AN EMPIRICAL STUDY OF A TWO-SIDED MODEL OF FRAUDULENT EXCHANGE

Research-in-Progress

Andrew Harrison
Iowa State University
Gerdin Business Building
Ames, IA 50010
ajharris@iastate.edu

Brian Mennecke
Iowa State University
Gerdin Business Building
Ames, IA 50010
mennecke@iastate.edu

William Dilla
Iowa State University
Gerdin Business Building
Ames, IA 50010
wdilla@iastate.edu

Abstract

Interpersonal fraud is a complex social action constituted by a series of dependent events and an accurate representation of this interaction requires the examination of both the victim and perpetrator in fraudulent exchanges. IS domain research on e-commerce provides behavioral models that can be used to describe a victim's perspective on fraud in online commerce. Similarly, research in the accounting domain has developed the fraud triangle, a behavioral model that describes a perpetrator's perspective in committing fraud. There is limited research exploring how the use of technology affects fraudulent behaviors despite a growing interest in studying computer mediated deception. We draw on research from the IS and accounting domains about the fraud triangle, e-commerce, and computer-mediated deception to develop a two-sided model that combines victim and perpetrator behaviors. The proposed model more accurately depicts the complex nature of the social exchanges between fraud victims and perpetrators that result in fraud.

Keywords: Fraud, fraud triangle, deception, e-commerce, TAM, TPB
Introduction

Fraud has been a focus of research in both information systems (IS) and accounting for several decades; yet, these two domains have been approaching the problem from opposing sides of the exchange. IS researchers tend to focus on the ability of the victim to detect fraud (Xiao and Benbasat 2011) and how a willingness to engage in an online exchange is affected by perceptions of risk and trust (Gefen et al. 2003; Pavlou 2003). In contrast, accounting researchers tend to focus on improving fraud detection and prevention mechanisms by exploring how the perpetrator’s characteristics or environmental conditions contribute to fraud (Grazioli et al. 2006). This paper synthesizes these two perspectives by considering fraud as an economic and social exchange and draws upon insights from research in computer-mediated deception. Consequently, we may derive important insights about variations of behavioral models, such as the theory of planned behavior (TPB) and the technology acceptance model (TAM). These insights expand the IS perspective on fraud while simultaneously supporting the development of behavioral models that expand the accounting perspective.

This manuscript discusses the theoretical implications for a fraud model that expands on previous research by describing the interdependent behaviors of both the perpetrator and the victim of fraud. This two-sided approach represents a significant contribution to the domains of IS and accounting. First, this model has functional implications for how individuals can reduce their risk of becoming victims in fraudulent exchanges by focusing on improving their technical, economic, and governance capabilities and evaluating those characteristics that make their exchanges prone to misrepresentation. Secondly, the proposed model is useful in evaluating how the characteristics of an IT artifact can influence the ability of one person to defraud another. Below we review the literature on fraud, present our proposed model, describe the relationship between this model and prior literature from both the accounting and IS domains, and describe proposed methodology for empirically testing the model.

Theoretical Foundation

Technology Acceptance Model and E-Commerce

In the context of IS adoption, TAM has become a dominant theoretical perspective because it parsimoniously explains the relationship between expected efforts required and the expected benefits of adopting a new technology. Though originally focused on describing the adoption of desktop computers within an organization to improve job performance, TAM is considered a strong theory in many areas of technology adoption and has been adapted to a wide range of other technology adoption behaviors (Lee et al. 2003). TAM is derivative of TRA and TPB and each shares the core proposition that behavior is rationally formulated prior to action (Ajzen 1991; Davis 1986; Fishbein and Ajzen 1975). Models within this lineage have been applied to examine the use of electronic exchange systems and extended to examine the perception of risk and trust involved in the adoption of online commerce (Featherman et al. 2006; Gefen et al. 2003; George 2004; Jarvenpaa and Todd 1996; Lee 2009; McKnight et al. 2002; Pavlou 2003; Suh and Han 2003). Potential consumers in online transactions weigh convenience and expected outcomes against the risks of the transactions to determine if they should proceed with the exchanges (Bhatnagar et al. 2000) and research shows that people will have a greater intention to use a website if it is perceived to be easy to use (Davis 1986; Karahanna et al. 1999).

