to the USA to control for the types of legal responses (eg civil, criminal). A total of 971 CFEs provided usable survey responses, and, of these, 663 cases involved occupational fraud.¹⁷ Participation in the study was voluntary, but CFEs were offered two hours of Continuing Professional Education (CPE) credit for their participation.¹⁸ Each respondent was asked to provide detailed information on the most recent single, completed fraud case he or she had investigated. This included a narrative explanation of how the fraud was committed. This information was used to group cases based on the original occupational fraud classification system. Detailed information about the organisations, perpetrators, and resulting legal proceedings was also provided.

FINDINGS

Types of fraud

All forms of occupational fraud are clandestine, violate the employee's fiduciary duties to the organisation, are committed for the purpose of direct or indirect financial benefit to the perpetrator, and cost the employing organisation assets, revenues, or reserves. Apart from these shared elements, the cases are divided into

three distinct categories based on their characteristics. Asset misappropriation included thefts of cash or other inventory. Asset misappropriation was the most common, comprising 85.5 per cent of cases. Examples ranged from skimming small amounts of cash from a register to larger-scale embezzlements. A second category, fraudulent statements, involved falsification of financial documents (eg overstating revenue or understating liabilities) or other documents (eg employee records), and included 8.7 per cent of the cases. Finally, corruption involved 5.7 per cent of the cases. Employees who committed corruption wrongfully used their influence in business transactions to obtain personal benefits contrary to their duties to the organisation. Table 1 presents the offender characteristics and median fraud losses in each setting.

Internal control mechanisms

Respondents were asked to report on the type and number of control mechanisms organisations had access to for detecting and/or preventing fraud. The available mechanisms included anonymous reporting (eg fraud hotlines), background checks, internal audit departments, and external audits (eg by a Certified Public Accountant). For the entire sample, victim organisations had an average of 1.8 existing control mechanisms. The type and number of controls varied by the organisational setting. For each setting, the median fraud losses are compared for organisations

Table 1: *Offender characteristics and median dollar loss by organisational setting (n = 663)*

<i>Victim</i>	<i>Offender</i>	<i>Median loss</i>
Government agency	Age: 43; Gender: 55.8% male & 44.2% female; Position: 66% employee & 34% manager or executive; Education: 55.6% high school, 32.7% bachelor's degree, 11.7% graduate degree	\$48,000
Non-profit agency	Age: 43; Gender: 44.6% male, 55.4% female; Position: 65.2% employee & 34.8% manager or executive; Education: 52.8% high school, 32.6% bachelor's degree, 14.6% graduate degree	\$40,000
Private business	Age: 39; Gender: 47.9% male, 52.1% female; Position: 56.7% employee; 43.3% manager or executive; Education: 60.6% high school, 32.2% bachelor's degree, 7.2% graduate degree	\$127,000
Publicly-traded company	Age: 40; Gender: 60.7% male, 39.3% female Position: 52.6% employee; 47.4% manager or executive Education: 55.2% high school, 34.4% bachelor's degree, 10.4% graduate degree	\$150,000

Table 2: Control mechanisms and comparison of median fraud losses by organisational setting

	Background checks		Anonymous reporting		Internal audit		External audit	
	Y	N	Y	N	Y	N	Y	N
Government agency	\$44K*	\$31K	\$41K	\$40K	\$36K	\$46K	\$42K	\$40K
Non-profit agency	\$40K	\$45K	\$45K	\$60K	\$40K	\$75K	\$30K	\$70K
Private business	\$100K	\$150K	\$78K	\$150K	\$75K	\$156K	\$92K	\$153K
Publicly-traded company	\$100K	\$100K	\$76K	\$250K	\$95K	\$400K	\$100K	\$129K

*K = 1000 US dollars

with and without control mechanisms, to determine whether the control mechanisms work equally well or vary across different organisational settings. Table 2 summarises these findings.

TYPES OF ORGANISATIONS

Government agencies

Approximately one-fourth of victims (24.7 per cent or 162) were government agencies. Like the sample as a whole, the types of fraud that occurred in government agencies consisted primarily of asset misappropriation (84 per cent or 136 cases), followed by fraudulent statements (10.5 per cent or 17 cases) and corruption (5.6 per cent or 9 cases). The median fraud loss in government agencies was \$48,000. The average offender age was approximately 43.3 years. The majority of perpetrators in this setting were male (55.8 per cent) with the remaining 43.3 per cent female. The findings for age and gender are consistent with many prior studies of white-collar offenders.¹⁹ Most perpetrators were lower level employees (66 per cent) rather than managers or executives (who comprised 34 per cent of the group). The largest percentage of perpetrators had a high school education (55.6 per cent); followed by 32.7 per cent with a bachelor's degree, and the smallest percentage with a graduate degree (11.7 per cent). In terms of position and level of education, these individuals more closely resemble David Weisburd and co-authors' 'middle class' offenders, as opposed to 'high-status' offenders.²⁰

