https://doi.org/10.48009/2_iis_2016_162-169

Issues in Information Systems
Volume 17, Issue II, pp. 162-169, 2016

AN ANALYSIS OF COLLUSION AND SINGLE PERPETRATOR FRAUDS IN RELATION TO INTERNAL CONTROLS

Orion Welch, St. Mary's University, owelch@stmarytx.edu
Tom Madison, St. Mary's University, tmadison@stmarytx.edu
Sandra Welch, University of Texas at San Antonio, sandra.welch@utsa.edu

ABSTRACT

This paper examines data collected via survey pertaining to 43 collusion fraud schemes, and compares them to 117 single perpetrator fraud schemes. The data used were submitted by accountants with direct knowledge of the real fraud occurrences. Properly implemented, strong internal controls should reduce fraud opportunities. The interest of this study was to examine what control weaknesses were identified as stronger contributing factors in collusion schemes versus single perpetrator schemes. The results of this study would be useful to understanding the relative importance internal control systems might play in reducing the opportunity for fraud. This information would be helpful in the design and implementation of preventive controls in information systems

Keywords: Ethics, Fraud, Collusion, Internal Controls, Information Technology Auditing

INTRODUCTION

Internal controls are defined as the policies, plans, and procedures implemented within an organization to protect its assets from risk of fraud. Increasingly, the mechanisms for preventing and detecting fraudulent activity are implemented though controls embedded in the information systems of the organizations. This study of how actual fraud schemes were used to circumvent various internal controls procedures would be useful to the designers of input, processing, and output controls in information systems. The comparison of collusion based schemes, involving multiple perpetrators versus simpler, single perpetrator schemes suggest that multiple layers of internal controls might be necessary to prevent and detect the more complicated collusion based schemes.

According to the Institute of Internal Auditors (1985), an employee, outside individual, or a party representing another entity perpetrates a fraud against an organization for direct or indirect personal benefit. In general, the fraud is undertaken through concealment or misrepresentation of events or data, through making false claims. Although no single study provides a comprehensive theory of fraud, many offer some insight into the complexities of this important issue.

The fraud triangle suggests there are three factors that are associated with management and employee theft of cash or other assets. The first is situational pressure on the perpetrators, most often financial pressure. The second factor is ethics and character weakness. The third factor is opportunity which involves the direct or indirect access to assets.

Inappropriate signals from the organization's leadership may be perceived as condoning or even encouraging unethical behavior (ASB, 2002; Coleman, 1987; Guercio, Rice, and Sherman, 1988; NCFFR, 1987; Soltani, 2014). Additionally, inadequate or missing formal deterrence mechanisms within the unit may exist (COSO, 2011; Cornish and Clarke, 1987; Cressey, 1973; Guercio et al., 1988; Holtfreter, 2005; NCFFR, 1987; PCAOB, 2006; Seidman, 1990; Shapiro, 1990). Albrecht, Abrecht, Albrecht, and Zimbelman (2012) notes collusive frauds appear to be on the rise. They cite the increased complexity of the business environment, and the increased use of vendor alliances that lack paper trails. A 2011 survey conducted by the Association of Certified Fraud Examiners found that 42% of employee frauds involve collusion. Mittendorf (2008) notes that the introduction of ethical personnel can make eliciting ethical behavior among others easier, "unraveling … detrimental norms" that could lead to such behaviors as tacit collusion (p. 365). These factors suggest certain organizational environments may be more conducive to fraud.