In TAM, the concept of perceived usefulness describes the notion that people tend to use or not use an application if they believe it will help them perform their job better. In the context of technology acceptance, the motivation to acquire technology is assumed to be associated with an improvement in personal performance. Victims typically engage in fraudulent transactions because they mistakenly perceive some type of financial gain. Consequently, the perceived usefulness of engaging in an online transaction is often gauged by the victim in terms of the financial, utilitarian, or hedonic value they would derive from the exchange. People may have varying assessments of what type of value they will derive from their participation in a transaction, and may consequently be more or less willing to engage in a potentially risky transaction. Reliance on ineffective fraud detection and prevention systems may also lower a victim’s risk assessment, thereby encouraging participation in risky exchanges. Fraud is more
likely when risk evaluation is faulty or incorrectly specified and may result in an incomplete decision-making process and a misinformed decision to participate in the fraudulent transaction.

Trust has been shown to play a critical role in e-commerce transactions by enabling one to overcome perceptions of risk and uncertainty associated with participating in a transaction (Gefen et al. 2003; McKnight et al. 2002; Pavlou 2003). Trust is a complex and multifaceted construct that can be interpreted in the context of e-commerce as the belief that allows consumers to become vulnerable after having considered the vendor’s characteristics (McKnight et al. 2002; Pavlou 2003). Trust has been incorporated into the structure of behavioral models describing e-commerce in a variety of ways (Gefen et al. 2003; Lee 2009; Pavlou 2003; Rofiq and Mula 2010; Shin 2008; Suh and Han 2003). For the purpose of this paper’s exploration of fraudulent exchanges, trust consists of assessments of competencies, benevolence, and integrity, which are dimensions that are evaluated separately by partners in the exchange (McKnight et al. 2002). This perspective builds on a trust-based model of e-commerce developed by Gefen, Karahanna, and Straub (Figure 1). In e-commerce, consumers often must trust that the other transacting party is acting in an ethical and socially responsible manner. Trust in the competence, benevolence, and integrity of others participating in the transaction are built on previous web experience and institution-based assessments of situational normality, structural assurances associated with the transaction space, and the general disposition of an individual to trust others (McKnight et al. 2002). Research demonstrates that the more trusting a consumer is during a specific transaction, the more likely he is to participate in that transaction (Gefen et al. 2003, Pavlou 2003; Pavlou and Gefen 2004). This belief can be exploited by fraudsters to manipulate the transaction for their own benefit, and fraud often occurs even when victims have high levels of trust in their exchange partner (Albrecht et al. 2009). Trust is important in exchanges because it is instrumental in the formulation of expectations of future actions of other actors (Blau 1964; Gefen et al. 2003; Kellerman 1984).

![Figure 1. Model of E-Commerce Behavior (adapted from Gefen et al. 2003)](image)

### Theory of Planned Behavior and Fraud

Fraud is a representation about a material point that is intentionally or recklessly false, where the misrepresentation is believed and acted upon by the victim to the victim’s detriment (Albrecht et al. 2009; Firozabadi et al. 1999). Fraud occurs when one individual defrauds another individual in an exchange, and these fraudulent exchanges are often mediated by web-based systems. Fraud is a special case of deception that is particularly germane in the domain of information systems because it is transactional by definition and is the result of the manipulation of information or information systems (Johnson et al. 2003). The manipulation of the content or presentation of information creates asymmetrical information for participants in a fraudulent exchange, giving the perpetrator an advantage (Albrecht et al. 2007; Xiao and Benbasat 2011). Fraud, by definition, requires the victim to incur a loss, which is typically financial. In this paper, a special subset of fraud, which is the material misrepresentation of assets, is the most salient and is explored in the scenario where a single person misrepresents the condition of assets on an auction site. Other types of fraud, most notably corporate fraud, are outside the scope of this paper.
The theory of planned behavior (TPB) is a general theory for describing how attitudes and beliefs precede actions (Fishbein and Ajzen 1975; Ajzen 1991) and has been applied to previous research into the behavioral antecedents of fraud. While TAM-like models represent a dominant perspective for examining the attitudes, beliefs, and behaviors of people about to engage in online transactions, TPB has proved useful in examining corporate fraud (Carpenter and Reimers 2005; Cohen et al. 2010) and the ethical decision making processes of public accountants (Buchan 2005). Accounting research on fraud has typically focused on detecting the means by which corporate stakeholders are able to defraud investors or the organizations in which they are employed (Hogan et al. 2008). The behavioral models developed for examining perpetrator characteristics in corporate fraud have also been extended to examine consumer fraud, which targets individuals instead of organizations (Albrecht et al. 2009).