Several control mechanisms were in place in the sub-sample of government agencies. Not surprisingly, a slight majority of government agencies (60.7 per cent) performed background checks on new

employees. Nearly half of the agencies (48.9 per cent) had some form of anonymous reporting, such as a fraud hotline. Most had an internal audit department (68.6 per cent) and the majority (79.4 per cent) of agencies were audited externally. Compared with government agencies with background checks, those who did not use this mechanism actually experienced lower median fraud losses (\$31,000 vs \$44,000, respectively). This unexpected finding may be explained by previous research suggesting that white-collar perpetrators are often first time offenders without criminal records.²¹ If this is true in the current sample, practising background checks would not significantly influence hiring potential fraudsters. Additionally, this result corresponds to an Associated Press review of US government agencies, which found that over half of the states failed to determine whether contractors were barred from doing business with the federal government due to fraud.²² It is also possible that non-criminal background checks (eg of prior employment history) were ignored or inconsistently performed, resulting in the hiring of employees with questionable but unknown characteristics.²³

In government agencies with anonymous reporting mechanisms, the median fraud loss of \$41,000 was slightly higher than in government agencies without them, who experienced median losses of \$40,000. This result implies that employees are more willing to report fraudulent activity of co-workers if it involves a greater dollar loss. External audits produced a similar finding: government agencies that were externally audited had median losses of \$42,000 while those without external audits had median losses of \$40,000. This result should not be interpreted negatively, as it suggests that external audits may simply discover more extensive losses from fraud.

For government agencies, the only control mechanism associated with smaller losses was internal audits. As Table 2 shows, in government agencies with internal audit departments, the median loss was approximately \$36,000, compared with \$46,000 in agencies without internal audits. This suggests that occupational fraud is discovered earlier when internal audits are performed, resulting in significantly lower dollar losses. This finding also implies that internal audits are followed according to agencies' guidelines, especially compared with the other control mechanisms.

Non-profit agencies

A total of 89 organisational victims (13.4 per cent) were non-profit agencies. In this setting, the types of fraud committed differed slightly from the sample as a whole. Nearly all of the cases reported (96.6 per cent) were classified as asset misappropriation, with the remaining cases classified as fraudulent statements (2.2 per cent) and corruption (1 per cent). The median fraud loss in non-profit agencies was approximately \$40,000. The average age of perpetrators, 42.9 years, was similar to government agency fraudsters. However, unlike government agencies, the majority of perpetrators in non-profit agencies were female (55.4 per cent) with the remaining 44.5 per cent male. The positions of these offenders consisted of 65.2 per cent who were working as lower-level employees and 34.8 per cent as managers or executives. The frequencies for gender and position, as well as the lower median fraud loss, are similar to previous research demonstrating that female white-collar offenders are situated in lower level jobs.²⁴ The distribution of perpetrators' education levels was similar to offenders in government agencies: over half (52.8 per cent) had high school diplomas, nearly one-third had bachelor's degrees (32.6 per cent) and 14.6 per cent had graduate degrees.

Compared with government agencies, non-profit agencies had fewer control mechanisms. Just over one-third (36.1 per cent) performed background checks, and a small percentage (16.4 per cent) had anonymous reporting mechanisms available. Additionally, while only 38.8 per cent had an internal audit department, the majority (77.6 per cent) were audited externally. Across all non-profit agencies, the median fraud losses were lower for agencies with each respective control mechanism. Non-profit agencies with background checks experienced median losses of \$40,000, compared to \$45,000 in those without background checks. This result suggests that, in this type of agency, background checks are

practised consistently, or may also include procedures that detect non-criminal indicators of fraud (eg financial history of applicants).²⁵

The difference in fraud losses was even greater for anonymous reporting: in non-profit agencies with this mechanism in place, median losses were \$45,000, in contrast to \$60,000 in agencies without this practice. Compared with government agencies, perhaps individuals working for non-profit agencies are motivated to turn in their criminal co-workers at the earliest signs of fraud, resulting in lower losses. In agencies with internal audit departments, the median dollar loss was approximately \$40,000. Comparatively, those agencies without internal audits had considerably greater losses at \$75,000, a finding consistent with this control mechanism's effect in government agencies. The loss difference exhibited for external audits paralleled that of internal audits: non-profit agencies that were audited externally suffered median losses of \$30,000, while their non-audited counterparts had losses of \$70,000. In this particular organisational setting, it appears that external control mechanisms are utilised on a regular basis, revealing early-stage frauds before dollar losses become substantial. In sum, the presence of each control mechanism in non-profit agencies corresponded to lower median fraud losses.

