FRAUD DYNAMICS AND CONTROLS IN ORGANIZATIONS

Jon S. Davis
Wisconsin School of Business
University of Wisconsin–Madison
975 University Ave.
Madison, WI 53706
608-263-4264
608-263-0477(fax)
jdavis@bus.wisc.edu

Heather L. Pesch
Wisconsin School of Business
University of Wisconsin–Madison

July 7, 2010

Version 3.1 Comments Welcome.

The authors acknowledge the support of the Arthur Andersen Center for Financial Reporting and the AICPA Center for Audit Quality. In addition, they would like to thank Laura Michalski for her helpful comments on an initial reading of this paper and comments from the participants at the Queen’s University Fraud Conference and workshops at University of Wisconsin-Madison, and Florida international University.
Fraud Dynamics and Controls in Organizations

Abstract

This paper develops an agent-based model to examine the emergent dynamic characteristics of fraud in organizations. In the model, individual heterogeneous agents, each of whom can have motive and opportunity to commit fraud, and ability to rationalize fraud, interact with each other. This interaction provides a mechanism for cultural transmission through which attitudes and rationalization regarding fraud can spread. In our benchmark model (in which every agent has motive and the perceived opportunity to commit fraud), we find two classes of organization identifiable by their different cultural transmission characteristics. In one class, we observe fraud tending toward a level consistent with a (Lyapunov) stable equilibrium. In the other class, fraud dynamics are characterized by extreme behaviors, with mostly honest organizations suddenly changing their state to predominantly fraudulent behavior and vice versa. These swings occur randomly over time. We then modify our model to develop proxies for various mechanisms thought to impact fraud in organizations, including the introduction of a system of internal controls, organizational hierarchy (tone at the top), introduction of a code of ethics, and enforcement efforts to detect and punish fraud. Each of these mechanisms has different impacts on the two classes of organizations in our benchmark model; with some mechanisms being more effective in organizations exhibiting equilibrium fraud and other mechanisms being more effective in organizations exhibiting extreme, rapidly changing behaviors. Our analysis and results have general implications for designing programs aimed at preventing fraud and for fraud risk assessment within the audit context.

Keywords: Agent-based modeling; fraud; internal controls; dynamics.

JEL Descriptors: M42, C63, K42

Data and computer code are available from the authors on request.
I. INTRODUCTION

The cost of corporate fraud is high.\textsuperscript{1} The ACFE and Peltier-Rivest (2007) estimate that fraud costs typical Canadian organizations five percent of their annual revenues. Applying this percentage to the 2008 Canadian gross domestic product of $1.6 trillion leads to an estimate of roughly $80 billion in fraud losses annually. Using this same approach, the ACFE (2008) estimates that loss to corporate fraud in the United States approaches US$1 trillion annually.

Because of the magnitude of losses and requirements imposed on auditors to explicitly address fraud (AICPA, 2009), the topic has become popular in the accounting literature. The vast majority of the research addresses fraud risk assessment by auditors (e.g., Bell and Carcello, 2000; Wilks and Zimbelman 2004; Carpenter 2007) and fraud detection (e.g., Matsumura and Tucker 1992; Cleary and Thibodeau 2005; Hoffman and Zimbelman 2009). Other streams of research examine fraud incentives (e.g., Gillett and Uddin 2005; Erickson et al. 2006) and the correlation of fraud with financial statement reporting choices and corporate governance variables (e.g., Beasley 1996; Sharma 2004; Jones et al. 2008).

In light of the high cost of corporate fraud, one would expect to observe substantial research investigating the efficacy of mechanisms designed to prevent or reduce fraud. However, despite its potential importance, a review of the research on fraud reveals a striking dearth of work examining the effectiveness of various prevention mechanisms, except for the role of audits as a deterrent (e.g., see Uecker et al. 1981; Schneider and Wilner 1990; Finley 1994). This lack of work on fraud prevention is likely due to the nature of fraud as a hidden crime. Because the

\textsuperscript{1} For purposes of our model, we define fraud as all forms of occupational fraud including asset misappropriation, corruption, and financial statement fraud.
extent of fraud is usually unknown in an organization, measuring the effectiveness of prevention mechanisms is difficult using traditional empirical methods.

In addition, research on fraud in organizations tends to focus at either the individual level or the organizational level (Holtfreter 2005). To date, no attempt has been made to explicitly link individual behavior in the organization to organizational outcomes within the fraud context. Understanding the individual–organization link is important because a focus on either individual behavior or the organization in isolation turns a blind eye to the social process through which individuals behaviors are influenced by the organization as a whole and vice versa. In other words, a narrow focus on individual behaviors or on the organization ignores the sociology of the organization, which may have profound effects on fraud outcomes and the efficacy of fraud prevention mechanisms.

We develop a model of fraud in organizations that allows an evaluation of the relative efficacy of mechanisms designed prevent fraud while explicitly recognizing the social processes underlying the formation of organizational norms. To develop our model, we use a method that is relatively new in accounting research, called agent-based modeling (ABM). ABM is designed to study the emergence of macro-level phenomena from micro-level interactions so it is well suited to address questions involving organizational outcomes (viz., fraud) resulting from the interactions between individuals within the organization and organizational variables.

2 Recognizing the failure to link individual- and organization-level research in fraud, Holtfreter (2005) attempts to provide some indirect insight into the link via a descriptive analysis of fraudulent individuals and the organizations that are their victims.

3 See, however, Kim and Xiao (2008), who examine the link between individual behavior and aggregate outcomes in the context of fraud in a public delivery program in health care.
Our model is comprised of an organization\textsuperscript{4} represented by 100 independent, heterogeneous agents (employees) and a set of simple interaction rules. In accordance with Cressey’s (1953) occupational fraud model (known as the “fraud triangle hypothesis”), any agent in our model possessing motive, opportunity, and a rationalization (creation of an attitude or belief) that frames the fraudulent act as acceptable will commit fraud. We allow the organization to evolve through interactions among agents with an eye toward aggregate fraud levels and the dynamics of fraud over time. We begin with a benchmark model in which all agents have opportunity and motive. We then modify our model to investigate the impact of mechanisms to prevent or detect fraud. We first investigate the impact of modifying the likelihood that agents will perceive the opportunity to commit fraud.\textsuperscript{5} Next, we consider the impact of tone at the top by introducing a hierarchy in which higher-level employees exert greater influence than lower-level employees. Then we consider the impact of changes in our model that could proxy for the introduction of a code of ethics and enforcement efforts.

In our benchmark model, two state distributions emerge, depending upon how susceptible individual agents are to social influence. When average susceptibility is low, a (Lyapunov) stable equilibrium level of fraud in the organization emerges. The histogram showing the frequency of fraud over time exhibits an inverted-U shape in this state. When average susceptibility is moderate to high, a very different, U-shaped state distribution of fraud emerges. This distribution

\begin{itemize}
\item \textsuperscript{4} In our model, the term “organization” could apply to an entire business entity, a branch, a division, an office, or even a department within an office.
\item \textsuperscript{5} Changes in perceived opportunity to commit fraud could arise through the introduction of a system of internal controls.
\end{itemize}
is characterized by rapid shifts in aggregate fraud levels between extremes where either virtually no one in the organization is committing fraud or virtually everyone is.