Albrecht, Albrecht, and Albrecht (2008) state that "every fraud perpetrator faces … perceived pressure," and that while most involve a financial pressure to perform, "beat the system" or frustration can also provide motivation (p. 3). Dominey, Fleming, Krunacher and Riley (2012) discuss several sociological and psychological antecedents that may motivate fraudulent behavior, e.g., the need to be seen as successful or furtherance of ideological beliefs. Cressey (1973) notes that a perpetrator will have an inherent ethical weakness, but must also possess a structural knowledge of the targeted organization in order to successfully commit the fraud. Further the perpetrator will be able to internally rationalize and justify the fraud. The magnitude of the losses from fraudulent activity has been found to be highly correlated with both the positions held by the perpetrators within the victim organizations (Mann, 1992; Wheeler and Rothman, 1982) and the specific level of responsibility involved (Guercio et al., 1988; Loebbecke, Eining, and Willingham, 1989). Moorthy, Seetharaman, Somasundaram, and Gopalan, (2009) noted that the participation of management in collusive frauds disrupts a major component of control, and Albrecht et al. (2012) and Dominey et al. (2012) note the influence of power on the ability of one person to influence another to participate in a fraud. The literature suggests that middle-aged males in management, who are under financial pressure and/or have a need to appear successful, will be likely candidates to commit fraud. Additionally, they may use their organizational position to convince or coerce subordinates to collude with them, as well as to provide the necessary structural knowledge of the target.

Within accounting literature, inappropriate management attitudes (particularly toward internal controls) have frequently been linked to fraud and its detection (Hooks, Kaplan, and Schultz, 2004; Soltani, 2014; Vinten, 1992). The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2011) states that management concerns for effective internal control must permeate the organization and that "[s]upport from the board of directors and senior management is needed to get the right focus, resources and attention" for enterprise risk management (p. 1). On the basis of a comprehensive review of the literature, Hooks et al. (2004) suggested that codes of conduct have little impact if not enforced. Thompson (1993) noted that when top management displays "willful ignorance, [it] sends a powerful message that it will tolerate [wrongdoing]" (p. 64). Cressey (1973) noted that frauds will occur in an organization when the perpetrator, who lacks the moral strength to resist temptation, is offered an opportunity to commit an offense. Entities that display lax attitudes toward controls offer such opportunities.

Barnard (1938) suggested that top management is responsible for encouraging cooperation in achieving a moral purpose through moral behavior. A strong corporate awareness of the danger of fraud should encourage support for tight internal accounting controls and create a greater sensitivity to the risk factors commonly associated with the commitment of fraud. Additionally, these dynamics should discourage unethical activity, and encourage the reporting of such illicit activities when they do occur. In contrast, organizations that display less awareness to the danger of fraud will provide inadequate support for internal controls. Such an environment might allow, or even encourage, unethical activity by some and discourage the reporting of suspicious activities by others. In sum, positive or strong ethical attitudes modeled by management encourage employee conscientiousness, while lax attitudes may cause reduced employee conscientiousness.

Although fraud perpetrated through collusion is often harder to uncover (Moorthy et al., 2009; Silver, Fleming, and Riley, 2008), and results in significantly higher losses (ACFE, 2014; Wells, 2011), the integrity of an organization's internal control structure, coupled with the effectiveness of the audits (both internal and external) conducted on the organization and its programs, can still have a significant impact on the likelihood that frauds will commence. If they do occur, then proper internal controls (Loebbecke et al., 1989; Matsumura and Tucker, 1992), open channels of communication (Holtfreter, 2005; Hooks et al., 2004), and a pool of sensitive personnel (Guercio, et al., 1988; Poneman, 1994) create important aids to detection and to detection on a timely basis (Holtfreter, 2005). The importance of internal controls as a fraud deterrent was further emphasized following the corporate failures of the early 2000's with the passage of the Sarbanes-Oxley Act of 2002, and the resultant Statement of Auditing Standards 109 in 2006 and Statement of Auditing Standards 115 in 2008. Sarbanes-Oxley was enacted, in part, due to over sixty years of congressional concern regarding the need for public reporting of the effectiveness of internal controls (Gupta et al., 2013) and section 404 explicitly established legal responsibility of corporate governance management for internal controls. As noted the literature suggests that lax attitudes toward internal controls and/or poorly

designed and executed internal controls will be involved in organizational fraud. There is little in the literature to suggest possible differences regarding internal controls in collusive versus non-collusive frauds, other than collusive frauds will facilitate a violation of segregation of duties (Trumpeter, Carpenter, Jones, and Riley, 2014).

