JOURNAL OF INFORMATION SYSTEMS
Vol. 24, No. 1
Spring 2010
pp. 1–21

American Accounting Association
DOI: 10.2308/jis.2010.24.1.1

The Impact of Internal Controls and Penalties on Fraud

Roberta Ann Barra
University of Hawai'i at Hilo

ABSTRACT: Little prior research exists on the parameters of internal control activities. The Sarbanes-Oxley Act of 2002 (SOX 2002) makes identifying the properties of these parameters under various conditions important. In this paper, an analytical/reliability engineering methodology is used to investigate the relative impact of penalties versus other types of internal controls on managerial and non-managerial employees' propensity to commit fraud. *Ceteris paribus*, increasing required effort with internal controls and/or increasing employee penalties, increases the minimum amount stolen when a fraud incident occurs; that is, more net assets will be taken per fraud incident with controls than without controls. The findings show that the firm's least-cost scenario with managerial employees is to enforce maximum penalties. The firm's least-cost scenario with non-managerial employees is to utilize alternative internal controls while imposing minimum penalties. Further, the effectiveness of separation of duties is dependent on the detective controls in the internal control system.

Keywords: detective controls; internal controls; internal control activities; fraud; internal control systems; preventive controls; Sarbanes-Oxley; separation of duties.

I. INTRODUCTION

The Sarbanes-Oxley Act of 2002 (SOX 2002) imposes potentially serious penalties on firm executives with fines of up to $5 million and/or imprisonment up to 20 years (SOX §906.c.2). At the same time, this legislation requires that these firms tighten their internal controls over financial reporting. This paper investigates which of these two, the penalties or the tightened controls, is more likely to have the greater effect on reducing fraud in a firm. Further, because SOX imposes penalties only on managerial employees, this paper also examines the relative effects of penalties and controls on managerial versus non-managerial employees.

The literature on fraud (e.g., AICPA 2007; Beck 1986; Bierstaker et al. 2006; Heier et al. 2005; Hooks et al. 1994; Mautz and Mini 1966; PCAOB 2008; Rae and Subramaniam 2008; Wales 1965; Wells 2008) consistently claims that an effective internal control system (ICS) is the primary means of preventing, detecting, and correcting fraud and errors. Yet, that which consti-

My warm thanks to Paul Steinbart, Arline Savage, Brad Schafer, two anonymous reviewers, and the anonymous associate editor at the *Journal of Information Systems* whose comments greatly strengthened this paper. I also received helpful comments from the participants of the 2008 AAA IS Section Midyear Meeting. Special thanks to Randall Shimooka for his insights and help during this process.

Published Online: March 2010

tutes an *effective* ICS is largely conjecture established through *ex post* forensics (a form of induction) performed by practitioners. Demski et al. (1991) and Mattessich (1995, 4) indicate that a symptom of accounting academia in crisis is when accounting research fails to lead practice. This is evident in the acceptance by academic researchers that the effectiveness of internal control activities can be established by a "common sense" approach; that research in this area is unnecessary (Barra and Griggs 2007). Yet, as early as 1970, Carmichael laid out eight behavioral hypotheses that are "implicit in discussions of internal control" (Carmichael 1970, 237). He discussed each of these hypotheses in turn, and laid out the empirical evidence to suggest that there was a general unreality about these accepted hypotheses of internal controls. He suggested formulation of new hypotheses that were "more in agreement with organizational reality" (Carmichael 1970, 245).

Three of the eight widely accepted hypotheses that Carmichael thought to be problematic are particularly relevant to this paper:

> **H3:** An Individual who is independent, i.e., functionally & structurally situated so that he does not perform incompatible actions, will recognize and report irregularities which come to his attention.
> **H4:** The consequences of rejection for suggestions of irregularities will normally be considered prohibitive and, therefore, the probability of collusion is low.
> **H5:** The plan of organization is the only determinant of power in the information processing system. (Carmichael 1970, 238)

Carmichael's paper is often cited, but his suggestions for research have largely been ignored. For example, Carmichael used empirical research to show that these three hypotheses were "modified by the existence of informal groups or cliques in the organizations" that can lead to "toleration of rule-breaking" and "provide the paths for collusive relationships" (Carmichael 1970, 244). This research uses Carmichael's results to support the relaxation of Beck's (1986) "double-cross" element in the models analyzed. This is discussed in the next section. Carmichael's results with respect to these three hypotheses are also used to justify not modeling low probabilities of collusion or high probabilities of whistle blowing.

Internal Control Research

Internal control activities have been established by practitioners, primarily auditors. Rather than investigate the control activities themselves, academics focused their research efforts on issues surrounding the controls using an explicit, or implied, assumption that the properties of the control activities are known. Examples of this type of research include Ashton (1974), Bodnar (1975), Cushing (1974), Doty et al. (1989), Hornik and Ruf (1997), Simon (1974), and Viator and Curtis (1998). Following Bodnar (1975) and Cushing (1974), a number of mathematical models were developed to evaluate internal control systems (e.g., Cooley and Cooley 1982; Grimlund 1982; Helal 1983; Knechel 1983; Robinson 1981; Srinidhi 1988). There are also numerous studies that investigate internal control evaluations. For example, Felix and Niles (1988) list 58 articles published in the 1970s and 1980s on audit-related internal control research.

Wand and Weber (1989) do not look at a specific internal control activity, but neither do they assume that the properties of internal controls activities are known. They bridge these two research paradigms by examining analytically when changes to a data processing system are "lawful" (i.e., working effectively), thus allowing auditors to focus their efforts on critical areas where control changes have occurred.

Limited empirical investigations into internal control activities began in the late 1970s. A small stream of research (Bergeron 1986; Nolan 1977; Olson and Ives 1982; Sen and Yardley 1989) examines the properties of chargeback control systems. Hollinger and Clark (1983), as part of a sociological study examining theft motivations and prevalence, attempted to correlate the effectiveness of inventory controls with employee theft. Murthy (2004) used an empirical methodology to investigate the performance degradation of three computer controls (calculation, lookup, and aggregate function) under three different load conditions (low, medium, and high). He found an interaction effect between the extent of the load and the type of controls being added.

Research by Barra and Griggs (2007) and Beck (1986) established some properties of separation of duties (SOD) using research methodology other than induction. Beck (1986) shows that SOD can be cost effective when used in conjunction with an employee reward program. Beck's reward program provides an opportunity for an approached agent to double-cross the fraud instigator and to receive a reward for notifying the firm of the instigator's intentions. A limiting factor of this study is that many firms do not have whistle-blowing reward programs in place (Schachter 2009). Rather, the whistle-blowing literature (LaVan and Katz 2005–2006; Maher 2006) indicates that informers are more often penalized than rewarded.

Barra and Griggs (2007) extended Beck's study by examining the problem without the specified reward program. They found that the cost effectiveness of SOD in a firm without the whistle-blowing reward program in place decreased by at least 20 percent. This investigation extends Beck (1986) and Barra and Griggs (2007) by examining the n-player problem, and by exploring the relative effects of penalties versus the effort imposed by the addition of SOD.

Collusion Research

It is widely acknowledged in the accounting literature that the effectiveness of SOD can be undermined by collusion. With few exceptions, the academic literature on collusion has been confined to collusion among firms; e.g., price fixing and the like. However, Kofman and Lawarree (1993) examine collusion between an internal auditor and a manager *ex post*; that is, the auditor colludes with the manager to cover up the manager's actions. Beck (1986) and Barra and Griggs (2007) investigate collusion between two agents. The current study generalizes from the two-player model to the n-agent problem.

Penalty Research

The penalty research has been largely confined to the sociology and the economics literature. The economics literature began with Becker (1968), who found that the optimal penalty equals the social harm divided by the probability of detection. Since Becker, others have looked at the problem of applying penalties to employees when corporations are also penalized via corporate fines (e.g., Cohen 1996; Davis 1996; Polinsky and Shavell 1993; Polinsky 2000). None of these, however, examined the differences between managerial and non-managerial employees. Nor did these earlier efforts compare the effects of penalties with other types of internal controls. This study makes a contribution to the literature in that it does both.