When we consider mechanisms to prevent and detect fraud, we find that a reduction in perceived opportunity or introduction of tone at the top in an organization do not qualitatively impact the shape of the state distributions or dynamics observed in our benchmark model. However, when we introduce a proxy for a code of ethics into an organization with moderate to high average emulation likelihoods, the nature of the U shape is transformed; average fraud levels reduce to near zero and fraud dynamics stabilize. In contrast, our proxy for a code of ethics does not qualitatively affect fraud in organizations with low average emulation likelihoods. The average aggregate fraud level reduces only slightly and the characteristics of the inverted U shape persist. Our findings suggest that the role of a code of ethics in fraud prevention is contingent on the nature of the organization, a relation that may prove important for fraud risk assessment by auditors. We also find that enforcement efforts (detection of fraud and termination of fraudsters) can be effective at reducing average fraud levels to near zero in both types of organizations. However, the effectiveness of enforcement regimes at preventing widespread fraud outbreaks also appears to be contingent on the type of organization and individual susceptibilities to fraud.

This paper continues with a brief introduction to ABM. This methodological introduction is followed by the development of a benchmark model in an organization with no interventions to prevent or detect and eliminate fraud. We then modify the benchmark model to examine the independent effects of implementing a system of internal controls, allowing for a hierarchy of authority and influence in the organization (tone at the top), introducing a code of ethics in the
organization, and allowing the organization to detect and terminate fraudsters. This paper ends with our conclusions and a discussion of the implications of our analysis.

II. AGENT-BASED MODELS

To address our research question, we adopt ABM as a method. ABM has been identified as a particularly apt methodology for analyzing emergent behavior in organizations (Prietula et al., 1998), particularly in studying fraud (Kim and Xiao, 2008) and certain other aspects of operational risk (Bonabeau, 2002).

Epstein (2006) identifies several shortcomings in traditional theoretical work in the social sciences. When aggregate behavior is the research subject, heroic assumptions about individual behavior and the population being modeled are typically required to maintain tractability (e.g., perfect rationality and homogeneity of individual actors). While these assumptions bear little resemblance to human behavior, it is often argued that such simplifications are necessary because no rigorous method exists that would allow their relaxation. Similarly, in traditional theory, the notion of an equilibrium plays a predominant role as a solution concept. Yet, in the natural ecology of human society, equilibria are rarely (if ever) observed. Instead, one would expect that nonequilibrium dynamics would be the natural focus for research. Defenders of traditional theoretical methods would argue that there are no straightforward approaches to studying dynamics in the social sciences. Experimental research in the social sciences that attempts to test hypotheses linking heterogeneous individual behavior to aggregate behavioral outcomes is also challenging because of an exiguity of theoretical work linking realistic individual behaviors to aggregate phenomena. Finally, the stove-pipe structure of the social science disciplines (sociology, economics, psychology, anthropology) represent artificial divisions based on the
mistaken assumption that no single approach can examine the evolution and emergence of social behavior.

ABM differs in fundamental ways from traditional social science models and its differences promise a solution to many of the shortcomings identified. The method allows for the specification of heterogeneous actors who follow simple, realistic (boundedly rational) behavioral rules. Its focus is on the emergence of macro-level phenomena from micro-level behavior and is therefore well suited for the study of social phenomena. Because ABMs are evolutionary, the natural focus of the research is on dynamic behavior rather than on equilibria that may never be achieved. Finally, ABMs naturally cross the boundaries of the various social sciences because of the requisite focus on modeling realistic individual behaviors (e.g., psychology), spatial and ecological considerations (anthropology), social interaction (e.g., sociology) and a wide range of other potential cross-disciplinary considerations.

The earliest social sciences work employing an ABM methodology was performed by Schelling (1969, 1971a, 1971b, 1978), who examined the antecedents of racially segregated neighborhoods. Schelling’s models randomly placed agents in a line or on a lattice. Agents were then allowed to move according to a set of rules and an individual preference for similar neighbors. The primary result in his work is that agents require only a very small preference for living near similar agents to create highly segregated neighborhoods. At the time, Schelling performed his simulations by hand with pencil and paper or with coins and a checkerboard. Since this early research, work using ABMs in the social sciences has advanced considerably (along

\[ \text{沿着} \]

The micro-level focus of agent-based models confers another benefit: It avoids the problematic representative agent assumption that is common in macro-level models (for a discussion of the shortcomings of the representative agent assumption, see Kirman 1992).
with available computational power), to the point where very large scale simulations have been
performed to examine a wide range of issues, from the disappearance of the Anasazi indians in
the southwestern United States (Dean et al. 2000) to how taxpayer behavior changes in response
to interactions with tax experts and with social circles in the presence of various tax agency
interventions (Carley and Maxwell 2006).

A fully specified ABM consists of agents (e.g., individuals in an organization, traders in a
market, organizations in an economy, or trees in a forest), an environment in which the agents
“live” and a set of rules that govern agent interaction with other agents and their environment.
Agents are characterized in an ABM by a collection of internal states, endowments (knowledge
and assets), and simple behavioral rules that recognize the existence of bounded rationality.
Some of these characteristics are static (unchanging over time), while others may change in
response to interactions with the environment or with other agents. Environments can be static or
can change on the basis of rules or as a result of interaction with agents. Environments can be
represented in a variety of ways. When location or resource placement is important in a model (a
common issue in anthropological or ecological research), the environment can be represented
spatially, using a lattice or a landscape developed from a geographic information system. In
economics, the environment of choice is a market (e.g., Gode and Sunder 1993). In research
examining sociological or sociopsychological phenomena (e.g., the development of a culture of
fraud in organizations in our instance), a social network (Breiger and Carley 2003) might be
favored. Finally, a set of institutional rules is specified that define how agents will interact with
each other and with their environment. As with agent and environmental characteristics, these
rules can be static, dynamic, or adaptive. A simple rule for an agent might be to sell to another
agent if the offer price is less than the bid price or in the context of our fraud model, to commit
fraud if one can either rationalize fraud or believe that it is acceptable behavior and if both motive and opportunity are present.

Once the elements of the ABM have been developed (usually instantiated in a computer program\textsuperscript{7}), the model is allowed to evolve over time, allowing agents to interact with each other and the environment. As the model evolves, the research focuses on the spontaneous emergence of aggregate or group behaviors resulting from interactions at the micro (agent) level. This approach has been characterized by Epstein and Axtell (1996) as attempting to “grow” social phenomena from the bottom up (modeling individual behavior) rather than from the top down (directly modeling aggregate phenomena). Thus, ABMs are not macro models but, rather, models of individual behavior and social interaction that produce macro-level behaviors.

Since ABMs are simulations, they rely on both deduction and induction. While each ABM is a strict deduction and constitutes a sufficiency theorem, multiple simulations can be thought of as a distribution of theorems that together are used to inductively test a proposition.

\textsuperscript{7} We employ Mathematica 7.0 (Wolfram Research Inc. 2008) as the programming platform for our model.
Thus, the flavor of ABM research is more similar to laboratory experimentation than to a deductive proof.8

III. BENCHMARK MODEL

Our model of fraud in an organization is based on Cressey’s (1953) occupational fraud model (known as the “fraud triangle hypothesis”), which still prevails as a popular view of the necessary and sufficient precursors for an individual’s decision to commit fraud.9 Cressey’s characterization identifies three key determinants of fraud. When the conjunction of these factors exists, an individual will commit fraud. The factors are a perceived non-sharable financial need (or, more generally, a motive), a perceived opportunity to commit fraud, and a rationalization (creation of an attitude or belief) that frames the fraudulent act as acceptable behavior. In our

8 Epstein (1999) observes that ABMs represent a new approach to science that can be used as instruments for either theory development or theory testing. Rather than fitting neatly into inductive or deductive realms, ABMs are more appropriately thought of as a generative form of science. To explain a macroscopic social phenomenon, the generativist asks, “How could decentralized local interactions of heterogeneous autonomous agents generate the given regularity?” (Epstein 1999, 41). Put another way, the generativist’s motto is “If you didn’t grow it, you didn’t explain its emergence” (Epstein 1999, 46).