Shapiro (1990) notes when a perpetrator can mask illicit behavior, the fraud examination may be both very time-consuming and only partially successful. Silver et al. (2008) describe the difficulty in uncovering collusive fraud, because management overrides weaken the effectiveness of segregation of duties. In many fraud examinations, investigators may need to link several seemingly unrelated situations in order to confirm the existence of fraud. The discrete nature of transactions, coupled with the power commanded by a given perpetrator, may allow the perpetrator to hinder or, in some instances, even block any investigations that do take place. Albrecht et al. (2012) state that descriptive research has shown that perpetrators face legal action in less than half of the cases and the ACFE (2014) estimates that victim organizations have no recovery of losses in over 50% of the frauds referred for legal action. Fraud investigators may be chosen from a variety of disciplines and may include certified fraud examiners (who also hold other positions), legal counsel, internal and external auditors, security personnel, IT personnel, human resource personnel, management and law enforcement (Wells, 2011),

RESEARCH METHODOLOGY

The study examines 43 collusion fraud cases and compares them to 117 single perpetrator fraud cases. The fraud information was collected by a survey distributed to the membership of a professional accounting society in south Texas. The survey consisted of 73 questions that requested detailed information about the perpetrators and fraud schemes. Surveys were sent to approximately 2,000 professional accountants. In order to successfully complete the survey, the accountants had to have significant detailed knowledge of a fraud committed in an organization. A total of 162 fraud case reports met the criterion presenting complete information. The usable response rate was approximately 6%. This response rate percentage might be misleading because the number of accountants surveyed that had detailed knowledge of a fraud case would be a subset of those receiving the survey request. Information from over half of the respondents was based on frauds occurring or that had occurred within two to three years of data collection.

The primary focus of this study was to determine if there was differences in the internal control weaknesses exploited between schemes that were used by single perpetrators versus schemes that involved collusion. The researchers believed this knowledge would be important to designers of computerized internal control systems, auditors, and fraud examiners. Seven common internal control activities were assessed regarding the degree to which a weakness was exploited to commit the crime. They included separation of duties, proper authorization, periodic checks and balances, lax attitudes, asset safeguards, required documentation, and competent personnel. Other questions that were of interest to the researchers included whether there was a difference in management participation, complication of the scheme, and altering of computer records between collusion versus single perpetrator frauds. The researchers suspected that weaknesses in separation of duties and asset safeguards would be a more observed weakness in single perpetrator crimes since collusion schemes often use weaknesses in multiple controls to offset the effect of separation of duties. The researches expected weaknesses related to lax attitudes, lack of competent personnel, absence of required documentation, and missing proper authorization would be more commonly observed in collusion cases. Lax attitudes and exploitation of incompetent personnel would be associated with a higher incidence of management involvement in collusion frauds. Transaction alterations involving authorization and modification of computer record documentation would also be more prevalent due to expected increased complexity of collusion frauds.

RESULTS

The Perpetrators

In addition to reviewing the characteristics of individual perpetrators, we also examined the relationship between collusion partners.. In the cases of collusion, we asked the respondents to identify a primary perpetrator and the secondary perpetrator with whom s/he colluded. Table 1 lists the relationships or roles the perpetrator(s) had in or with the victim organization.

Table 1. Roles of the Perpetrators

	Collusion		Single
	Primary	Secondary	Perpetrator
Relationship to Victim Organization			
Owner/Manager (%)	60	32	37
Employee/Non-Manager (%)	30	32	57
Vendor (%)	5	12	2
Customer (%)	0	12	2
Other/Not Identified (%)	5	12	2

From Table 1, one can see obvious differences in the roles the perpetrators had in or with the victim organizations, associated with each type of fraud. If the fraud involved collusion, then the primary perpetrator is much more likely to be in an owner or management position while the partner is much more likely to be an employee or non-manager. The difference in power of position held may have helped the owner/manager persuade or coerce another, lower-ranking employee to participate, in order for the fraud to succeed. In 60% of the collusive cases the primary perpetrator was an owner/manager. In the non-collusive frauds in this study, only 37% of the perpetrators were owner/managers. Non-parametric tests indicate a significant difference in the distributions of roles between the primary perpetrator in the collusive frauds and the single perpetrator in the non-collusive frauds at the .03 level.