The results with respect to the deterrence effect of penalties on crime have been mixed. Williams and Gibbs (1981) reviewed early work on the deterrent effect of penalties on crime and concluded that the mixed results were due to methodological issues. Yet, research in the ensuing decades continues to find mixed results, even though the methodological concerns have been addressed. The evidence suggests that the deterrent effect of penalties differs for types of crimes. For example, Owen (2006) finds empirical support for the inverse relationship between penalties and traffic crime, while *The Economist* (2004) reports no corresponding empirical support for increasing penalties on violent crime. Other research suggests that penalties may also be dependent upon other factors as well, such as industry characteristics (Simpson and Koper 1992) and perceived risk of being caught (Varma and Doob 1998).

Given the mixed results of prior research, it appears clear that penalties are sensitive to type of crime and the circumstances surrounding the crime. It is not a stretch, then, to suspect that the deterrent effect of penalties may also be sensitive to *type* of criminal as well. There appears to be no prior research that specifically looks at the deterrent effect of penalties on white collar criminals, nor whether penalties have an equally deterrent effect on both managerial and non-managerial employees. SOX applies only to managerial employees; this research investigates whether SOX's policy of assigning high penalties only to managerial employees is an effective strategy. Reliability engineering theory is used to model managerial and non-managerial employees. The firm's cost minimization problem and the deterrent effect of penalties and internal controls on managerial and non-managerial employees is examined.

Research Methodology

An analytical approach is used for this investigation because this methodology is the most suitable for providing generalizable results. While simplifying assumptions can limit the generalizability of analytic research, to the extent the assumptions are valid and/or reasonably close to the actual state of nature, generalizability is increased.

An alternative methodology would be an experimental study. However, the monetary incentives that could be feasibly utilized in an experiment would be small. Accordingly, experiments may be more useful for studying the effects of internal controls on petty theft. Controlling petty theft may be fundamentally different from controlling major fraud (Luengo 2004; Vaz 1969); therefore, this study uses an analytical approach to investigate the effects of internal controls on major fraud.

The rest of this paper is organized as follows: Section II presents an analytical model of fraud from the employee's perspective. Section III examines the firm's perspective, which involves how to minimize fraud costs across both managerial and non-managerial employees. Section IV concludes by summarizing the findings and discussing their implications.

II. FRAUD FROM THE EMPLOYEE'S PERSPECTIVE

This section examines the employee's perspective on fraud. The analysis begins with a simple model in which there is only one employee, and then investigates the situation where there are multiple employees. For all models, it is assumed that there is a one-period time horizon for the employees whose utility function is increasing in end-of-period monetary wealth and decreasing in effort and penalties. For tractability, it is further assumed that employee's utility function is additively separable in wages, fraud, and penalties. This implies that employees are risk-neutral and have linear utility functions.

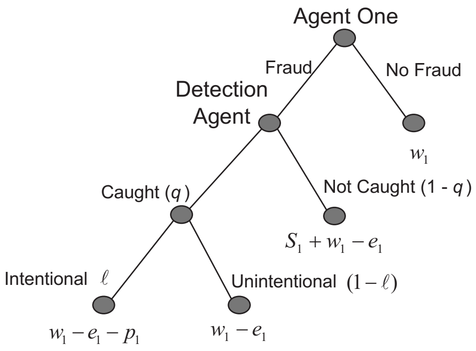
In the one-period model used in this investigation, the Principal is the firm, which can be thought of as represented by the owner(s) of the firm. The Agent is any employee, managerial or non-managerial, subject to at least some portion of the firm's ICS. The concept of reservation amount (*RA*) is introduced as the minimum amount of theft of assets in order for fraud to be a dominant strategy. Theft of assets is broadly construed to include tangible assets as recorded in the balance sheet (e.g., cash, fixed assets) as well as the economic assets that might be gained through financial statement fraud.

This model has complete information in that there is only one employee type and the firm knows this. Employees are all of the type who will reduce their fraudulent actions if the effort required increases (i.e., internal control activities operate on employee's incentives, as intended[1]).

Figure 1 illustrates the nature of the single employee model fraud problem. An individual employee has two *actions* in the feasible set $A_1 =$ no fraud, fraud. The employee also has two

[1] One can imagine situations in which a firm can be overly controlled, causing some types of employees to commit fraud just to beat the system as a challenge or out of anger.

FIGURE 1
Decision Problem for a Single-Agent Contemplating Fraud



The employee chooses fraud or no-fraud. The Detection Agent moves by either detecting fraud or not. If detected, then the Firm determines whether the detected act is fraudulent or unintentional. Payoffs at the end of each node are for Agent One.

Variable Definitions:

q = detection probability;
ℓ = probability the detected act is determined to be intentional;
w = agent wages;
p = fraud penalty;
e = effort required to perpetrate and attempt to conceal the fraud; and
S_1 = amount stolen during the fraud.

strategies.[2] In the first strategy, the employee can choose not to commit fraud and work for wages. Alternatively, the employee can choose to commit fraud and, if caught, attempt to convince the firm that the act was unintentional—thereby escaping penalty.

If the choice is to not commit fraud, the employee's payoff equals current and future wages. If the employee commits fraud and is not caught, the payoff equals the amount obtained by the fraud, plus current and future wages, less the effort required to commit and attempt to conceal the fraud. If the employee commits fraud and is caught, the payoff is dependent on whether the Detection Agent (*DA*)[3] decides the act was intentional (i.e., a fraud) or just the result of an error. Distinguishing between fraud and error is difficult, because they often have similar effects on the

[2] Actions refer to the moves the players can make, in this case, for Agent One, in Figure 1, it is Fraud or No Fraud. All other moves are made by the other players: the Detection Agent and the Firm. The Strategy embodies the entire game, much like playing chess involves more than the current move. The Strategy involves the Agent examining the payoffs at the end nodes, what happens if caught, and if the Firm determines the event to be intentional or unintentional. It is by examining the entire game and determining the best Strategy that the player decides which Action to take.

[3] The *DA* could, for example, be an internal auditor, external auditor, or a member of the audit committee of the board of directors. The DA need not be a person, but could be another internal control activity included in the internal control system.

accounting records.[4] Consequently, Figure 1 includes a measure (ℓ) to reflect the probability of concluding that an act was intentional. If the act is determined to be unintentional, the employee's payoff includes current and future wages less his or her effort to commit the fraud. If the act is determined to be intentional, the payoff is the current wages already earned but not future wages (based on the assumption that all such employees will not be retained by the firm), less effort and penalties. As these are all one-period models, it is assumed that detection is timely enough to either prevent the theft or allow the firm to recover the stolen assets.

The employee chooses an amount to steal S_1; if $S_1 \in [\underline{S}, \bar{S}]$ then $\underline{S} \geq 0$, and $\bar{S}$ is bounded above by some asset limitation. Depending on the employee's utility function, this asset limitation could be as large as the net available assets of the firm or as small as what can be easily slipped into a pocket. That is, $\bar{S}$ is firm- and employee-specific. While $\underline{S} \geq 0$, for all firms and all employees, there can be employees with utility functions such that $\underline{S}$ is strictly zero; e.g., honest employees who will always choose the "no fraud" path such that $S_1 = 0$.

This is a game of incomplete information for the firm and the employee, so it can be said that the first moves, for the employee and the firm, are "simultaneous." The firm implements an internal control system; the entire system is not completely known to all employees. Simultaneously, while observing this internal control system, the agent determines whether the reservation amount (RA), computed below, is greater than or less than S_1. If $S_1 \geq RA$, then the agent commits fraud. If $S_1 < RA$, then no fraud occurs. The firm cannot know for certain whether fraud has occurred.