9 Cressey’s hypothesis is incorporated in a discussion of the characteristics of fraud in the AICPA’s 2009 exposure draft of Statement on Auditing Standards (SAS) 99, which addresses the auditor’s responsibilities relating to fraud in an audit of financial statements. In addition, Cressey’s hypothesis is discussed at length in the context of determinants of occupational fraud in the Fraud Examiner’s Manual (Association of Certified Fraud Examiners 2007).
model, agents become fraudsters if they face a conjunction of perceived opportunity \((O)\), motive \((M)\), and an attitude \((A)\), formed via rationalization that fraud is an acceptable behavior, or:

\[ O \land M \land A \rightarrow F. \]

Conversely, over time, if a fraudster no longer has opportunity, motive or attitude, then he or she will reform to become an honest agent.\(^{10}\)

Each of the agents in our model may or may not have a motive for fraud (determined randomly with some predetermined probability at each step of the simulation).\(^{11}\) Perceived opportunity is an organizational-level variable that proxies for the overall strength of a system of internal controls. It is represented as the probability that each agent will perceive an opportunity to commit fraud: For example, a 20 percent opportunity implies that each agent independently has a 20 percent chance of perceiving an opportunity to commit fraud at each point in the

\(^{10}\) For simplicity, we assume a free flow between the honest and fraudster classes. If all three legs of the fraud triangle exist, an individual commits fraud. Conversely, if one of the legs ceases to exist (e.g., opportunity no longer exists or the agent can no longer rationalize), then the agent no longer commits fraud. In the natural ecology, such a free flow is not always observed; instead, the decision to commit fraud is sometimes “sticky.” Fraud often requires additional fraud in the future to keep the original fraud hidden. An assumption of sticky fraud in our model would raise the level of fraud on average in the population and would be equivalent to an increase in the likelihood of the cultural transmission of fraud. The effect of introducing “sticky” fraud is the opposite of that observed in our “code of ethics” manipulation, addressed later in the paper.

\(^{11}\) At the outset, for simplicity, we assume that every agent has a motive for fraud but the model admits the possibility of heterogeneity in motives across individual agents.
Finally, an individual’s ability to rationalize fraud in our model is a function of both organizational culture and factors exogenous to the organization.

**Characterizing Agents**

We begin developing our model of fraud in organizations by characterizing individual agents. In particular, each agent is represented by a vector whose elements indicate the agent’s attributes (endowments and individual behavioral attributes). These endowments and attributes are represented by numbers and lists of numbers. In our benchmark model, agent attributes include the following:

- A unique integer that identifies the agent (a “name”).
- Four independent probabilities, each drawn from a bounded uniform distribution. The first two represent the likelihood of the agent taking on a particular characteristic (motive for fraud and perceived opportunity to commit fraud) and the second two represent (i) the likelihood \( p \) of one’s attitude toward fraud changing as a result of factors not related to interaction with other agents and (ii) the likelihood \( q \) of one’s attitude toward fraud changing as a result of interacting with co-workers who have rationalized fraud. These probabilities are static and, with the exception of the opportunity likelihood, randomly determined for each agent. The opportunity likelihood is a static organizational-level variable.
- Four binary variables indicating whether a motive for fraud is present, whether perceived opportunity is present, whether fraud has been rationalized, and finally whether the agent is committing fraud. The presence of motive, opportunity, and rationalization is determined at each step in the simulation for each agent based on the assigned probabilities above. Fraud exists if motive, opportunity and rationalization exist.
The Organization

To create an organization, we develop a matrix. Each row in the matrix is an agent vector. To allow for interaction between agents, we represent a social network (a set of co-workers) for each agent by adding a list to each agent’s vector, where each element in the list is an integer referring to another agent’s name. In our social network, co-worker relationships are symmetric (if agent 1 knows agent 3, then the reverse is also true). The list of co-workers assigned to each agent is randomly determined (subject to the symmetry constraint) and remains static throughout the model’s evolution.

Evolving the Organization

After establishing a starting population in the organization, we allow the model to evolve by repeatedly applying a complex transformation to the organization matrix. The matrix transformation updates agent states via a set of behavioral rules (e.g., if motive, opportunity and rationalization exist, then the fraud variable should be positive for the agent). It implements interaction between agents by repeatedly and randomly pairing each agent with a member of his or her social network as the organization evolves. The pairing allows one agent to observe another. As noted previously the observing agent will emulate the behavior (or attitude)\(^ {12} \) of the observed with probability \( q \). Consider, for example, an agent who goes to lunch with co-workers

\(^ {12} \) The model presented in this paper assumes that agent behavior is influenced by other agents’ attitudes and actions. We also evaluated an alternative model where agent behavior is influenced only by other agents’ actions. The only qualitative effect is observed in the context reducing opportunity to commit fraud (e.g., via a system of internal controls). In this instance, u-shaped organizations respond to reduced opportunity in a fashion similar to that observed in our “code of ethics” analysis.
and observes that one of them treats the personal lunch as a reimbursable business expense. We assume that the more often this behavior is observed, the more likely the agent will begin to rationalize committing similar behavior. We also allow for the possibility that one’s ability to rationalize fraud can change (with probability $p$) independently of observing others (e.g., as a result of family upbringing or moral values).

In the model, agents’ rationalizations about the acceptability of fraud evolve according to their particular experiences with other agents and their personal proclivities. At any given time, agent behaviors and rationalizations will be heterogenous because each agent has a unique set of characteristics and different experiences in the organization. Any given agent’s behavior may or may not represent the overall behavior of the organization. One particular agent can be a fraudster at a given time while the remaining agents are honest. When interacting with an honest agent in the organization, the fraudster can trigger a fraud rationalization in the honest agent (and possibly convert the honest agent into a fraudster, if both motive and perceived opportunity exist) or the honest agent can convert the fraudster into an honest person. In the case of two honest agents interacting, one or both agents can become able to rationalize fraud because of factors exogenous to their interaction. These rules for interaction and behavior define a social dynamic. As the organization evolves, the culture changes dynamically in response to both agent interactions and their spontaneous behavior. The model is “bottom up,” in that a culture of fraud emerges spontaneously in the organization as a result of the interactions of individual agents with each other.
An Example

Recall that our model begins with an initial organization represented by a matrix in which each row represents an agent and each element in a row represents an agent attribute. For clarity, we present this example of an organization matrix with a population size of five:

\[
\begin{array}{cccccccccccc}
ID & p(M) & M & p & q & A & p(O) & O & F & E & S & SN \\
1 & 0.00449253 & 0 & 0.0242858 & 0.90035 & 0.95 & 1 & 0 & 0 & 1 & \{4\} \\
2 & 0.426662 & 0 & 0.0292374 & 0.585986 & 0.95 & 1 & 0 & 0 & 0 & \{\} \\
3 & 0.354574 & 0 & 0.0322799 & 0.511431 & 0.95 & 1 & 0 & 0 & 2 & \{4, 5\} \\
4 & 0.0897837 & 0 & 0.036227 & 0.525595 & 0.95 & 1 & 0 & 0 & 2 & \{1, 3\} \\
5 & 0.496052 & 0 & 0.0205544 & 0.892721 & 0.95 & 1 & 0 & 0 & 1 & \{3\} \\
\end{array}
\]