Private businesses

Privately owned businesses comprised the largest group (208 or 31.9 per cent) of organisational victims. Like government agencies, private businesses were victimised most often by asset misappropriation (88.9 per cent), followed by fraudulent statements (6.7 per cent) and corruption (4.3 per cent). Unlike government agencies and non-profit agencies, however, the median fraud loss in private businesses was considerably greater at \$127,000. The average age of perpetrators (approximately 39 years) was youngest in private businesses. Similar to the findings for non-profit agencies, a slight majority of perpetrators in private businesses were also female (52.1 per cent) with the remaining 47.9 per cent male. This setting had a sizeable percentage of lower level employees (56.7 per cent) but the percentage of managers or executives (43.3 per cent) was greater than those in government agencies or non-profit agencies. This finding may explain the higher median fraud loss in this setting: compared to employees, managers and executives have increased access to organisations' financial procedures, resulting in increased opportunities for fraud.²⁶ Perpetrators' education levels

included 60.6 per cent with high school degrees, nearly one-third (32.2 per cent) with bachelor's degrees, and 7.2 per cent with graduate degrees.

Approximately one-third (31 per cent) of private businesses practised employee background checks, and an even smaller percentage (18.8 per cent) had some type of anonymous reporting mechanism. These findings are not surprising given that private businesses also tend to have fewer employees, and as a result, they may have less available resources to implement a variety of control mechanisms. Internal audit departments were present in 32.1 per cent of private businesses, but external audits were performed in over half of these businesses (53.3 per cent).

While the percentages of private businesses with each control mechanism were relatively low, the presence of each respective mechanism corresponded to a notably smaller median fraud loss. For private businesses with background checks, the median loss of \$100,000 was approximately \$50,000 less than in businesses without such checks. Like non-profit agencies, this result indicates that, when available, background checks are performed consistently, and may also incorporate a variety of safeguards (eg criminal history, credit history and employment history).

A striking outcome also reflective of the findings for non-profit agencies was the comparison for anonymous reporting mechanisms: those who had them experienced median fraud losses of approximately \$78,000, while the losses in those without the method were nearly twice as great (\$150,000). This difference suggests that anonymous reporting mechanisms may be taken more seriously in private businesses than in government agencies. Moreover, it is also possible that fraud hotlines and related procedures are accompanied by factors such as employee training, and support from upper management.²⁷ In private businesses that were externally audited, the median fraud loss was \$92,000 while those without external audits suffered losses of \$153,000. As with the comparisons for non-profit agencies, the availability of each separate control mechanism was associated with reduced median fraud losses. However, the smaller proportion of private businesses with each control mechanism implies that it is not simply the presence of a control that matters, as much as consistent enforcement.²⁸

Publicly traded companies

A total of 192 publicly traded companies (30 per cent) were victimised by occupational fraud. This group

also experienced asset misappropriation most often (78.6 per cent) but had higher percentages of fraudulent statements (11.5 per cent) and corruption (9.9 per cent) than the other three types of organisations. This finding was not unexpected given that fraudulent statements often involve overstating revenue or understating corporate liabilities, which would rarely apply in the other three organisational settings. The median fraud loss of \$150,000 was the highest of any setting. The average age of these perpetrators (40 years) was similar to offenders in private businesses, and slightly younger than those who victimised government agencies and non-profit agencies. The majority of these offenders were male (60.7 per cent) and 39.3 per cent were female. Just over half of the perpetrators were lower-level employees (52.6 per cent) while the remaining 47.4 per cent were managers or executives. Compared to the three other types of organisations, publicly traded companies had the highest percentage of managers or executives as perpetrators, the highest percentage of males, and the greatest median fraud losses, all of which confirm prior white-collar crime research on opportunities for fraud at different levels of the organisational hierarchy.²⁹

A large percentage of publicly traded companies (63.8 per cent) performed background checks on new employees, and over half (52.1 per cent) had some form of anonymous reporting mechanism. The overwhelming majority (80 per cent) also had an internal audit department, and an even higher percentage (85.9 per cent) was audited externally. The presence of each form of control mechanism produced some noteworthy differences. As the table shows, background checks had a null effect, with equal losses of \$100,000 across all publicly traded companies. However, the comparisons for the other three mechanisms represent the strongest differences in median fraud losses across all four types of organisations. While publicly traded companies with anonymous reporting experienced losses of \$76,000, companies without it had a median fraud loss of approximately \$250,000. In this setting, the presence of a non-public, unidentifiable means of turning in co-workers may result in earlier detection of fraud, restricting the dollar loss.