Referring to Figure 1, and recalling that the employee's alternative to fraud is to work for wages (w_1), a single employee will commit fraud only if the utility derived from the fraud exceeds the utility of working for wages (note that as this is a one-period model, future wages should be thought of as the present value of expected future wages; all amounts are, naturally, expectations). The utility from fraud is reduced by the possibility the agent could be caught in the fraudulent act and suffer the effort of committing the fraud without receiving the corresponding utility of the fraudulent takings. The utility from fraud is further reduced by the possibility that the fraudulent act, once identified, will be determined intentional by the firm and penalties will be imposed. This is expressed by:

$$q\ell[w_1 - e_1 - p_1] + q(1-\ell)[w_1 - e_1] + (1-q)[S_1 + w_1 - e_1] \geq w_1 \tag{1}$$

where:

q = probability of being caught in the act of fraud;
ℓ = probability the detected act is determined to be intentional by the firm;
w_1 = agent's wages;
e_1 = agent's effort required to commit fraud;
p_1 = penalty if caught ($p_1 = f(w_1, damages)$); and
S_1 = amount of fraud (amount stolen; a loss to the firm).[5]

[4] For example, consider an audit finding that a tangible asset recorded on the books is not present. This discrepancy could be the result of theft, deliberate inflation of the recorded value of assets, or merely an error. Additional evidence is needed to determine which of these three plausible explanations is correct. Similarly, additional evidence is required to determine whether failure to record a transaction is due to an error or reflects an intentional act of fraud.

[5] The cost of fraud to the firm would almost certainly exceed S_1 due to additional costs of legal fees, audit fees, and so on. That is, the cost to the firm is S_1 + other costs = S^1 where S^1 is assumed to be monotonically increasing in S_1 but limited to the net assets of the firm. For ease of notation, and without loss of generality, the cost to the firm is modeled as S_1. The utility derived from fraud ($U(S_1)$) provides the incentive for fraud. Without loss of generality one can consider intangibles, such as the thrill of beating the system, as incorporated within the individual's utility function.

It is assumed that the monetary penalty is equal to the difference between the net present value of future earnings in the agent's current position and the next-best alternative (e.g., a new job), plus court-imposed punitive and/or restitution damages, if any. It is further assumed that wages are an exogenous constant; thus, the effect of a particular employee's penalty is dependent on the damages, if any.

With simple algebra (see the Appendix) and rearranging the terms, Equation (1) becomes Equation (2):

$$S_1 \geq \frac{e_1 + q\ell(p_1)}{1-q} = RA. \tag{2}$$

The reservation amount (*RA*), or net utility from committing the fraud, therefore, is equivalent to the sum of the effort it takes to commit the fraud plus the expected value of the penalty[6] (note that the loss of future wages can be thought of as part of the penalty the employee pays), indexed by the probability of not getting caught. Equation (2) shows that the employee will commit the fraud and steal S_1 if and only if $S_1 \geq RA$. Equation (2) also shows that *RA* is positively related to *q*, the probability of detection, ℓ, the probability of being found intentional, and also positively related to both effort and penalty; with the strongest effect being that of the probability of detection − *RA* approaches infinity as the probability of detection approaches 1. (The equation is undefined at $q = 1$.) Thus, the likelihood of a single employee committing fraud can be reduced by increasing the required effort to commit the fraud, the penalties if caught, and the probability of detection.

With more than one employee, the internal control system changes by including SOD which now requires collusion in order for fraud to occur. This is modeled for two agents in Figure 2. The two-player model (and n-player model introduced next) assumes that the employees either accept or reject the collusive offer. This differs from Beck (1986), who assumed that the employees might also choose to double-cross one another; that is, appear to accept a collusive offer, then actually not collude but rather report on each other in order to receive a reward offered by the firm. Because this research models no reward system, there is no incentive for a double cross. Therefore, in the collusion models it is assumed that if the second Agent informs the Detection Agent of the intended misappropriation prior to the actual commitment of the act, then this is equivalent to a reject-and-tell path. That is, unlike Beck (1986), there can be no double cross once an offer to collude has been accepted. It is further assumed that, if collusive fraud occurs, all agents receive equal shares and productivity is not affected by separation of duties.

The cost of collusion, as well as the probability that a non-colluding employee will blow the whistle, changes the *RA* to Equation (3):

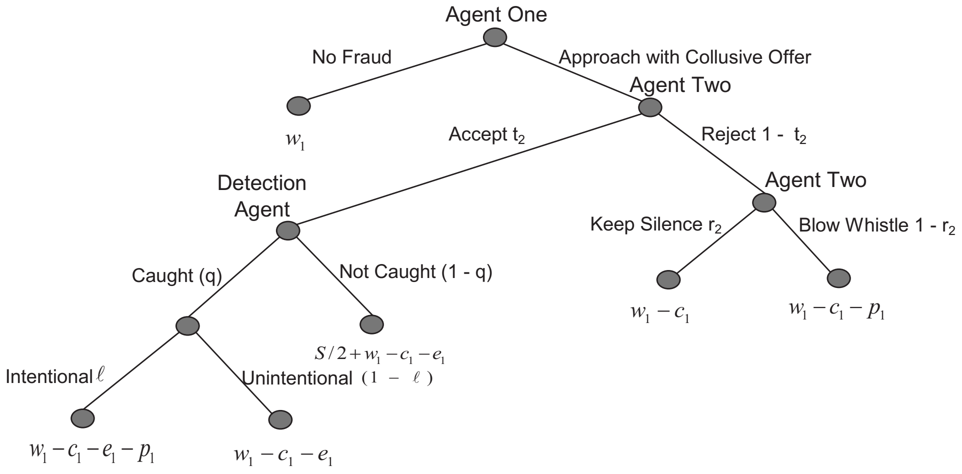
$$RA_1 = \frac{c_{1_2}}{t_2(1-q)} + \frac{e_1}{1-q} + \frac{ql(p_1)}{1-q} + \frac{(p_1)(1-t_2)(1-r_2)}{t_2(1-q)} \tag{3}$$

where:

c = agent one's cost of collusion, i.e., the cost involved in approaching a second agent with a collusive offer;
t = probability that a second agent will accept a collusive offer from agent one; and

[6] The derivative of this function with respect to the penalty is not a function of the amount stolen, it is a function of the probabilities. Yet, it may be likely that the penalty may be a function of the amount stolen, hence, this equation may be chaotic in the mathematical sense. This is not evaluated. The point here is that the penalty, like all the variables modeled here, is not a fixed amount but is relative to the other variables; here, for example, the penalty would be relative to the amount stolen.

FIGURE 2
Two-Agent Collusion Problem



Agent One's decision problem is whether to approach the second agent with a collusive offer. Agent Two can accept or reject the offer. If Agent Two accepts, then the Detection Agent may detect the fraud and determine the fraud is intentional. If Agent Two rejects the collusive offer, then Agent Two could inform the Firm of the collusive offer. Payoffs at the end nodes are for Agent One.

Variable Definitions:

q = detection probability;
ℓ = probability the detected act is determined to be intentional;
w = Agent One's wages;
p = fraud penalty imposed on Agent One;
e = effort required by Agent One to perpetrate the fraud;
S = total amount stolen, Agent One receives half in a two-agent problem;
c = effort required by Agent One to approach Agent Two with a collusive offer;
r = probability that Agent Two will not inform; and
t = probability that a second agent will accept a collusive offer from Agent One.

r = probability that a second agent will reject a collusive offer and not inform the Detection Agent; (i.e., $(1 - r)$ = whistle blowing probability).

Note that the model is undefined at $t = 0$, and $q = 1$.

With n-agents, the model becomes intractable for visual representation and the equations become too lengthy for inclusion here and are consequently left to the Appendix where the proof is provided. From those proofs, one can see that what holds for one agent and two agents also holds for n-agents; that is, in Equations (2) and (3), and the corresponding n-agent equation:

$$e > p. \tag{4}$$

This is expressed in the following theorem:

Theorem: An increase in effort has more of an impact on the *RA* than a corresponding increase in penalties. That is, changing employee effort and/or changing employee penalties changes the *RA*. However, changing employee effort has a greater effect on the *RA* than changing the employee penalty, *ceteris paribus*.
Proof: See Appendix.