The elements in each column represent the following agent attributes:

- **ID** = agent’s unique identifier
- **p(M)** = likelihood of agent’s motive to commit fraud changing
- **M** = a binary variable indicating the presence of motive
- **p** = likelihood of agent rationalizing (or ceasing to rationalize) as a result of factors exogenous to agent interactions
- **q** = likelihood of agent rationalizing (or ceasing to rationalize) as a result of interactions with co-workers
- **A** = binary variable indicating the presence of rationalization
- **p(O)** = likelihood of agent perceiving an opportunity to commit fraud
- **O** = binary variable indicating the perceived opportunity to commit fraud
- **F** = binary variable indicating whether agent is committing fraud.
- **E** = binary variable to be used later when enforcement is considered
- **S** = social network size
- **SN** = list of agent’s social network
In the sample matrix, agent 3’s likelihood of a change in motive is 0.354, opportunity is currently perceived as present, no fraud is being committed, the enforcement variable is set to 0, the agent’s social network size is two, and the social network consists of agents 4 and 5. The matrix represents the organization and agent characteristics for one period in time.

As noted previously we iteratively apply a series of transformations to this matrix, which allows agents to interact and the organization to evolve over time. For example, assume the sample matrix represents the organization at time $t$. To move to time $t + 1$, we apply the transformation rules to the matrix once. As a result of this application agents interact and update their beliefs and behaviors. For the purposes of our example, assume agent 4 observes agent 1 during the transformation. The resulting matrix illustrates the states of agents in the organization at time $t + 1$, after the transformation has been applied. Comparing this new matrix with the previous, original one, two changes are evident. First, agent 1’s $A$ variable has changed from 0 to 1 signifying that agent 1 now rationalizes fraud as a result of factors exogenous to agent interaction. Second, because agent 4 has been influenced by agent 1, agent 4 now also rationalizes that fraud is acceptable.

<table>
<thead>
<tr>
<th>ID</th>
<th>$p(M)$</th>
<th>M</th>
<th>p</th>
<th>q</th>
<th>A</th>
<th>$p(O)$</th>
<th>O</th>
<th>F</th>
<th>E</th>
<th>S</th>
<th>SN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.00449253</td>
<td>0</td>
<td>0.0242858</td>
<td>0.90035</td>
<td>1</td>
<td>0.95</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>{4}</td>
</tr>
<tr>
<td>2</td>
<td>0.426662</td>
<td>0</td>
<td>0.0292374</td>
<td>0.585986</td>
<td>0</td>
<td>0.95</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>{}</td>
</tr>
<tr>
<td>3</td>
<td>0.354574</td>
<td>0</td>
<td>0.0322799</td>
<td>0.511431</td>
<td>0</td>
<td>0.95</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>{4, 5}</td>
</tr>
<tr>
<td>4</td>
<td>0.0897837</td>
<td>0</td>
<td>0.036227</td>
<td>0.525595</td>
<td>1</td>
<td>0.95</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>{1, 3}</td>
</tr>
<tr>
<td>5</td>
<td>0.496052</td>
<td>0</td>
<td>0.0205544</td>
<td>0.892721</td>
<td>0</td>
<td>0.95</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>{3}</td>
</tr>
</tbody>
</table>

In this matrix we can see that although agents 1 and 4 now rationalize fraud and both perceive the opportunity to commit fraud, neither has motive and therefore neither commits fraud in the period $t + 1$. 
**Benchmark Model Design**

We use ten unique starting populations in order to study a sample of possible realizations from the process.\(^{13}\) To establish a benchmark, we initially assume that every agent has a motive for fraud and that the organization has no controls in place (every agent perceives an opportunity for fraud). We set the size of the organization to 100 agents and observe 15,000 interaction periods. To evaluate sensitivity in starting conditions, for a subset of five of the populations, we systematically vary the number of agents who begin with a rationalization for fraud. In the first set of simulations, all agents start with a fraud rationalization; in the second set, all agents start without a fraud rationalization; and, in the third set of simulations, agents are randomly assigned (with a 50 percent probability) to begin with either a fraud rationalization or no fraud rationalization.\(^{14}\) For the remaining five starting populations, agents are randomly assigned (with 50 percent probability) to begin with either the presence or absence of fraud rationalization. Finally, we begin by allowing agents to have a very small but heterogeneous likelihood of

---

\(^{13}\) Our initial model design (choice of parameters) was constrained by computational power and practicality (approximately 5000 hours of computing time were expended analyzing our models).

\(^{14}\) Since motive and opportunity exist for everyone in our benchmark analysis, everyone at the outset of the organization is either a fraudster or honest, or approximately one-half of the population are fraudsters. Even though there appears to be homogeneity in behavior in the starting population under some conditions, recall that each agent is unique in individual characteristics such that populations will evolve along different paths.
rationalizing (or ceasing to rationalize) fraud as a result of factors exogenous to agent interaction (probability $p$ drawn independently for each agent from a uniform distribution from 0 to 0.005).\textsuperscript{15}

**Emergence: Two States**

In the benchmark analysis, we study the effect of a systematic change in individuals’ tendencies to be impacted by the behavior of others in the organization (emulation likelihood). We explore the entire parameter range by varying the average emulation likelihood in increments of 5 percent. Each subject is initially assigned an independent probability drawn from a uniform distribution between a maximum and a minimum value, previously denoted as $q$. The assigned

\begin{itemize}
  \item Our choice of a small probability here is consistent with a belief that individuals’ attitudes regarding the acceptability of fraud are relatively stable in response to non-organizational factors.
  \item As noted by the AICPA (2009) in their exposure draft of the revised SAS 99, the ability to rationalize can be affected, in part, by one’s attitude, character, or set of ethical values (which we believe to be stable with only small likelihood of change over time). This is the aspect of rationalization captured by our small exogenous probability $p$. In contrast, the likelihood of being influenced via interactions in the organization, $q$, captures a second source of rationalization noted in SAS 99, the organizational environment.
\end{itemize}
probability is static for each agent. Since the likelihood is bounded, as we approach the extremes we manipulate either the minimum or the maximum to reach the desired average.\textsuperscript{16}

Our analysis focuses on both the overall state distribution of fraud in the organization that emerges over time (a distribution of the proportion of fraudsters in the organization over time in the form of a histogram) and on the dynamic path of fraud in the organization with an eye toward the periodic existence of widespread fraud in the organization. Our histogram shows the number of periods during which \( n \) agents are committing fraud, where \( n \) ranges from 0 to 100 (the entire population). In Figure 1a, for example, the \( y \) axis represents the number of periods in which a level of fraud was observed, while the \( x \) axis represents the number of agents committing fraud. Figure 1b illustrates changes in the frequency of fraud over time, which can have implications for auditors. In the time series, the \( y \) axis represents the number of agents committing fraud in a given period and ranges from 0 to 100 (the entire population) and the \( x \) axis represents time (or interactions) and ranges from 1 to 15,000.