The difference was also vast for external audits: companies that were audited lost \$100,000, while those without this practice lost \$129,000. Finally, the most remarkable difference was between publicly traded companies with and without internal audit

departments: those with this mechanism suffered median fraud losses of \$95,000, while their counterparts had median fraud losses over four times greater, at \$400,000. The findings suggest that companies with internal audit departments, as well as those who are audited externally, may catch occupational fraud earlier in the process, before it leads to more extensive financial damage. This corroborates previous research findings that the practice of regular audits serves to reduce losses from fraud.³⁰

CONCLUSION

Validating previous research, this study found that the direct costs of occupational fraud are extensive. What is more, related societal outcomes, such as diminished trust in governmental and corporate institutions, reduced consumer confidence, and increases in commercial product prices are also insurmountable, but remain impossible to measure accurately.³¹ This research also revealed that, in the USA, virtually no organisational setting is immune to fraud from within. Organisations must take the necessary steps to detect fraud in progress and also prevent its initial occurrence. Researchers should continue to focus on fraud in a variety of organisational contexts, which will require cooperation with practitioners. Such endeavours will undoubtedly contribute to further development of white-collar crime theory as well as strategic approaches to fraud prevention.

As this study demonstrated, successfully controlling and reducing fraud requires diverse strategies based on the organisational setting. Given the legal system's inconsistent approaches to white-collar offenders, organisations' strict stances toward occupational fraud is especially salient.³² Although a variety of control mechanisms may be available to organisations, this study found that access alone does not curb dollar losses. Control mechanisms are never a guaranteed organisational defence if they are overridden or ignored, a situation referred to in the literature as a 'non-control' factor.³³ To effectively combat fraud, implementing control strategies remains an obvious step, but consistently following practices and enforcing organisational policies is even more vital.

REFERENCES

- (1) Association of Certified Fraud Examiners (2002) *Report to the Nation*, Austin, TX.
- (2) *Ibid.*
- (3) Shapiro, S. (1990) 'Collaring the Crime, Not the Criminal: Reconsidering the Concept of White-Collar Crime', *American Sociological Review*, Vol. 55, pp. 346–365.
- (4) Clinard, M. B. and Quinney, R. (1967) *Criminal Behavior Systems: A Typology*, Holt, Rinehart, and Winston, New York.
- (5) Calavita, K., Pontell, H. N. and Tillman, R. (1997) *Big Money Crime: Fraud and Politics in the Savings and Loan Crisis*, University of California Press, Berkeley, CA; Calavita, K. and Pontell, H. N. (1990) 'Heads I Win, Tails You Lose: Deregulation, Crime, and Crisis in the Savings and Loan Industry', *Crime and Delinquency*, Vol. 36, pp. 309–341; Calavita, K. and Pontell, H. N. (1990) 'Other People's Money Revisited: Collective Embezzlement in the Savings and Loan and Insurance Industries', *Social Problems*, Vol. 39, pp. 94–112; Tillman, R. and Pontell, H. N. (1985) 'Organizations and Fraud in the Savings and Loan Industry', *Social Forces*, Vol. 73, pp. 1439–1463.
- (6) Krambia-Kapardis, M. (2002) 'Fraud Victimisation of Companies: The Cyprus Experience', *Journal of Financial Crime*, Vol. 10, No. 2, pp. 184–191.
- (7) Riddle, K. (1999) 'Unbuttoning White-Collar Crime', *Security Management*, Vol. 45, No. 1, pp. 57–63.
- (8) *Ibid.*
- (9) Albrecht, W. S. (2003) *Fraud Examination*, Thompson-Southwestern, Mason, OH.
- (10) Riddle, ref. 7 above.
- (11) Hemraj, M. (2002) 'The Detection of Financial Irregularities in US Corporations', *Journal of Financial Crime*, Vol. 10, No. 1, pp. 85–90.
- (12) Hemraj, ref. 11 above.
- (13) Osborn, C. (1998) 'Restructuring to Reduce Losses', *Security Management*, Vol. 42, No. 12, pp. 63–68.
- (14) Flesher, D. (1999) 'Attitudes Toward Whistle-Blowing Hotlines', *Phi Kappa Phi Forum on Business and Economics*, Vol. 79, No. 2, pp. 5–6.
- (15) Latimer, P. (2002) 'Reporting Suspicions of Money Laundering and "Whistleblowing": The Legal and Other Implications for Intermediaries and Their Advisors', *Journal of Financial Crime*, Vol. 10, No. 2, pp. 23–29.
- (16) Lewis, D. (1997) 'Whistleblowing at Work: Ingredients for an Effective Procedure', *Human Resource Management Journal*, Vol. 7, No. 4, pp. 5–12.
- (17) The remaining 308 cases also victimised organisations, but were committed by non-employees (eg vendors, customers) so they were not included in this study of occupational fraud.
- (18) CPE credit contributes to the current status of a CFE's professional licence. Typical opportunities for credit include attendance at workshops or training seminars sponsored by ACFE.
- (19) Wheeler, S., Weisburd, D., Waring, E. and Bode, N. (1988) 'White-Collar Crime and Criminals', *American Criminal Law Review*, Vol. 25, pp. 331–357.
- (20) Weisburd, D., Wheeler, S., Waring, E. and Bode, N. (1991) *Crimes of the Middle-Classes: White-Collar Offenders in the Federal Courts*, Yale University Press, New Haven, CT; Sutherland, E. (1940) *White-Collar Crime*, Dryden Press, New York.
- (21) Albrecht, ref. 9 above.
- (22) Anonymous (2000) 'States Fail to Check for Criminal Records', *Organized Crime Digest*, Vol. 21, p. 4.
- (23) Osborn, ref. 13 above.
- (24) Daly, K. (1989) 'Gender and Varieties of White-Collar Crime', *Criminology*, Vol. 27, pp. 769–793.
- (25) Riddle, ref. 7 above.
- (26) Piquero, N. and Piquero, A. (2001) 'Characteristics and