The principal model in accounting for examining fraud is the fraud triangle (Albrecht et al. 1982; Cressey 1953; Sutherland 1949, 1983). The focus in accounting research, whether in the corporate or peer-to-peer context, has primarily been centered on the factors that motivate individuals to commit fraudulent actions. While the literature about corporate fraud suggests that the factors represented in the fraud triangle parallel the factors represented in TPB, no behavioral model has yet been suggested or widely applied to fraud research or interpersonal fraud (Carpenter and Reimers 2005; Cohen et al. 2010; Grazioli and Jarvenpaa 2000; Rofiq and Mula 2010). Consequently, we seek to utilize frameworks created for integrating the fraud triangle with TPB to develop a model describing the behavioral processes of potential perpetrators of computer mediated interpersonal fraud. The fraud triangle identifies and defines three perpetrator-related factors that are necessary antecedents for fraud to occur. A perpetrator is motivated to act because of financial or social pressures, perceives that opportunities exist where trust can be exploited for personal gain, and is able to rationalize the violation of another’s trust to commit the fraud. The fraud diamond is an extension of the fraud triangle and adds the capability of the perpetrator to commit fraud (Rittenberg et al. 2010; Wolfe and Hermanson 2004). Financial (e.g., greed or financial stress) and social pressures (e.g., the desire to manipulate or demonstrate achievement, power, or dominance) can motivate people to behave in an opportunistic fashion, which may lead to fraudulent behaviors (Albrecht et al. 2009; Cohen et al. 2010; Dilla et al. 2011). In addition, a potential perpetrator must recognize an opportunity where he could gain an advantage through deception. This opportunity may arise as perpetrators recognize weaknesses in control procedures or the structure of transactions or realize that the complexity of a system or transaction precludes observers from detecting the fraud (Cohen et al. 2010). External factors, such as faulty regulatory policies or anonymity, may also present opportunities for fraud (Zahra et al. 2005), making e-commerce a particularly accommodating environment for fraudulent behaviors. The rationalization component of the fraud triangle involves a person reconciling his behavior with accepted social norms prior to engaging in fraud (Albrecht et al. 2009; Rittenberg et al. 2010). This justification is often based on the notion that the fraudulent act will be a one-time occurrence necessary to resolve a crisis, on strong social tendencies embracing financial success, or on the perception that the act is necessary for the achievement of a worthy outcome (Choo and Tan 2007; Cohen et al. 2010). Finally, a perpetrator must be capable of committing deception and reaping a reward (Wolfe and Hermanson 2004), which may be derived from a unique or privileged understanding of technical, governance, financial, or economic characteristics of the situation. Personal charisma and communication skills are also considered to be capabilities that facilitate fraud.

Computer Mediated Deception

A model with multiple actors is supported by research about computer-mediated deception, which is largely based on previous models of dyadic communication and acknowledges the complex social exchanges that occur in deception. Nevertheless, Interpersonal Deception Theory (IDT) has also been shown to describe communication in groups as well as individuals (Marret 2004). The main contribution of IDT is the recognition of the complex and strategic manipulations by multiple parties in an exchange (Buller and Burgoon 1996). In IDT, each participant in an exchange pursues their own agendas with deceivers intentionally influencing the outcome of the exchange by manipulating the information they choose to share and the method by which it is shared. Any inconsistencies in information that are unintentionally leaked into the conversation by the sender are evaluated by receivers who make judgments about the veracity of the message (Ekman 1992; Ekman and Friesen 1969).