Note that the agent's current wages do not have a direct effect on RA_1 because they are due to the employee for past services rendered. Any attempt to take back these wages in restitution for amounts taken in a fraudulent action changes the nature of these current wages from current wages to penalties. In other words, one may not withhold an employee's wages for services already performed by the employee in the event of a fraud. One must pay the wages and then seek restitution for the fraud in a court of law. Future wages, lost as a result of firing or garnishment, are mathematically identical to other penalties and can, therefore, be thought of as part of the penalty. Therefore, future wages have a direct effect on RA_1.[7]

Equilibrium Analysis

In the single-agent model Equation (2), the two-agent model Equation (3), and the n-agent model (Appendix), notice that the equation is undefined when the probability of detection, q, = 1. As the probability of detection approaches 1, the reservation amount approaches infinity. That is, the more likely it is the perpetrators will be detected, the less likely it is that there will be sufficient assets to tempt them to commit fraud. This detection probability is a function of the entire internal control system. For example, the perpetrators can be caught by other internal controls, internal auditors, and/or external auditors.

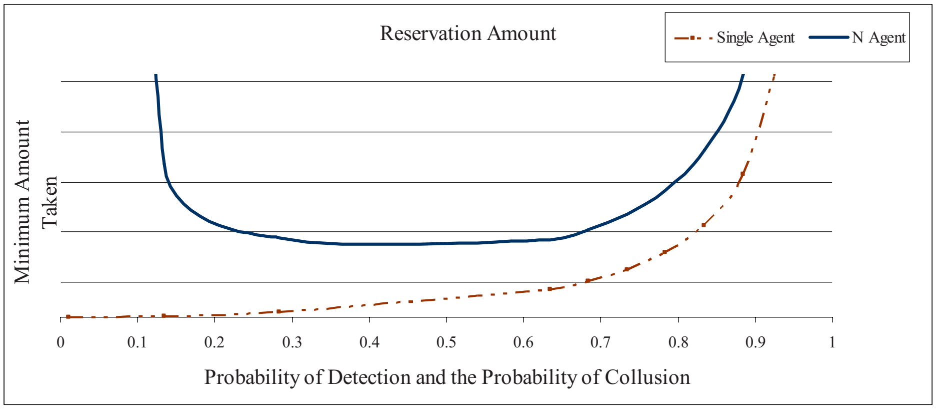
As the probability of detection approaches zero, the single-agent model devolves into a model in which only effort matters. This should be intuitive. If there is no detection, there can be no penalties imposed. In the collusion model, there exists some possibility of penalties, even when the probability of detection approaches zero, because the collusive partner has some probability of rejecting the collusive offer and blowing the whistle. Even so, penalties play a reduced role, even in the collusion model, when the probability of detection approaches zero.

In the collusion model, the model is relatively insensitive to the whistle-blowing probability, $(1 - r)$. However, the model does react to interaction effects of the probability of whether the actors decide to accept a collusive offer, t, and the probability of detection, q. Both of these probabilities appear in the denominator of the model. Thus, both of these probabilities have a large impact on the reservation amount individually. Moreover, these two probabilities also have an interaction effect. When those two probabilities move together, that is, when there is a low probability of detection and a simultaneous low probability of collusive acceptance, then the reservation amount approaches infinity in the collusive model. The reservation amount also approaches infinity when these probabilities approach 1. Wherever the reservation amount approaches infinity, fraud should not occur. At zero, for both probabilities, the equation is undefined. This scenario is presented graphically in Figure 3.

Where the two probabilities move in opposite directions to one another, then the reservation amount approaches infinity only when the detection probability approaches one (or certainty.) When the probability of detection moves in the opposite direction, for example, when the probability of detection is 0.1 and the probability that the collusive partner will accept the collusive offer is 0.9, then fraud should occur, but, perhaps paradoxically, the amount taken is relatively low. This may seem paradoxical but may reflect the lack of risk to the employees. That is, with low risk to the employees, they have no incentive to risk taking large amounts; this may be the scenario

[7] Loss of future wages may be part, or even all, of the penalty in a two-period, or more, game.

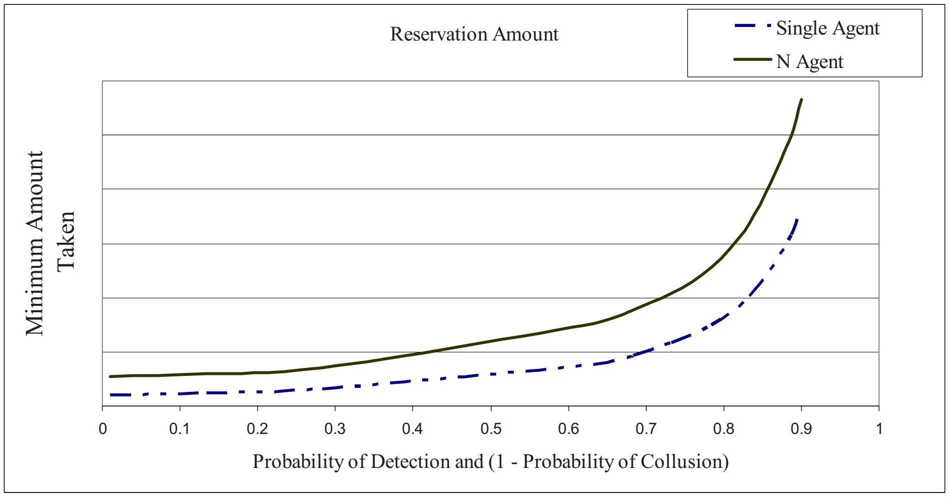
FIGURE 3
Comparison of Minimum Amount Taken by Single Employee versus Collusion When Probability of Detection is Positively Correlated with Probability Agreement to Collude



where employees take multiple, small amounts over time. As this is a one-period model, only one fraud act is captured in this model. At zero, for both probabilities, the equation is undefined. These scenarios are presented graphically in Figure 4.

In all cases, the minimum amount taken is greater with the collusive model.

FIGURE 4
Comparison of Minimum Amount Taken by Single Employee versus Collusion with Probability of Detection Inversely Related to Probability of Agreement to Collude



III. THE PROBLEM FROM THE FIRM'S PERSPECTIVE

In this section, the firm's problem is examined. In this model, the firm's problem is whether to utilize controls, given that using controls increases the amount taken per fraud incident, and also keeping in mind that controls are required under SOX. This is a cost minimization problem. Two situations are explored: the first situation utilizes a simplifying assumption that all employees are of the same type (i.e., all either managerial or non-managerial). The second situation is more realistic and examines the case where there are managerial and non-managerial employees. It is assumed that detected amounts are completely recoverable, i.e., the firm's costs include only undetected fraud and errors.

All Employees of the Same Type

Note that the reservation amount with two or more employees is greater than the reservation amount with a single employee; that is, the minimum amount taken per fraud incident is greater with controls than without controls. This is because with controls greater effort is required of the employees in order to perpetrate their fraudulent activities. In this case, collusive effort is required. That is, controls require circumvention effort of employees; without the controls, circumvention effort, such as collusion or some other methodology, would not be necessary.

If one assumes that with controls some frauds will be detected and, of those frauds, a percentage of the amount taken will be recovered, these recovered amounts help to defray the cost of the controls. Moreover, it is popularly assumed that controls reduce the overall number of frauds. While this has yet to be shown via research, it is safe to assume that the number of frauds will be different with controls than without controls for a variety of reasons. It would be rational to utilize controls if the cost of doing so is less overall than the cost of not having those controls in place, *ceteris paribus*. Considering just the issue of fraud, the problem becomes:

$$NRA_{NC} < MRA_{WC} + C - \%MRA_{WC}$$

$$NRA_{NC} + \%MRA_{WC} - MRA_{WC} < C \tag{5}$$

where:

N = number of frauds without controls;
M = number of frauds with controls;
C = cost of controls;
RA_{NC} = the amount taken without controls;
RA_{WC} = the amount taken with controls; and
$\%$ = the percentage of frauds detected and recovered.