\textbf{Insert Figure 1 Here}

\textsuperscript{16} For example, if the maximum likelihood is set at 100 percent and the minimum at 0, the average likelihood is 50 percent. Holding the floor constant at 0, as the ceiling is reduced from 100 percent, the average will drop below 50 percent. To examine the parameter space where averages exceed 50 percent, we increase the floor and hold the ceiling constant at 100 percent. Since this approach to manipulating the mean value of \( q \) also varies the range from which the value of \( q \) is drawn, we performed additional analysis using a variety of mean preserving ranges. Our results are qualitatively similar across these ranges, with the exception that a u-shaped distribution is observed more frequently when mean-preserving range is reduced.
Two states emerge in our analysis. At relatively high emulation likelihoods, the majority of periods exhibit extreme behavior, where either virtually all agents are committing fraud or virtually no agents are committing fraud. We call this state the “U-shaped” distribution after the appearance of its associated histogram. Figure 1a illustrates this U-shaped distribution from one of our simulations where the mean emulation likelihood is 60 percent. Figure 1b (from the same simulation) shows a typical time series for a U-shaped organization, characterized by rapid swings between extremes. For example, in Figure 1b, at approximately the 11,000th pairing, a rapid shift occurs from a period in which few agents are committing fraud to a period in which virtually everyone is committing fraud.\footnote{The sudden extreme shifts observed in our model are consistent with the behavior observed in similar characterizations of recruitment developed to explain the behavior of ants (e.g., see Kirman 1993).} We find that the characteristic U shape and sudden dramatic shifts between extreme states persist across starting conditions ranging from very high average emulation probabilities down to approximately 30 percent.\footnote{Unless noted otherwise, the results are consistent and clearly observable across all starting populations and all initial fraud distributions in the populations.}

At low average emulation likelihoods (30 percent and below), a very different outcome emerges. Instead of extremes, the population tends toward what appears to be a (Lyapunov) stable equilibrium\footnote{In the study of dynamics, an equilibrium can be considered stable under different benchmarks. Lyapunov stability is achieved if outcomes are in the neighborhood of the equilibrium and tend to remain in the neighborhood over time.} level of fraud within the organization. We call this the inverted-U shape after the appearance of the histogram associated with this state, illustrated in Figure 2a. Notice in this
example that the majority of periods are characterized by roughly half of the organization committing fraud. When we consider the evolution of fraud behavior over time in Figure 2b, we see that the rapid shifts in fraud level found in the U-shaped distributions disappear for the most part. Instead, we see smaller (noisy) movements around an equilibrium level of fraudsters.

**Insert Figure 2 Here**

The possibility of two states of fraud dynamics observed in our benchmark model raises an additional question: Do efforts to prevent or detect fraud have differential effects on the two fraud dynamics observed? We now turn our attention to the impact of attempts to prevent or eliminate fraud in the organization.

**IV. PERCEIVED OPPORTUNITY**

We begin our investigation into the effectiveness of fraud prevention mechanisms by systematically manipulating perceived opportunity, which could be impacted by a variety of control activities. We reduce the likelihood of perceived opportunity over the entire parameter range, starting at 100 percent and reducing it in increments of 10 percent down to 0 for each level of emulation likelihood used in our benchmark analysis. All other parameters are held constant and are at the same level used in the benchmark analysis.

Recall that each agent vector has an identical perceived opportunity likelihood parameter — column $p(O)$ in the sample matrix presented in our example earlier — that represents the strength of internal controls within the organization. Because this parameter is a proxy for the overall strength of control in the organization, it is homogenous across all agents. While the likelihood is identical for all agents, each can differ in their perceptions of opportunity as the model evolves. For example, if the opportunity parameter is set at 0.90, opportunity will be present and independently and randomly determined for each agent 90 percent of the time.
While we investigate the entire emulation likelihood range (as in the benchmark model) for each opportunity likelihood parameter value considered (from 10 percent to 100 percent in increments of 10 percent), our analysis focuses on the two state outcomes (U shaped and inverted-U shape distributions) identified during the benchmark parameter sweeps. When we evaluate the effect of reducing opportunity in organizations with moderate and high emulation levels, the characteristic U shape of the distribution and related time series remain unchanged. Figures 3 and 4 below summarize the fraud dynamics for two U shaped organizations that are identical except for opportunity. Figure 3 illustrates outcomes when opportunity is set at 100 percent and Figure 4 illustrates outcomes when opportunity is set at 70 percent. In Figure 4, notice that the shape of the state distribution is similar to the shape exhibited in Figure 3 and that the organization continues to vacillate between extremes (from no fraud to around 70 percent of organization committing fraud). The majority of periods are still spent at the extremes and rapid swings between extremes continue to occur. This result is consistent across our parameter sweep for U shaped organizations. Decreasing opportunity lowers the upper support of the distribution but the U shape is retained, as are the rapid swings in behavior.

Insert Figure 3 Here

Insert Figure 4 Here

A similar result emerges when we consider the inverted-U distribution characteristic of low emulation likelihood organizations. The shape of the state distribution of fraud over time and related dynamics persist when control strength is increased (likelihood of perceived opportunity is decreased) but the average fraud level is reduced. Figures 5 and 6 provide a illustration. The organization represented in both Figures 5 and 6 is identical in all respects except for the level of opportunity (100 percent and 70 percent in Figures 5 and 6, respectively). In both organizations,
a stable equilibrium is evident and the lower perceived opportunity present in Figure 6 reduce that equilibrium level of fraud.

Insert Figure 5 Here

Insert Figure 6 Here

Thus, overall, we find that reducing perceived opportunity in the organization simply shifts the average fraud level closer to zero, but does not qualitatively affect the shape of the distribution of fraud over time or the nature of the fraud dynamics. The two emergent states observed in our benchmark model persist and the extreme swings between honesty and widespread fraud in moderate and high emulation likelihood organizations remain. The results of our analysis suggest that, while reducing perceived opportunity can limit the extent of fraud in an organization, culture and individual susceptibility to influence continue to exert an important influence on the nature of fraud dynamics.

V. TONE AT THE TOP

Tone at the top is often noted as an important characteristic in organizations for controlling fraud (Association of Certified Fraud Examiners, 2007). To better understand the impact of tone at the top on dynamics in our model, we begin by extending our benchmark analysis to create a hierarchical organization with two levels of employees: managers and staff. We assume that managers are more likely than staff to influence the rationalizations of others. When an agent observes a manager, the agent’s likelihood of emulating the manager’s rationalization toward fraud (or lack thereof) will be higher than if the manager were identified as staff instead. For purposes of analysis, we make no other modifications relative our benchmark model. Motive and opportunity remain constant, at 100 percent. We systematically vary the proportion of managers in the population (span of control) and investigate the impact of
this manipulation over the range of emulation likelihood values (as in the benchmark model). We compare the results of our benchmark model (no managers) to those of hierarchical models that include one, two, four, or six managers.

We introduce a hierarchy to the organizations by adding a status identifier to each agent vector in the benchmark model. Agents are randomly identified as managers in the organization prior to the first period of agent interaction. Agents identified as managers are assigned a hierarchical status identifier equal to 2 (resulting in twice the impact on emulation likelihood), while the remaining agents are considered staff and assigned a hierarchical status identifier equal to 1. We use this identifier to scale emulation likelihoods during agent interactions. For example, assume agent 1 is assigned an emulation likelihood of 0.15 when the organization is formed. In our benchmark model, when agent 1 observes another agent, the agent 1 will change her rationalization state to match the observed agent’s rationalization state with a 15 percent probability. However, in our hierarchical model the likelihood of emulating another agent is doubled, to 30 percent, when the agent observed is a manager.