In 6 of the 43 collusion cases, we were unable to determine if power differences existed between the perpetrators, e.g., both were classified as former associates, as relatives, as vendors, etc. In the 37 remaining cases, we identified 13 cases in which both perpetrators were classified as owner/managers or both were classified as employee/non-managers and 24 cases in which the roles of the perpetrators indicated the possible existence of power differences, i.e., an owner/manager and an employee/non-manager was involved. We created a power difference variable coded "1" for those instances in which an owner/manager was one of the parties to the collusive fraud, and "0" when there was no owner/manager involved. However, a binomial test for equal probabilities indicates only marginal statistical significance (.10) that power differences existed between the perpetrators in the collusive frauds. What is clear, however, is substantial involvement by owners/mangers in the collusive frauds.

The Fraud Event

The literature predicts that internal control weaknesses contribute to the likelihood of fraud. We asked the respondents to indicate the extent to which internal controls contributed to the perpetration of the fraud. A scale of 1 to 7 was provided, with 1 indicating that a control weakness did not contribute to the fraud, and 7 indicating that the control weakness contributed significantly to the fraud. Table 2 offers the respondents' ratings. The higher the rating the more significantly the weakness was viewed by the respondent as an enabling factor of the fraud. In Table 6 we report the ratings by type of internal control weakness reported as well as a comparison between frauds involving collusion and those with single perpetrators.

Table 2. Exploitation of Internal Control Weakness

Weakness Mean (1 to 7 scale)	Collusion	Single Perpetrator	P* Sig.	NP* Sig.
Separation of duties	5.42	5.69	ns	ns
Proper authorization	5.90	4.88	.03	.06
Periodic checks and balances	5.44	5.69	ns	ns
Lax attitudes	5.74	4.84	.06	.01
Asset safeguards	5.10	4.28	ns	.01
Required documentation	5.03	3.98	.06	.07
Competent personnel	4.72	2.90	.00	.00

P indicates t-test*
NP indicates non-parametric tests*

Both parametric tests of means and non-parametric tests of medians indicate differences in the exploitation of internal control weaknesses. For the collusive frauds, lack of proper authorization, lax attitudes, failure to safeguard assets, lack of required documentation, and lack of competent personnel were all mentioned as contributing more to the success of the fraudulent activities. The observation of the lack of competent personnel is noteworthy in the collusions. Given the number of owner/managers involved in the collusive schemes, the manager may have first identified an incompetent employee as a weak link in a critical control system, which would allow exploitation of other weaknesses. That employee could then have been exploited in a number of ways: directly assisting with the fraud; not realizing a control was being overridden; not recognizing that a control was important; or being instructed to ignore a control step. The role of management in the collusive frauds is also reflected in the importance the respondents attributed to lack of proper authorization in an environment of lax attitudes. The literature suggests that collusive frauds, by their nature, will obviate the effectiveness of separation of duties as an internal control.

We also asked the respondents to assess a variety of characteristics about the scheme, also on a scale of 1 to 7. The assessment involved rating the degree to which the scheme was unusual (rare =1; common = 7); was complex (simple = 1; complicated = 7; occurred frequently (one-time =1; continual = 7; and difficult to detect (difficult = 1; easy = 7). We used t-tests to compare the means and non-parametric tests of medians. Based on the literature, we expected that the collaborative nature of the collusion schemes would trigger significant differences, particularly with regard to the continuous nature of the scheme and the difficulty in detecting it. Our results are displayed in Table 3.

Table 3. Nature of Scheme

Characteristic (1 to 7 scale)	Collusion	Single Perpetrator	Sig.
Common	3.47	3.91	ns
Complicated	3.55	2.12	.00
Continual	5.41	5.16	ns
Easy to detect	4.09	4.71	ns

Only one significant difference was observed between the collusive schemes and the non-collusive schemes. Collusive schemes were deemed to be more complex than non-collusive. This may reflect not only the number of weaknesses in internal controls that were exploited, but other aspects of the scheme. In the course of business, if something appears to involve unusually complex activities or explanations, this might be an indication that collusion is occurring.