Equation (5) indicates that a control will be effective when the cost of the control is less than the cost of fraud without controls added to the cost of undetected/unrecovered fraud *with* the control. This is somewhat intuitive. The equation makes explicit that we have a number of unknown variables for most, if not all, controls; that is, in order to do a cost/benefit analysis for any given control, we need to know how the control affects the number of fraud incidents that occur (one can think of this as M, N, and $[M - N]$ in Equation (5)). We also require information that indicates how a given control affects the amount of fraud that occurs, is detected, and recovered (i.e., RA_{NC}, RA_{WC}, $\%$, and $[RA_{NC} - RA_{WC}]$ in Equation (5)).

Managerial versus Non-Managerial Employees

The preceding analysis was for generic employees, both managerial and non-managerial. Yet, the provisions of Sarbanes-Oxley apply largely to managerial employees. Sarbanes-Oxley imposes high penalties on managerial employees. In this section, a different model is built that looks at the firm's least-cost scenario; a cost minimization problem assuming that controls will be utilized. Given the results of the first section that *e* (effort) had greater impact than *p* (penalties), the question is whether SOX penalties should be imposed.

A firm's choice in this model is restricted to a choice of employee function: process (non-managerial) or process/control (managerial). The concepts of Process versus Process/Control functions are taken from reliability theory (Devor et al. 1992, 124–135). Process or non-managerial employees are employees who confine themselves, or are confined, to performing assigned tasks. These employees perform no tasks designed to identify errors of other employees. Consequently, they detect few errors and frauds. It is assumed that an agent who functions as a non-managerial employee is aware of his/her assigned task. This agent is not aware of how his/her task fits in the firm's overall control structure. Thus, employee effort to commit fraud is large for non-managerial employees relative to managerial employees. Because non-managerial employees know less about the internal control system and the processes of the firm, they are assumed to make more errors. These employees can also claim ignorance more successfully than managerial employees and, by doing so, can reduce the probability that a fraud will be determined intentional. Non-managerial employees can be thought of as operating in series (in the reliability engineering sense) with little responsibility, effort, training, or expectation that employees will check their own or a prior individual's work for error.

Process/Control or managerial employees are employees who perform their assigned tasks and additional tasks that should identify errors of other employees. Using the language of reliability theory, managerial employees can be considered partially or fully redundant because they have the responsibility to catch and correct errors; thus, they serve as their own control. It is assumed that an agent who functions as a managerial employee is aware of his/her own task and how that task fits in the firm's overall control structure. This agent is responsible for evaluating and correcting documents that pass through his/her possession. Because of their control function, managerial employees are also assumed to detect more fraud. Wages are held constant for both types of employees in the firm's cost function in order to analyze the effects of fraud on the firm's cost function, *ceteris paribus*.

At first glance, it may seem implausible that one agent can function as a non-managerial employee as defined here. However, this seems to be the standard assumption implicit in the extant literature (e.g., AICPA 2007, AS No. 2). The conventional argument is that people more easily find and correct others' errors than their own errors. The assumption, therefore, is that an employee working alone may not find his or her own errors. If an employee finds his or her own errors, one could argue that no error was made. This implies a process or non-managerial employee, one with no control or error-checking function, rather than a process/control or managerial employee. Nonetheless, it also seems plausible that an agent working alone may, over time, transition from a non-managerial to a managerial employee by virtue of experience and attitude. This possibility is assumed away in this model by assuming that the firm can directly control wages and employee function. It is assumed that the probability that a discovered fraud will be determined by the firm to be intentional increases as employee function moves from non-managerial to managerial; that is, the probability of an employee failure being considered fraud is lower for non-managerial employees than for managerial employees.

Ignoring production costs and considering only the costs of errors and fraud, the firm's objective is to minimize total costs. Thus, costs to the firm include wages, cost of errors, and cost of fraud. The firm can decide whether to seek maximum penalties if fraud is detected.

Because a firm should seek to minimize costs, it is entirely possible that allowing some fraud is less costly than attempting to eliminate fraud entirely. Thus, while a firm seeks to minimize fraud, it does so only as long as fraud minimization is cost effective. Using the same notation used earlier and introducing Φ as the probability of *not* detecting *un*intentional errors and E as the cost of *un*intentional errors, the firm's cost function is:

$$TotalCost = w_1 + (1 - q)S + \Phi E. \tag{6}$$

Recall from Equation (2) that $S \geq RA$. If increasing the RA decreases the probability of fraud,[8] then it is rational for a firm to attempt to maximize RA_1 in order to reduce S and minimize the cost function, *ceteris paribus*. The firm can use other strategies to control wages and unintentional errors. To control fraud, the firm must use an employee function that affects the RA_1 and, through the RA_1, try to minimize S.

Non-Managerial Employees

When non-managerial employees are used, the probability that an agent's errors will be considered intentional (ℓ) will be low because these employees do not catch their own mistakes, by definition. Hence, errors found will be considered unintentional more often (i.e., ℓ is low), decreasing RA_1, which increases the probability of fraud. However, ℓ has a minimal effect on RA_1 relative to the other variables. For these employees, effort (e_1) is high because they have less control access to the system; this increases RA_1, and decreases the probability of fraud with more impact than changes in ℓ.

Managerial Employees

Conversely, with managerial employees, ℓ (the probability the act will be considered intentional) is high (increasing RA_1), but, again, with minimal impact relative to the other variables. For this employee function, effort is low, which decreases RA_1. The net effect is that the probability of fraud increases.

These relationships are presented in Table 1.

Table 2 shows the two cost functions obtained when the firm uses non-managerial and managerial employees. From Table 2, it is clear that the Firm's least-cost case is, by inspection, to use managerial employees [$F_{F_{P/C}}$ (P/C employees)] when the amount of fraud that occurs with each type of employees is identical ($S_{1_P} = S_{1_{P/C}}$); when this is the case, it is always true that the firm's cost is less with managerial employees than with non-managerial employees ($F_{F_{P/C}} < F_{F_P}$), *ceteris paribus*.[9]

Analysis

Firms are not run by management alone. Also, in this particular model, the amount of fraud is chosen *a priori*. That is, the amount of fraud that occurs, S_1, does not vary with employee function. Rather, S_1 depends on the reservation amount, RA_1, where:

[8] It may not be true that increasing the RA decreases the probability of fraud for all employees. This will be discussed in more detail in the n-agent section.

[9] The most unlikely of the *ceteris paribus* conditions is that the wages are kept equal for both managerial and non-managerial employees. Holding wages equal for both managerial and non-managerial employees allows for the analysis of the effects of the costs of fraud and errors. Obviously, a very large differential in wages between managerial and non-managerial employees would negate any effects one might see in the model developed here, hence, the need to hold wages constant for analytical purposes. Future research might consider the interplay of these variables.

TABLE 1
Fraud Reservation Amount

Panel A: One-Agent Model

Employee Function	Employee Effort	Detection Probabilities	Reservation Amount	Case
Non-Managerial	High	Low	$\frac{e_H + q_L(\ell_L)(p_1)}{1 - q_L}$	F_{E_P}
Managerial	Low	High	$\frac{e_L + q_H(\ell_H)(p_1)}{1 - q_H}$	$F_{E_{P/C}}$

Panel B: Two-Agent Model

Employee Function	Employee Effort	Detection Probabilities	Reservation Amount	Case
Non-Managerial	High	Low	$\frac{c_{1_2}}{t_2(1 - q_L)} + \frac{e_H}{1 - q_L} + \frac{q_L \ell_L(p_1)}{1 - q_L} + \frac{(p_1)(1 - t_2)(1 - r_2)}{t_2(1 - q_L)}$	F_{E_P}
Managerial	Low	High	$\frac{c_{1_2}}{t_2(1 - q_H)} + \frac{e_L}{1 - q_H} + \frac{q_H \ell_H(p_1)}{1 - q_H} + \frac{(p_1)(1 - t_2)(1 - r_2)}{t_2(1 - q_H)}$	$F_{E_{P/C}}$