Our analysis indicates that adding a hierarchy has no qualitative effect on observed outcomes relative to the benchmark model. Figure 7 illustrates the effect of going from zero to six managers in an identical population with a high average emulation likelihood. While there are small differences in state distributions, the amount of time spent by the organization in the two extremes is approximately equal across conditions and does not systematically vary as the number of managers is increased. The tendency toward extreme behavior persists. Likewise, no clear pattern emerges from an examination of the fraud time series in this set of simulations.

20 We tested the sensitivity of the emulation likelihood scalar introduced by interacting with a manager by increasing it from 2 to 4. No qualitative effect was observed on aggregate outcomes.
Figure 8 illustrates the effect of introducing a hierarchy in low emulation likelihood (inverted-U) organizations. As with U-shaped organizations, no consistent pattern emerges as managers are introduced into the population and their span of control is decreased.

We conclude from our analysis that the presence of a hierarchical organization does not, in itself, influence fraud dynamics or organizational tendencies toward fraud. However, the notion of tone at the top incorporates more than a hierarchical organization with influential management. It is usually characterized as a management team with a consistent message regarding ethical values and appropriate behavior. To capture this idea, we extend the hierarchical model by introducing a group of identical managers. Each is assigned an anti-fraud attitude in the initial period of the simulation. To ensure their attitudes do not change, the managers’ likelihood of emulating a worker (q) and likelihood of spontaneous attitude change (p) are both set to zero. Our investigation is identical to the analysis performed in the hierarchical case, above.

We find that a monolithic, honest management team in a U-shaped organization effectively changes the characteristic shape of aggregate fraud outcomes. Figure 9a illustrates the effect of going from zero to six managers in an identical population with a high average emulation likelihood. With even one honest manager, we see the tendency to remain for periods of time at maximum levels of fraud disappear (the upper tail in the U shape is gone). A clearer picture of the qualitative effect of the manipulation is provided by an examination of the dynamics of fraud over time. While there is an overall tendency towards honesty in organizations with a positive tone at the top, the time series in Figure 9b shows frequent but
short-lived outbreaks of fraud in the organization. This remains the case regardless of the number of managers that we examined (up to 6).

**Insert Figure 9 Here**

To complete our analysis of a monolithic, honest management team we consider its impact on the aggregate fraud outcomes and dynamics when average emulation levels are low (i.e., inverted-U shape organizations). We find that, while introducing a monolithic honest management team reduces average fraud levels, it has no effect on either the shape of the distribution (Figure 10a) or on the qualitative characteristics of the time series in Figure 10b. Furthermore, as shown in Figure 10, increasing the relative size of the management team does not qualitatively alter this general finding.

**Insert Figure 10 Here**
VI. CODE OF ETHICS

We assume that agents will be less likely to rationalize fraud in the presence of a well-implemented code of ethics. To investigate the effect that a code of ethics might have on fraud, we add a scalar \( c \) to our benchmark model. The scalar is constant across all agents because we assume that the code of ethics would be implemented across the entire organization. During agent interaction, the scalar changes the likelihood of emulating a fraud rationalization relative to non-rationalization in the following manner:

---

21 Research suggests that the impact of a corporate code of ethics on individual behavior is equivocal. In a field study investigating the effect of a corporate codes of ethics on employees and organizational climate, Adams, Tashchian and Shore (2001) found that employees in organizations with a code of ethics felt more supportiveness for ethical behavior, more freedom to act ethically, and more satisfaction with the outcome of ethical problems. This effect was observed even when respondents could not recall specific content in the code of ethics. In a second study examining management accountants, Somers (2001) found a decrease in perceived wrongdoing but no increase in the propensity to report observed unethical behavior in organizations that had adopted a code of ethics. We argue that the extent to which a code of ethics impacts individual behavior may depend on its implementation, which has been observed to vary greatly between organizations (Weaver, Treviño and Cochran 1999). Our operationalization of a code of ethics presumes that it has at least some impact on individual behavior. It might also be viewed to encompass more than a code of ethics (e.g., an ethics training and awareness program).
\[ Q = \frac{qc}{c + 1}, \text{ when the agent observes another agent rationalize and} \]
\[ Q = q \text{ otherwise,} \]

where \( Q \) is the emulation likelihood in the code of ethics model, \( q \) is the emulation likelihood in the benchmark model, and \( c \) is the code of ethics scalar. To illustrate the application of this rule set, assume agent A’s emulation likelihood \((q)\) is 0.50 and the code of ethics scalar \((c)\) is set to 9 in the organization. When agent A observes another agent rationalizing, agent A will have a 45 percent likelihood of beginning to rationalize as well. However, if agent A is rationalizing fraud and observes non-rationalization in another agent, he or she will stop rationalizing with a 50 percent likelihood. Thus, the smaller the value of the scalar, \( c \), the higher the likelihood than an agent will emulate an honest co-worker relative to a fraudster, and the more effective the code of ethics.

To evaluate this version of our model, we systematically vary the scalar \( c \) so that the likelihood of emulating rationalization relative to non-rationalization is first set at 99 percent and then at 95 percent down to 75 percent in 5-percent increments.\(^{22}\) Each of these scalar values is examined at every emulation likelihood level used in the benchmark model so that the effect of a code of ethics can be assessed across both the moderate to high emulation likelihood (U shaped) organizations and low emulation likelihood (inverted-U) organizations. We compare the results of these parameter sweeps to matched (identical) starting organizations examined in our benchmark model.

\(^{22}\) To achieve these likelihoods, the code of ethics scalar is set at 99 (for 99 percent relative weight), 19 (for 95 percent relative weight), 9 (for 90 percent relative weight), and down to 3 (for 75 percent relative weight).
For organizations with moderate to high average emulation likelihoods, the implementation of a code of ethics dramatically affects both the shape of the cumulative fraud distribution and the dynamics of fraud behavior over time. As the effectiveness of the code of ethics is increased (by decreasing the scalar $c$), the upper support of the U shape rapidly disappears. Similarly, the dramatic swings between extremities that characterize organizations with moderate to high average emulation likelihoods in our benchmark model disappear. As the code of ethics scalar decreases, a (Lyapunov) stable equilibrium approaching zero fraud emerges. This trend is illustrated in Figure 11.

**Insert Figure 11 Here**

A very different result emerges when we observe the impact on the inverted-U distribution found in organizations with low average emulation likelihoods. As seen in Figure 12, the shape of the state distribution and the related fraud dynamics in low emulation likelihood organizations persist as $c$ decreases. In all cases, we observe stable equilibria centered at a level between 30 and 50 percent. Thus, as the effectiveness of the code of ethics increases, the level of fraud decreases but does not approach the low levels (at or near zero) seen when we introduce a code of ethics in high and moderate emulation likelihood organizations.