Table 4. Red Flags Present

Red flags present	Collusion	Single Perpetrator	Sig.
Missing documentation (%)	31	22	ns
Altered documents (%)	47	46	ns
Computer records altered (%)	47	27	.04
Lifestyle changes (%)	9	7	ns
Financial anomalies (%)	80	37	.00

Both missing and altered documents were common to both types of frauds but only the alteration of computer records differed (.04) with computer records more likely to be altered among the collusive frauds. Financial anomalies were common to both, but much more likely to be a signal of fraud in the instances of collusion.

SUMMARY

The goal of this paper was to examine collusion and single-perpetrator frauds, and identify potential differences between the two in respects to internal control weaknesses. This information might be useful for internal control system design and auditing. The study suggested there was significantly more management involvement in collusive fraud than in single-perpetrator fraud. This supports the Committee of Sponsoring Organizations COSO framework that the control environment is the foundation for all internal controls to be effective. The managements' ethical values, philosophy and operating style set the tone at the top and influence the perceived strength of the internal control system. Having multiple employees/management involved in collusive fraud behavior is indicative of break downs in the control environment. As expected collusion frauds were judged to be more complicated than single-perpetrator frauds and more frequently exploited lack of competency issues. Alteration of computer records and the presence of financial anomalies were also significant for collusions frauds. These findings suggests the use of computer –assisted audit tools and techniques software such as ACL or IDEA might be valuable in detecting and investigating collusion based frauds. While separation of duties weaknesses were identified as a bigger contributor in single perpetrator frauds the difference was not significant. While emphasizing controls on separation of duties and periodic checks balances might be deterrence for single perpetrator frauds they are probably not sufficient to deter collusion frauds. In fact that category was listed high for both collusion and single perpetrator fraud indicating a focus in designing and auditing controls in this area should be a primary focus. For example, adding layers of separation of duties in assigning access controls for information systems might be suggested to help prevent collusion. Also embedding detective controls in information systems that can promptly search for and identify financial anomalies are also recommended by the research.

REFERENCES

Albrecht, W. S., Albrecht C., and Albrecht, C. C. (2008). Current trends in fraud and its detection. *Information Security Journal: A Global Perspective*, *17*, 2-12.

Albrecht, W., Abrecht, C. O., Albrecht, C. C. and Zimbelman, M. (2012). *Fraud examination*. Mason, OH: South-Western.

American Institute of Certified Public Accountants, Auditing Standards Board (ASB). (2002). Consideration of fraud in a financial statement audit, *Statement of Auditing Standards No. 99*). New York, NY.

Association of Certified Fraud Examiners (ACFE) (2014). Report to the Nations on Occupational Fraud and Abuse. Austin, Texas.

Bainbridge, D. (2007). Criminal law tackles computer fraud and misuse. *Computer Law & Security Report*, *23*, 276-281.

Barnard, C. I. (1938). *The Functions of the Executive*. Cambridge, MA: Harvard University Press.

Coleman, J. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology*, *93*(2), 406-439.

Collins, J., and Schmidt, F. (1993). Personality, integrity, and white collar crime: A construct validity study. *Personnel Psychology*, *46*(2), 295-311.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1978). *Internal control-integrated framework*. New York, NY.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1992). *Internal control—integrated framework*. Harborside, NJ: American Institute of Certified Public Accountants.

_____. (2011). *Embracing enterprise risk management: Practical approaches for getting started*. www.coso.org

Cornish, D., and Clarke, R. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, *25*(4), 933-947.

Cressey, D. (1973). *Other People's Money*, NewYork: The Free Press.

Daly, K. (1989). Gender and varieties of white-collar crime. *Criminology*, *27*(4), 769-793.

Dominey, J. Fleming, A. Krunacher, M and Riley, R. (2012). The evolution of fraud theory. *Issues in Accounting Education*, *27*(2), 555-579.