In addition to articulated communication, senders also exhibit latent cues of deceptive behavior (Buller
These non-verbal cues are often a more accurate and consistent method to determine when deception is occurring (DePaulo et al. 2003; Marret 2004; Rao and Lim 2000). Given a choice, deceivers will attempt to choose a medium that they perceive will mask or obscure leaked cues (George and Carlson 1999). Fraud, as a specific type of deceptive behavior that typically involves deception as a means to manipulate a financial transaction, is subsumed within other types of deceptive behavior. As a result, it is useful to analyze how research about computer mediated deception and IDT are related to the study of e-commerce behaviors and fraud. IDT and research on computer mediated deception would both suggest that technology facilitates an opportunity for deceivers to mask cues of their deception while simultaneously allowing prospective victims the ability to evaluate communication for any cues to others’ deceptive intentions. Although the names of individual constructs may vary, there is a strong convergence in all of these domains suggesting they represent a shared core associated with human rationality, motivation, and norms. We draw on these research domains to form a combined and integrated model of technology mediated interpersonal fraud.

**Fraud Model Development**

The key contribution of the fraud model proposed in Figure 2 is the unification of perpetrator and victim behaviors in the context of fraudulent transactions. The goal of this integrative model is to utilize the strength of the existing fraud triangle framework in conjunction with the behavioral e-commerce models to describe online fraud as a social exchange process that includes both a perpetrator and victim. Previous models have integrated fraud concepts including deception, risk, and trust that lead to a willingness of a potential victim to engage in an exchange despite the risk of fraud (Grazioli and Jarvenpaa 2000; Pavlou 2003; Rofiq and Mula 2010). Other models have explored the factors that can lead to the perpetration of fraudulent actions (Buchan 2005; Carpenter and Reimers 2005; Chang 1998; Cohen et al. 2010). Because fraud is subsumed in deception, we have also applied models from deception and communication research that investigate two-sided deceptive exchanges (Albrecht et al. 2007; Carlson et al. 2004). In this perspective, the deceiver must formulate their deception in such a way that they anticipate the motivations of the person who they are attempting to deceive (Johnson et al. 1993) and simultaneously obscure from the victim the true nature of the risk involved in the transaction. The proposed two-sided model makes an important contribution by expanding on robust behavioral models and representing fraud as a social exchange.
Variations of the TPB have already been used in multi-stage analyses of technology adoption (Johnstone and Bedard 2003; Szajna 1996) and e-commerce (George 2004; Pavlou and Fygenson 2006). We consider fraud to be analogous to these other transactions, albeit with different goals, attitudes, evaluations, and decision criteria for the participants in the transaction. In such exchanges, parties engage in a series of interactions by which they come to an agreement about the terms of the transaction. Throughout these exchanges, both parties constantly reevaluate the evolving agreement in accordance with any newly acquired information. During fraudulent exchanges, a perpetrator manipulates the terms of the agreement through misrepresentation and achieves an unfair advantage from asymmetrical information. Simultaneously, potential victims utilize detection tactics to varying degrees of success in an effort to detect deception and assess cues of misrepresentation (Grazioli et al. 2006). The proposed model represents a parsimonious representation of these complex behaviors and provides a foundation for interpersonal fraud research. The advantage of the model is that it identifies and defines the role of behavioral intentions and actions of both the perpetrator and victim of fraud in the context of social exchange theory, accounting research, and technology adoption research. Our model customizes TPB to the context of fraud while applying some of the lessons learned from the widespread use of TAM. In a departure from TPB, a key contribution of TAM is that it separates subjective perceptions of ease of use from perceived usefulness allowing one to compare how these different attitudes have idiosyncratic effects on usage (Davis 1989). This distinction is relevant because these attitudes are reflected in the fraud triangle’s exploration of individuals’ perceptions of motivation, opportunity, and rationalization. By grounding our model of fraud on a behavioral accounting perspective, the core of our model is intrinsically specific and relevant to the domain of fraud.