**Insert Figure 12 Here**

Introducing asymmetric emulation likelihoods (consistent with a well-implemented code of ethics) dramatically reduces average fraud levels and stabilizes fraud dynamics in organizations with high average emulation likelihoods. However, in organizations with low average emulation likelihoods, the effect is modest at best. Relative to our earlier analysis examining the effect of a system of internal controls and tone at the top, a code of ethics is the first change in the model to affect the shape of the distribution of fraud states, but only under in
certain conditions. The results suggest that the role of a code of ethics in fraud prevention is contingent on the nature of the organization, a relation not previously recognized in the literature that could prove important in fraud risk assessment.

VII. ENFORCEMENT

Our investigation so far has focused on organizational interventions associated with fraud prevention. We now turn our attention to the effect of detecting and eliminating fraud in the organization via an active anti-fraud enforcement program. To model enforcement, we assume that fraudsters will be detected with some probability $t(e)$. Once detected, agents are removed from the organization (“fired”) and replaced with a new agent.

While we anticipate implementation of organizational enforcement policies company-wide, we expect the existence of budget constraints with regard to enforcement efforts. As a result, we assume fraud detection programs will be more successful in organizations with lower levels of fraud. For example, at higher fraud levels, we anticipate that collusion among employees will impede the enforcement process. Therefore, in each period, we determine the likelihood of detection and termination as

$$t(e) = e \left( \frac{N - f}{N} \right),$$

where $t(e)$ is the likelihood of detection and termination, $e$ is the likelihood of detection and termination unadjusted for the number of fraudsters in the population, $N$ is the number of agents.
in the organization \((N = 100)\), and \(f\) is the number of fraudsters in the population at the start of the simulation period.\(^{23}\)

In our enforcement model, when a fraudster is terminated and replaced, we assign new values for all agent attributes (using the process described in the benchmark model) with the exception of the agent identifier (\(ID\)), social network (\(SN\)), and social network size (\(S\)). These three attributes remain unchanged under the assumption that when an employee is replaced, the new employee will interact with the same individuals as the previous one.

In our analysis of the enforcement model, we set the unadjusted enforcement likelihood \(e\) at 1 percent and then increase it from 5 to 20 percent in increments of 5 percent. We run these simulations over the entire range of emulation likelihood values examined in the benchmark model to investigate the impact of enforcement on our two classes of organizations (U shaped and inverted-U shaped). We compare the results of these parameter sweeps to the matching populations in our benchmark analysis.

When we consider organizations with moderate to high average emulation levels (U-shaped organizations), we find that the introduction of an enforcement regime transforms the U-shape distribution found in our benchmark model into a distribution characterized by extremely low fraud levels. In Figure 13a one can see that the cumulative distribution of fraud over time qualitatively resembles the impact of code of ethics discussed earlier in our analysis (see Figure 11a). However, a comparison of the time series of fraud in Figure 13b with the matching time series in Figure 11b (where a code of ethics was introduced) highlights an important difference in...\(^{23}\) Presumably, introduction of an enforcement regime might also decrease the agents’ perceived opportunity to commit fraud. However, for purposes of our analysis, we investigate both effects independently to gain a better understanding of their individual effects.
the resulting fraud dynamics: At high enforcement levels ($e$ equal 0.20), while average levels of fraud decrease to very low levels, we continue to see occasional outbreaks of fraud involving up to 80 percent of the agents in the organization. Similar outbreaks are not evident in organizations with a code of ethics.

**Insert Figure 13 Here**

When we consider organizations with low emulation likelihoods, we find the first instance of an intervention triggering a dramatic change in the shape of the inverted-U distribution. Enforcement systematically reduces the level of fraud to near zero levels, where it remains. Considering the fraud dynamics, we find stability and do not see evidence of widespread fraud outbreaks. This is illustrated in Figure 14.

**Insert Figure 14 Here**

Our analysis suggests that enforcement efforts can be effective at reducing average fraud levels to near zero in both types of organizations (U and inverted-U shaped). However, the effectiveness of enforcement regimes at preventing widespread fraud outbreaks appears contingent on the type of organization and related individual susceptibilities to fraud.

**VIII. DISCUSSION AND CONCLUSIONS**

We used an ABM to investigate the dynamics of fraud within organizations and the impact of fraud prevention and detection mechanisms. Our model consisted of an organization, agents (employees), and a set of simple social interaction rules. In accordance with Cressey’s (1953) occupational fraud model, any agent within our model encountering the union of motive, opportunity, and a pro-fraud rationalization (creation of an attitude or belief) committed fraud. We evolved the organization by allowing agents to interact, resulting in changes in agent attitudes toward fraud (via cultural transmission). We found that two types of organizations
emerged, dependent upon how susceptible individual agents were to social influence. When susceptibility to influence was low, a distribution emerged where aggregate fraud levels tend to a (Lyapunov) stable equilibrium. When susceptibility was moderate to high, we observed a outcome characterized by unpredictable, extreme swings in behavior from an overall honest population to an overall fraudulent one.

After identifying these two types of organizations, we turned our attention to the impact of mechanisms to prevent, detect, and eliminate fraud. Mechanisms considered included overall strength of internal controls, tone at the top, a code of ethics, and enforcement (fraud detection and termination). We found the effectiveness of a mechanism to prevent or detect fraud to be contingent on the type of organization and individual social influence susceptibilities. The findings are summarized in Table 1, below.

**Insert Table 1 Here**

The model suggested that a code of ethics is particularly effective at preventing fraud for moderate to high average emulation likelihoods. However, a code of ethics was observed to be much less effective in organizations with low emulation likelihoods. A different result emerged when we considered the impact of an enforcement regime. The introduction of enforcement reduced fraud to near zero levels in both types of organizations. However, its effectiveness at preventing occasional outbreaks of widespread fraud was contingent on the type of organization and individual susceptibilities to social influence. General internal controls merely reduced the average aggregate level of fraud within an organization. In our model, they did not affect the nature of fraud dynamics, regardless of emulation likelihood levels. The presence of a hierarchical organization did not directly affect the nature of fraud dynamics, but introduction of a monolithic honest management team effectively reduced the amount of fraud in both types of
organizations. Furthermore, while it eliminated the tendency to remain at high levels of fraud for periods of time in U-shaped organizations, it did not eliminate sporadic, short-lived fraud outbreaks.

Our findings have important implications for auditors and other individuals responsible for assessing fraud risk and detecting and preventing fraud. First, for certain types of organizations aggregate fraud levels can vary tremendously over time. Furthermore, the effectiveness of mechanisms to prevent and detect fraud can be contingent on the type of organization and individual susceptibilities to social influence. Therefore, it may be inappropriate for auditors to evaluate fraud prevention and detection mechanisms in a uniform manner. Our results suggest that the same fraud prevention and detection mechanisms implemented in a similar manner in two different organizations cannot be expected to be equally effective without considering the average susceptibilities to social influence of the individuals therein. Similarly, some mechanisms (e.g., enforcement regimes) can appear very effective the majority of the time but in actuality are sometimes ineffective at preventing occasional outbreaks of widespread fraud. In general, there is no one-size-fits-all fraud prevention (and/or detection) mechanism and fraud risk may be contingent on individual susceptibilities to social influence.

While the ABM method used in our investigation confers a number of advantages over traditional models in the social sciences, it presents several limitations as well. First, seemingly innocuous assumptions have sometimes been shown to have unexpected outcomes that are not yet fully understood because the method is still young (e.g., see Huberman and Glance 1993). In the context of our model, additional research might examine alternative updating rules for modeling the evolution of the organization (for example, one alternative model might randomly select agents and then randomly determine for that agent whether they will interact with another
agent or make a decision about committing fraud) or alternative characterizations of social norm formation. Second, the solution concepts employed in ABMs tend to be relatively weak and, to date (again because of the novelty of the method), there has been little formal work on the replicability of results using different models (Axtell et al. 1996). Finally, ABM still lacks a set of standard, generally accepted practices, which makes replication difficult.