Guercio, J. P., Rice, E. B., and Sherman, M. F. (1988). Old fashioned fraud by employees is alive and well: Results of a survey of practicing CPAs. *The CPA Journal*, *58*(9), 74-77.

Hollinger, R. C., and Clark, J. P. (1983). Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Social Forces*, *62*(2), 398-418.

Holtfreter, K. (2005). Is occupational fraud "typical" white collar crime? A comparison of individual and organizational characteristics. *Journal of Criminal Justice*, *33*, 353-365.

Hooks, K. L., Kaplan, S. E., and Schultz, J. J. (1994). Enhancing communication to assist in fraud prevention and detection. *Auditing: A Journal of Practice and Theory*, *13* (Fall), 86-117.

Institute of Internal Auditors. (1985). Deterrents, detection, investigation, and reporting of fraud (*Statement on Internal Auditing Standards No. 3*), Sarasota, FL.

Loebbecke, J. K., Eining, M. M., and Willingham, J. J. (1989). Auditor's experience with material irregularities: Frequency, nature, and detectability. *Auditing: A Journal of Practice and Theory*, *9*(1), 1-28.

Mann, K. (1992). White-collar crime and the poverty of the criminal law. *Law and Social Inquiry*, *17*(2), 561-571.

Matsumura, E. M., and Tucker, R. R. (1992). Fraud detection: A theoretical foundation. *The Accounting Review*, *7*(4), 753-782.

Mittendorf, B. (2008). Infectious ethics: How upright employees can ease concerns about tacit collusion. *The Journal of Law, Economics, & Organization*, *24*(2), 356-370.

Moorthy, M., Seetharaman, A., Somasundaram, N., and Gopalan, M. (2009). Preventing employee theft and fraud. *European Journal of Social Sciences*, *12*(2), 259-268.

National Commission on Fraudulent Financial Reporting (NCFFR). (1987, October). *Report of the National Commission on Fraudulent Financial Reporting*. Washington, DC. Author.

Ponemon, L. A. (1994). Whistle-blowing as an internal control mechanism: Individual and organizational considerations. *Auditing. A Journal of Practice and Theory*, *13*(2), 118-139.

Public Company Accounting Oversight Board (PCAOB). (2006). Understanding the entity and its environment and assessing the risks of a material misstatement (*Statement of Auditing Standards No. 109*). New York, NY.

_____. (2008). Communicating internal control related matters identified in an audit. *Statement of Auditing Standards No. 115*. New York, NY.

Sarbanes-Oxley Act of 2002. (2002). Available: http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html.

Seidman, J. S. (1990). A case study of employee frauds. *The CPA Journal*, *60*(l), 28-35.

Shapiro, S. (1990). Collaring the crime, not the criminal: Reconsidering the concept of white-collar crime. *American Sociological Review*, *55*(3), 346-365.

Silver, S. E., Fleming, A. S., and Riley, R. A. (2008, October). Preventing and detecting collusive management fraud. *The CPA Journal, (78)*, 10, 46-48.

Soltani, B. (2014). The Anatomy of Corporate Fraud: A Comparative Analysis of High Profile American and European Corporate Scandals. *Journal of Business Ethics*, *120*, 251-274.

Thompson, C. (1993). Fraud findings. *Internal Auditor*, *50*(3): 64–65.

Trumpeter, G. Carpenter, T., Jones, K. and Riley, R. (2014). Insights for research and practice: what we learned about fraud from other disciplines. *Accounting Horizons*, *28*(4) 769-804.

Vinten, G. (1992). The whistle blowing internal auditor: The ethical dilemma. *Internal Auditing*, *8*(3), 26–33.

Wells, J. T. (2011). *Principles of Fraud Examination*. Hoboken, NJ: John Wiley & Sons, Inc.

Wells, J. T. (2013). *Corporate Fraud Handbook*, *Prevention and Detection*, Fourth Edition. . Hoboken, NJ: John Wiley & Sons, Inc.

Wheeler, S., and Rothman, M. (1982). The organization as weapon in white-collar crime. *Michigan Law Review*, *80*, 1403-1426.