TABLE 2

Firm Cost
(One-Agent Model)

Employee Function	**Probability of Not Detecting Errors**	**Cost of Errors**	**Firm Cost**	**Case**
Non-Managerial	High	High	$w_1 + \Phi_H E_H + (1 - q_L)S_P$	F_{F_P}
Managerial	Low	Low	$w_1 + \Phi_L E_L + (1 - q_H)S_{P/C}$	$F_{F_{P/C}}$

$\Phi_H \equiv$ high probability;
$\Phi_L \equiv$ low probability;
$E_H \equiv$ high probability; and
$E_L \equiv$ low probability.

$$S_1 = \begin{cases} 0 & if\ RA_1 > \bar{S} \\ \bar{S} & if\ RA_1 \le \bar{S} \end{cases} .$$

Since $F_{F_{P/C}}$ is the firm's least-cost case, it remains to be determined if $F_{E_{P/C}}$ results in a maximum RA. For the employee $F_{E_{P/C}} > F_{E_P}$ when:

$$q_H \ell_H (1 - q_L) - q_L \ell_L (1 - q_H) > \frac{e_H(1 - q_H) - e_L(1 - q_L)}{(p_1)} \tag{7}$$

where:

F_{E_P} = employee case one: non-managerial employees;
$F_{E_{P/C}}$ = employee case two: managerial employees;
F_{F_P} = firm case one: firm cost with non-managerial employees;
$F_{F_{P/C}}$ = firm case two: firm cost with managerial employees;
q_H = high probability $q_L \equiv$ low probability;
ℓ_H = high probability $\ell_L \equiv$ low probability;
e_H = high probability $e_L \equiv$ low probability;
S_{1_P} = amount of fraud that occurs in F_{F_P}; and
$S_{1_{P/C}}$ = amount of fraud that occurs in $F_{F_{P/C}}$.

Note that the right hand side of Equation (7) is minimized when (P) increases.

That is, when the firm seeks the maximum penalty (both civil and criminal), when penalties increase, the right hand side of Equation (7) decreases, and the probability that $F_{E_{P/C}} > F_{E_P}$ increases. When this occurs, the firm can achieve its goal of minimizing costs while maximizing RA_1. Thus, reducing the probability of fraud and making it more likely that $S_{1_P} = \bar{S}$. And $S_{1_{P/C}} = 0$ then becomes a function of increasing penalties; that is, higher penalties imply less fraud by managerial employees.

Therefore, if the firm seeks maximum penalties and utilizes managerial employees, the firm has the maximum probability of decreasing fraud and minimizing firm costs, *ceteris paribus*. Note that this is just a probability. The firm cannot know for certain whether Equation (5) will occur because there is no research to tell us what these probabilities might be for any given control.

However, this does support the strong penalties present in Sarbanes-Oxley for managers (P/C) employees.

Conversely, if the firm is not going to maximize the penalty (which is the case when firms fail to press criminal and civil charges or pay a "living" wage),[10] the firm is maximizing the right-hand side of Equation (7). In this case, it is more likely that:

$$q_H\ell_H(1-q_L) - q_L\ell_L(1-q_H) \leq \frac{e_H(1-q_H) - e_L(1-q_L)}{(p_1)}, \tag{8}$$

and therefore more likely that $F_{E_{P/C}} \leq F_{E_P}$. This, in turn, makes it more likely that $S_{1_{P/C}} = \bar{S}$ and $S_{1_P} = 0$. In this case, the use of non-managerial employees is less costly to the firm, *ceteris paribus*.

IV. DISCUSSION AND CONCLUSION

The major result of this study is that, in terms of deterring fraud, $e > p$, *ceteris paribus*, where e is the collusive effort imposed by separation of duties and p constitutes the penalties imposed when fraud is detected. This suggests that utilizing an internal control system that incorporates separation of duties (SOD) does increase an employee's cost of committing fraud. This increased cost means that, with SOD, an employee will require a greater gain from his fraud efforts than without SOD.

This major finding was *ceteris paribus*. This study also examined the effect of using managerial and non-managerial employees. Given these two choices, controls other than penalties, such as separation of duties, should be employed when a firm uses non-managerial employees. If penalties are used for non-managerial employees, these should be minimized as they appear to be largely ineffective as a fraud disincentive. Conversely, maximum penalties should be imposed on managerial employees. Consequently, this research provides support for the high penalties imposed on top management by the SOX Act of 2002 and also supports the contention that high penalties are more effective at deterring managerial employees from committing fraud than other types of internal control activities. Thus, SOX may have been appropriately designed, if its purpose was to curtail fraud by managers.

Equilibrium analysis indicates that this model is sensitive to the interaction between the probability of detection and the probability of a collusion agreement being reached. Also, if fraud does occur, the *minimum amount taken will be greater with controls than without*.

SOD is thought of as a preventive control. Yet, this analysis indicates that SOD's effectiveness is dependent on the detective controls in the system (e.g., the control activities, internal auditors, and/or external auditors) and the probability that these controls will detect the fraud.

This research used an analytical approach. As with all analytical research, these results are only as generalizable as the assumptions utilized in the model. An important driver of the results is the assumption that all employees will reduce their incidence of fraud if the effort required to commit fraud increases. Anthropological studies of employee theft (e.g., Mars 1982, 15) suggest that tighter controls can induce an otherwise honest employee to commit theft by causing "frustration at doing a highly constrained job." This assumption may, therefore, limit the generalizability of this research, and is an issue to consider in future research.

[10] Recall that the present value of future wages are part of the penalty. To the extent that wages are substandard in any way (too low for the cost of living, too low for the industry, too low relative to comparable employees, etc.), these substandard wages will effectively reduce the impact of the penalty.

The other major assumptions used in the model are widely accepted in practice and academia to support the use of internal controls. Nevertheless, these assumptions are important topics worthy of empirical research. Carmichael called for research investigating internal control activities using more realistic assumptions. Yet, very little research has been done to investigate internal control activities, and even less has been done by relaxing these assumptions. This paper is merely a beginning of what could be an entire field of research.

For example, the result $e > p$ is driven, in part, by the assumption that collusion is costly to the employee—an assumption that drives our use of separation of duties as an effective control in most organizations today (Carmichael 1970, 238). That is, if this assumption were not made by virtually everyone, then we could not justify the use of SOD as an effective internal control. This assumption is implicit in the use of SOD, which is why it was used in this model. Yet, Carmichael (1970) viewed this assumption as unrealistic. Research needs to be done to determine whether, when, and how collusion is costly to employees in order to establish when and how SOD is effective.

This model assumed the controls exist that are cost beneficial. Thus, an important topic for empirical and behavioral researchers is to identify specific examples of controls that satisfy this assumption and to assess the relative cost effectiveness of various internal controls.

One of the provisions of SOX is a whistle-blowing reward for those individuals who cooperate with federal investigations. Some firms also provide rewards to employees for blowing the whistle. It would be interesting to know whether these rewards have a positive impact on deterring fraud.

Finally, the research is not entirely clear whether the size of the theft affects the probability of detection and/or the probability of collusion. Empirical research in this area would be important.

In closing, this paper extends our understanding of internal controls by showing that the relative effectiveness of two types of internal controls, penalties and segregation of duties, to deter fraud differs for managerial and non-managerial employees. Yet, as the concluding discussion indicates, much additional research on internal controls is needed.