Our initial investigation of fraud leads to a variety of other opportunities for future research. In our analysis, we examine interventions in isolation. Our design choice was driven by a desire to develop a deeper understanding of the effects of each mechanism for controlling fraud. However, in organizations, these mechanisms are seldom implemented alone. Future research might extend our work by investigating the relative efficacy of combining different interventions. In addition, a more detailed examination of each leg of the fraud triangle could be undertaken. For example, future research might refine our characterization of motivation by explicitly considering social psychological factors in the organization. Equity theory (Adams 1965) would suggest that an honest individual in an organization replete with fraudsters would be more likely to have a motivation to commit fraud in order to re-establish fairness in their relationships with co-workers and the organization. Our model could be modified to incorporate this effect by making motivation a function of the number of fraudsters in the agent’s social network. Similarly, the representation of enforcement in our model (detection and removal of fraudsters) ignores the deterrent effect that can be generated by an active enforcement program. Future research could extend our characterization to incorporate deterrence effects, which would likely affect perceived opportunity.
REFERENCES


### TABLE 1
Summary of Findings

<table>
<thead>
<tr>
<th>Control Mechanism</th>
<th>Effect on U-Shaped Organization</th>
<th>Effect on Inverted U-Shaped Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Controls</td>
<td>• Upper support lowered</td>
<td>• Average fraud level reduced</td>
</tr>
<tr>
<td></td>
<td>• Dynamics preserved</td>
<td>• Dynamics preserved</td>
</tr>
<tr>
<td>Hierarchy</td>
<td>• No effect</td>
<td>• No effect</td>
</tr>
<tr>
<td>Tone at the Top</td>
<td>• Upper support removed</td>
<td>• Average fraud level reduced</td>
</tr>
<tr>
<td></td>
<td>• Spontaneous outbreaks persist</td>
<td>• Dynamics preserved</td>
</tr>
<tr>
<td>Code of Ethics</td>
<td><strong>Highly effective</strong></td>
<td>• Average fraud level reduced</td>
</tr>
<tr>
<td></td>
<td>• Upper support removed</td>
<td>• Dynamics preserved</td>
</tr>
<tr>
<td></td>
<td>• Stops spontaneous outbreaks</td>
<td></td>
</tr>
<tr>
<td>Enforcement</td>
<td>• Upper support removed</td>
<td><strong>Highly effective</strong></td>
</tr>
<tr>
<td></td>
<td>• Spontaneous outbreaks persist</td>
<td>• Fraud reduced to near zero</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stops spontaneous outbreaks</td>
</tr>
</tbody>
</table>
FIGURE 1
State Distribution for a U-Shape Organization with a Mean Emulation Likelihood of 60 percent and Maximum Motive and Maximum Perceived Opportunity

Panel A: Aggregate Fraud Frequency Histogram

Panel B: Time Series
FIGURE 2
State Distribution and Dynamics for an Inverted U-Shape Organization with a Mean Emulation Likelihood of 5 percent, Maximum Motive and Maximum Opportunity

Panel A: Aggregate Fraud Frequency Histogram

Panel B: Time Series
FIGURE 3
State Distribution and Dynamics for a U-Shape Organization with a Mean Emulation Likelihood of 95 percent and a Perceived Opportunity Likelihood of 100 percent

Panel A: Aggregate Fraud Frequency Histogram

Panel B: Time Series
FIGURE 4
State Distribution and Dynamics for a U-Shape Organization with a Mean Emulation Likelihood of 95 percent and a Perceived Opportunity Likelihood of 70 percent

Panel A: Aggregate Fraud Frequency Histogram

Panel B: Time Series
FIGURE 5
State Distribution and Dynamics for an Inverted U-Shape Organization with a Mean Emulation Likelihood of 5 percent and a Perceived Opportunity Likelihood of 100 percent

Panel A: Aggregate Fraud Frequency Histogram

Panel B: Time Series
FIGURE 6
State Distribution and Dynamics for an Inverted U-Shape Organization with a Mean Emulation Likelihood of 5 percent and a Perceived Opportunity Likelihood of 70 percent

Panel A: Aggregate Fraud Frequency Histogram

Panel B: Time Series
FIGURE 7
State Distribution for a U-Shape Organization with a Mean Emulation Likelihood of 95 percent across Hierarchies Ranging from 0 Managers to 6 Managers
FIGURE 8
State Distribution for an Inverted U-Shape Organization with a Mean Emulation Likelihood of 5 percent across Hierarchies Ranging from 0 Managers to 6 Managers
FIGURE 9
State Distribution and Dynamics for an U-Shape Organization with a Monolithic Honest Management Team

Panel A: Aggregate Fraud Frequency Histograms for an Organization with a Mean Emulation Likelihood of 95 percent across Hierarchies Ranging from 0 Managers to 6 Managers

Panel B: Time Series for an Organization with a Mean Emulation Likelihood of 95 percent across Hierarchies Ranging from 0 Managers to 6 Managers
FIGURE 10
State Distribution and Dynamics for an Inverted U-Shape Organization with a Monolithic Honest Management Team

Panel A: Aggregate Fraud Frequency Histograms for an Organization with a Mean Emulation Likelihood of 10 percent across Hierarchies Ranging from 0 Managers to 6 Managers

Panel B: Time Series for an Organization with a Mean Emulation Likelihood of 10 percent across Hierarchies Ranging from 0 Managers to 6 Managers
FIGURE 11
State Distribution and Dynamics for a U-Shape Organization with a Mean Emulation Likelihood of 95 percent across Code of Ethics Relative Emulation Likelihoods

Panel A: Aggregate Fraud Frequency Histograms across Code of Ethics Relative Emulation Likelihoods Ranging from 100 percent down to 80 percent

Panel B: Time Series across Code of Ethics Relative Emulation Likelihoods Ranging from 100 percent down to 80 percent
FIGURE 12
State Distribution and Dynamics for an Inverted U-Shape Organization with a Mean Emulation Likelihood of 5 percent across Code of Ethics Relative Emulation Likelihoods

Panel A: Aggregate Fraud Frequency Histograms across Code of Ethics Relative Emulation Likelihoods Ranging from 100 percent down to 80 percent

Panel B: Time Series across Code of Ethics Relative Emulation Likelihoods Ranging from 100 percent down to 80 percent
FIGURE 13
State Distribution and Dynamics for a U-Shape Organization with a Mean Emulation Likelihood of 90 percent across Enforcement Likelihoods

Panel A: Aggregate Fraud Frequency Histograms across Enforcement Likelihoods Ranging from 0 percent to 20 percent

Panel B: Time Series across Enforcement Likelihoods Ranging from 0 percent to 20 percent
FIGURE 14
State Distribution and Dynamics for a Inverted U-Shape Organization with a Mean Emulation Likelihood of 10 percent across Enforcement Likelihoods

Panel A: Aggregate Fraud Frequency Histograms across Enforcement Likelihoods Ranging from 0 percent to 20 percent

Panel B: Time Series across Enforcement Likelihoods Ranging from 0 percent to 20 percent