Sources of White-Collar Crime', in N. Shover and J. P. Wright, *Crimes of Privilege: Readings in White-Collar Crime*, Oxford University Press, Oxford, UK, pp. 329–341.

(27) Flesher, ref. 14 above.

(28) Osborn, ref. 13 above.

(29) Vaughn, D. (2001) 'Transaction Systems and Unlawful Organizational Behavior', in N. Shover and J. P. Wright, *Crimes of Privilege: Readings in White-Collar Crime*, Oxford University Press, Oxford, UK, pp. 136–144; Vaughn, D. (1983) *Controlling Unlawful Organizational Behavior: Social Structure and Corporate Misconduct*, University of Chicago Press, Chicago, IL.

(30) Osborn, ref. 13 above.

(31) Krambia-Kapardis, ref. 6 above.

(32) Croall, H. (2003) 'Combating Financial Crime: Regulatory Versus Crime-Control Approaches', *Journal of Financial Crime*, Vol. 11, No. 1, pp. 45–55.

(33) Albrecht, ref. 9 above.

Kristy Holtfreter, PhD, Assistant Professor, School of Criminology and Criminal Justice, Florida State University, Tallahassee, FL; e-mail: kholtfre@fsu.edu. The author would like to thank Mike Reisig for his helpful comments on an earlier draft.

Commission tells EU member states to implement 2001 framework decision on money laundering in full

A draft report critical of the slow progress by some member states in taking measures to comply with the Council framework decision of 26th June, 2001, on money laundering and the identification, tracing, freezing, seizing and confiscation of instruments and proceeds of crime has been adopted by the European Commission.

The report — sent to the European Parliament, the Council and the European Economic and Social Committee — includes an attachment which summarises the implementing provisions taken by individual member states for each Article of the decision. This concludes that a number of member states still have a long way to go to ensure the rapid and complete transposition of the decision, and the Commission urges them to take the remaining measures as quickly as possible and inform it of action taken no later than 1st September, 2004.

The framework decision was one of the measures identified by the European Council in its declaration on the fight against terrorism adopted on 25th–26th March, 2004.

Article 6 of the decision obliged member states to take the necessary measures to comply with the decision by 31st December, 2002. By 1st March, 2003, member states were required to forward to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations arising for them from the framework decision and, when appropriate, the notifications made under Art. 40(2) of the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime ('The 1990 Convention').

The Council was asked to ascertain, by 31st December, 2003, on the basis of this information and the written report by the Commission, to what extent member states have taken the necessary measures to comply with the framework decision. Not all member states transmitted all relevant texts of their implementing provisions in due time, and two (Austria and Portugal) had not sent any information at all by 1st November, 2003. This has led to the delay in the production of the report by the Commission, and also means that the factual assessment and conclusions drawn are sometimes based on incomplete information.