APPENDIX
PROOFS OF INTERNAL CONTROL MODELS

Single-Agent Model Description—No SOD

A single agent will misappropriate assets if the expected utility from misappropriation is greater than the utility obtained from wages (current and future.) Current wages are explicitly modeled. Future wages can be thought of as lost to the employee and part of the penalty an employee will pay; thus future wages are incorporated in the penalty by definition. Using Figure 1 this is expressed as:

$$q\ell[w_1 - e_1 - p_1] + q(1-\ell)[w_{11} - e_{11}] + (1-q)[S_1 + w_{11} - e_1] \geq w_1 \tag{2}$$

which is expressed as:

$$q\ell w_1 - q\ell p_1 - q\ell e_1 + qw_1 + - qe_1 - q\ell w_1 + q\ell e_1 + w_1 + S - e_1 - qw_{11} - qS + qe_1 \geq w_1$$

canceling and rearranging terms:

$$(1-q)S_1 - qlp_1 - e_1 \geq 0$$

$$S_1 \geq \frac{e_1 + q\ell(p_1)}{1-q}. \tag{3}$$

Proof of Theorem

***n* = 1**

Let $RA_{1_A} = \frac{e_{1_A}+ql(p_{1_A})}{1-q} s.t. (p_{1_A}) > e_{1_A}$.

Let $RA_{1_B} = \frac{e_{1_B}+ql(p_{1_B})}{1-q} s.t. e_{1_B} > (p_{1_B})$ and $e_{1_B} = (p_{1_A}) > e_{1_A} = (p_{1_B})$ so that $RA_{1_B} = \frac{(p_{1_B})+qle_{1_A}}{1-q}$.

Suppose $RA_{1_A} \geq RA_{1_B}$, then $\frac{e_{1_A}+ql(p_{1_A})}{1-q} \geq \frac{(p_{1_A})+qle_{1_A}}{1-q}$:

$$e_{1_A} + ql(p_{1_A}) \geq (p_{1_A}) + qle_{1_A}$$

$$(1 - ql)e_{1_A} \geq (1 - ql)(p_{1_A})$$

$$e_{1_A} \geq (p_{1_A})$$

which is a contradiction. Therefore, $RA_{1_A} < RA_{1_B}$.

***n* = 2**

Let $RA_{1_A} = \frac{c_{1_{2A}}}{t_2(1-q)} + \frac{e_{1_A}}{1-q} + \frac{ql(p_{1_A})}{1-q} + \frac{(p_{1_A})(1-t_2)(1-r_2)}{t_2(1-q)}$ be s.t. $(p_{1_A}) > e_{1_A} = c_{1_{sA}}$ so that $RA_{1_A} = \frac{e_{1_A}}{t_2(1-q)} + \frac{e_{1_A}}{1-q} + \frac{ql(p_{1_A})}{1-q} + \frac{(p_{1_A})(1-t_2)(1-r_2)}{t_2(1-q)}$.

Let $RA_{1_B} = \frac{c_{1_{2B}}}{t_2(1-q)} + \frac{e_{1_B}}{1-q} + \frac{ql(p_{1_B})}{1-q} + \frac{(p_{1_B})(1-t_2)(1-r_2)}{t_2(1-q)}$ be s.t. $e_{1_B} = c_{1_{2B}} > (p_{1_B})$ and $c_{1_{2B}} = e_{1_B} = (p_{1_A}) > (p_{1_B}) = c_{1_{2A}} = e_{1_A}$ so that $RA_{1_B} = \frac{(p_{1_A})}{t_2(1-q)} + \frac{(p_{1_A})}{1-q} + \frac{e_{1_A}ql}{1-q} + \frac{e_{1_A}(1-t_2)(1-r_2)}{t_2(1-q)}$.

Suppose $RA_{1_A} \geq RA_{1_B}$ then:

$$\frac{e_{1_A}}{t_2(1-q)} + \frac{e_{1_A}}{1-q} + \frac{ql(p_{1_A})}{1-q} + \frac{(p_{1_A})(1-t_2)(1-r_2)}{t_2(1-q)} \geq \frac{(p_{1_A})}{t_2(1-q)} + \frac{(p_{1_A})}{1-q} + \frac{e_{1_A}ql}{1-q} + \frac{e_{1_A}(1-t_2)(1-r_2)}{t_2(1-q)}.$$

Rearranging terms this becomes:

$$e_{1_A}\{1 + t_2 - t_2ql - (1 - t_2)(1 - r_2)\} \geq (p_{1_{A1_A}})\{1 + t_2 - t_2ql - (1 - t_2)(1 - r_2)\} \text{ or}$$

$e_{1_A} \geq (p_{1_A})$ which is a contradiction, so that $RA_{1_A} < RA_{1_B}$.

Similar arguments hold for $e_{1_A} \neq c_{1_{2A}}$ and $e_{1_B} \neq c_{1_{2B}}$.

***n* Agents**

Suppose the Lemma is true for n-agents and $RA_{1_A}(n) < RA_{1_B}(n)$. Let $RA_{1_A}(n+1) = RA_{1_A}(n) + \frac{(1-t_{n+1})c_{1_{n+1_A}}+(1-t_{n+1})(1-r_{n+1})(p_{1_A})}{t_{n+1}(1-q)}$ be s.t. $(p_{1_A}) > e_{1_A} = c_{1_{n+1_A}}$. Let $RA_{1_B}(n+1) = RA_{1_B}(n) + \frac{(1-t_{n+1})c_{1_{n+1_B}}+(1-t_{n+1})(1-r_{n+1})(p_{1_B})}{t_{n+1}(1-q)}$ be s.t. $e_{1_B} = c_{1_{n+1B}} > (p_{1_B})$ and $c_{1_{n+1_B}} = e_{1_B} = (p_{1_A}) > (p_{1_B}) = e_{1_A} = c_{1_{n+1_A}}$ so that:

$$RA_{1_A}(n+1) = RA_{1_A}(n) + \frac{(1 - t_{n+1})e_{1_A} + (1 - t_{n+1})(1 - r_{n+1})(p_{1_A})}{t_{n+1}(1 - q)} \text{ and}$$

$$RA_{1_B}(n+1) = RA_{1_B}(n) + \frac{(1-t_{n+1})(p_{1_A}) + (1-t_{n+1})(1-r_{n+1})e_{1_A}}{t_{n+1}(1-q)}.$$

Suppose $RA_{1_A}(n+1) \geq RA_{1_B}(n+1)$, then:

$$RA_{1_A}(n) + \frac{(1-t_{n+1})e_{1_A} + (1-t_{n+1})(1-r_{n+1})(p_{1_A})}{t_{n+1}(1-q)} \geq RA_{1_B}(n) + \frac{(1-t_{n+1})(p_{1_A}) + (1-t_{n+1})(1-r_{n+1})e_{1_A}}{t_{n+1}(1-q)}$$

$$t_{n+1}(1-q)RA_{1_A}(n) + (1-t_{n+1})e_{1_A} + (1-t_{n+1})(1-r_{n+1})(p_{1_A}) \geq t_{n+1}(1-q)RA_{1_B}(n) + (1-t_{n+1}) \times (p_{1_A}) + (1-t_{n+1})(1-r_{n+1})e_{1_A}$$

$$t_{n+1}(1-q)RA_{1_A}(n) + [(1-t_{n+1}) - (1-t_{n+1})(1-r_{n+1})]e_{1_A} \geq t_{n+1}(1-q)RA_{1_B}(n) + [(1-t_{n+1}) - (1-t_{n+1})(1-r_{n+1})](p_{1_A})$$

$$t_{n+1}(1-q)RA_{1_A}(n) + (1-t_{n+1})r_{n+1}e_{1_A} \geq t_{n+1}(1-q)RA_{1_B}(n) + (1-t_{n+1})r_{n+1}(p_{1_A})$$

$$\frac{t_{n+1}(1-q)}{(1-t_{n+1})r_{n+1}}RA_{1_A}(n) + e_{1_A} \geq \frac{t_{n+1}(1-q)}{(1-t_{n+1})r_{n+1}}RA_{1_B} + p_{1_A}$$

which is a contradiction, so that $RA_{1_A}(n+1) < RA_{1_B}(n+1)$. **Q.E.D.**

(Note that $\frac{t_{n+1}(1-q)}{(1-t_{n+1})r_{n+1}} > 0$ so that if $RA_{1_A}(n) < RA_{1_B}(n)$ then $\frac{t_{n+1}(1-q)}{(1-t_{n+1})r_{n+1}}RA_{1_A}(n) < \frac{t_{n+1}(1-q)}{(1-t_{n+1})r_{n+1}}RA_{1_B}(n)$.)

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2007. *Consideration of Fraud in a Financial Statement Audit*. AU Section 316. PCAOB Standards and Related Rules as of December 2006. New York, NY: AICPA.

Ashton, R. H. 1974. An experimental study of internal control judgments. *Journal of Accounting Research* (Spring): 143–157.

Barra, R. A., and K. Griggs. 2007. Internal controls: Lessons to be learned from fire. *International Journal of Services and Standards* 3 (4): 375–389.

Beck, P. J. 1986. Internal control technologies within industrial organizations. *Managerial and Decision Economics* 7 (2): 81–89.

Becker, G. 1968. Crime and punishment: An economic approach. *The Journal of Political Economy* 76: 169–217.

Bergeron, F. 1986. Factors influencing the use of DP chargeback information. *MIS Quarterly* 10 (3): 225–235.

Bierstaker, J. L., R. G. Brody, and C. Pacini. 2006. Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal* 21 (5): 520–535.

Bodnar, G. 1975. Reliability modeling of internal control systems. *The Accounting Review* 50 (October): 747–757.

Carmichael, D. H. 1970. Behavioral hypotheses of internal control. *The Accounting Review* 45 (April): 235–245.

Cohen, M. 1996. Theories of punishment and empirical trends in corporate criminal sanctions. *Managerial* *and Decision Economies* 17 (Special Issue: Corporate Crime): 399–411.

Cooley, J. W., and B. J. Cooley. 1982. Internal accounting control systems: A simulation program for assessing their reliabilities. *Simulation and Games* 13 (2): 211–231.

Cushing, B. E. 1974. A mathematical approach to the analysis and design of internal control systems. *The Accounting Review* 49 (January): 24–41.

Davis, M. 1996. The impact of rules allocating legal responsibilities between principals and agents. *Managerial and Decision Economics* 17 (Special Issue: Corporate Crime): 413–420.

Demski, J. S., N. Dopuch, B. Lev, J. Ronen, G. Searfoss, and S. Sunder. 1991. *A Statement on the State of Academic Accounting*. Statement to the Research Director of the American Accounting Association. Nashville, TN: American Accounting Association.

Devor, R., T. Chang, and J. Sutherland. 1992. *Statistical Quality Design and Control: Contemporary Concepts and Methods*. New York, NY: Macmillan Publishing Company.

Doty, C., A. Sen, and S. Wang. 1989. Effect of internal controls in data base design. *Journal of Information Systems* (Spring): 70–91.

Economist, The. 2004. The tipping point. *The Economist* 371 (Issue 8370): 28.

Felix, W. L., and M. Niles. 1988. Research in internal control evaluation. *Auditing: A Journal of Practice & Theory* 7 (2): 43–60.

Grimlund, R. A. 1982. An integration of internal control system and account balance evidence. *Journal of Accounting Research* 20 (2): 316–342.

Heier, J., M. T. Dugan, and D. L. Sayers. 2005. A century of debate for internal controls and their assessment: A study of reactive evolution. *Accounting History* 10 (3): 39–70.

Helal, S. R. 1983. An application of reliability engineering concepts to the analysis of the accounting control systems. Unpublished dissertation, University of Illinois.

Hollinger, R., and P. Clark. 1983. *Theft by Employees*. Lexington, MA.: Lexington Books.

Hooks, K., K. Steven, and J. Schultz. 1994. Enhancing communication to assist in fraud prevention and detection. *Auditing: A Journal of Practice & Theory* 13 (2): 86–117.

Hornik, S. and B. Ruf. 1997. Expert systems usage and knowledge acquisitions: An empirical assessment of analogical reasoning in the evaluation of internal controls. *Journal of Information Systems* 11 (2): 57–74.

Knechel, W. R. 1983. The use of quantitative models in the review and evaluation of internal control: A survey and review. *Journal of Accounting Literature* 2: 205–219.

Kofman, F. and J. Lawarree. 1993. Collusion in hierarchical agency. *Econometrica* 61 (3): 629–656.

LaVan, H., and M. Katz. 2005–2006. Disciplining employees for free speech, whistle blowing, and political Activities. *Journal of Individual Employment Rights* 12 (2): 119–135.

Luengo, A. 2004. Characteristics and psychiatric comorbidity in pathological slot-machine gamblers in treatment: A study of population below 30 years old. *Adicciones* 16 (1): 7–18.

Maher, K. 2006. Ethical but unemployed. *ABA Journal* 92 (3): 28–29.

Mars, G. 1982. *Cheats at Work: An Anthropology of Workplace Crime*. Boston, MA.: George Allen & Unwin.

Mattessich, R. 1995. *Critique of Accounting: Examination of the Foundations and Normative Structure of an Applied Discipline*. Westport, CT: Quorum Books.

Mautz, R. K., and D. Mini. 1966. Internal control evaluation and audit program modification. *The Accounting Review* 41 (2): 283–291.

Murthy, U. 2004. An analysis of the effects of continuous monitoring controls on e-commerce system performance. *Journal of Information Systems* 18 (2): 29–47.

Nolan, R. 1977. Effects of chargeout on user/manager attitudes. *Communications of the ACM* 20 (3): 177–185.

Olson, M., and B. Ives. 1982. Chargeback systems and user involvement in information systems—An empirical investigation. *MIS Quarterly* 6 (2): 47–60.

Owen, E. 2006. What traffic wardens can teach us. *New Statesman* 135 (4776): 18.

Polinsky, A., and S. Shavell. 1993. Should employees be subject to fines and imprisonment given the existence of corporate liability? *International Review of Law and Economics* 13: 239–257.

———. 2000. The economic theory of public enforcement of law. *Journal of Economic Literature* 38: 45–76.

Public Company Accounting Oversight Board (PCAOB). 2008. *An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements*. AS No. 5. PCAOB Standards and Related Rules as of October 1, 2008. New York, NY: PCAOB.

Rae, K., and N. Subramaniam. 2008. Quality of internal control procedures: Antecedents and moderating effects on organizational justice and employee fraud. *Managerial Auditing Journal* 23 (2): 104–124.

Robinson, M. A. 1981. An integer goal programming methodology for multiple objective cost/benefit analysis of internal accounting control systems. Unpublished dissertation, University of Illinois.

Sarbanes-Oxley Act. 2002. 107th Congress of the United States, H.R. 3763. Washington, D.C.: Government Printing Office.

Schachter, H. 2009. Welcome the whistle-blower. *The Globe and Mail; Canada* (June 22): B7.

Sen, T., and J. Yardley. 1989. Are chargeback systems effective? An information processing study. *Journal of Information Systems* 2 (3): 92–103.

Simon, J. R. 1974. Standards for the evaluation of internal controls—An empirical test in the public sector. Unpublished dissertation, University of Illinois.

Simpson, S., and C. Koper. 1992. Deterring corporate crime. *Criminology* 30 (3): 347–375.

Srinidhi, B. N. 1988. Mathematical formulation of the task segregation problem in internal control system design. *Decision Sciences* 19: 1–16.

Varma, K., and A. Doob. 1998. Deterring economic crimes: The case of tax evasion. *Canadian Journal of Criminology* 40 (2): 165–184.

Vaz, E. 1969. Delinquency and the youth culture: Upper and middle class boys. *The Journal of Criminal Law and Criminology* 60 (1): 33–46.

Viator, R. and M. Curtis. 1998. Computer auditor reliance on automated and nonautomated controls as a function of training and experience. *Journal of Information System* 12 (1): 19–30.

Wales, S. 1965. *Embezzlement and Its Control*. Richmond, IN: Igelman Printers & Publishers.

Wand, Y., and R. Weber. 1989. A model of control and audit procedure change in evolving data processing systems. *The Accounting Review* 64 (1): 87–107.

Wells, J. T. 2008. The real secret to fraud deterrence. *The CPA Journal* 78 (6): 6.

Williams, K., and J. Gibbs. 1981. Deterrence and knowledge of statutory penalties. *The Sociological Quarterly* 22: 591–606.