Technology

It is central to our research to understand how technology affects interpersonal fraud. Communication mode controls which deception cues are leaked to potential victims, and cues based on response time and other physical responses may be obscured by some forms of media (DePaulo et al. 2003). E-commerce is usually regarded as providing less interactive feedback between parties and less personal interaction (Buller and Burgoon 1996). Interactive deception is more taxing on deceivers and more leakage is likely to occur (Buller and Burgoon 1996; Eckman 1992; Ekman and Friesen 1969), making communication media with less feedback preferred by fraudsters because they believe these media increase their ability to commit fraud (Carlson et al. 2004). Consequently, we believe that the characteristics of the mediating exchange technology will influence the potential fraudster perceptions of opportunity.

Potential victims are also influenced by the characteristics of the exchange technology. Perceptions of competence and integrity are key aspects of an individual’s evaluation of a potential web vendor in an online transaction (Pavlou and Fygenson 2006; Suh and Han 2003). Nevertheless, potential victims will not show equal concern for all aspects of their personal security. For example, the perceived trustworthiness of the transaction is often of greater influence than concerns about personal information privacy (George 2004). In an online transaction both trust in the computer system and in the other social actor are relevant. Trust can involve assessments of the dependability of the system as well as the believability of the information presented (Fogg and Tseng 1999). Consumers also exhibit a “truth bias,” which suggests that social actors default to the expectation that others will be decent, pleasant, and worthy of positive regard (Buller and Burgoon 1996; Kellerman 1984). As a result, we propose that characteristics of technology play a role in a potential victim’s rationale for engaging in a transaction but they are mediated by the perceptions of benefits and costs associated with engaging in the transaction.

Motivation

Motivations for fraud vary, but the most common motivation is based on perceived financial benefits (Cohen et al. 2010). For fraud to occur the perpetrator must perceive a benefit to utilizing misrepresentation in an exchange; however, behavioral motivation is based on a subjective perception that does not inevitably reflect objective reality (Davis 1989). Fraud is often committed to acquire financial resources used to maintain expectations of status and achievement when more conscientious means to reach those goals have been exhausted. Pressures to commit fraud are primarily self-prescribed.
and often based on greed or a predisposition to wealth-based achievement (Choo and Tan 2007).

The cost-benefit paradigm that underlies behavioral theories like TPB asserts that people will weigh the trade-off between effort and the quality of the resulting decision. This trade-off is particularly significant in the development of a behavioral model of fraud, because the motivations of perpetrators are typically based on financial desire or personal achievement (Beach and Mitchell 1978). In TAM, the concept of perceived usefulness replaced affect from TPB, because the notion of affect does not represent the driving force in the decision process to reach means-oriented goals (Davis 1989). Perceived usefulness describes the notion that people tend to use or not use an application if they believe it will help them perform their job better. In the context of technology acceptance, the motivation to acquire technology is assumed to be associated with an improvement in personal performance; however, the perpetrator’s motivations are typically financial or power-based when engaging in fraud (Albrecht et al. 2007; Dilla et al. 2011).

**Opportunity**

For fraud to occur, both the perpetrator and victim must perceive an opportunity to engage in an exchange and the perpetrator must perceive an additional opportunity to act dishonestly. Perceptions about the nature of an opportunity to engage in a fraudulent exchange are subjective in nature. In fraud, opportunity represents the recognition by the perpetrator that the victim’s trust may be exploited. Opportunity reflects the notion of the perception of effort involved in completing the exchange, with honest intentions by the victim and dishonest intentions by the perpetrator. To create a greater opportunity to defraud another individual a perpetrator may portray some type of expert knowledge or capability (Albrecht et al. 1982), and these beliefs often result from misrepresentation. For example, many frauds are predicated on the false belief by the victim that their financial investment will result in supernormal profits due to the perpetrator’s expert financial prowess. Opportunities can also arise due to the characteristics of the technology being used to facilitate the exchange. The asymmetrical nature of technical and financial knowledge of parties in the exchange can present one party the opportunity to manipulate the other party. Opportunities are primarily derived from the perceptions of ease with which a person can perform a behavior under certain environmental factors and the capabilities of participants in the exchange, and are very closely conceptually aligned with perceived behavioral control as proposed by Ajzen. Ineffective regulatory statutes, inconsistent financial reporting standards, identity obfuscation, and poorly designed information systems can create opportunities for clever potential perpetrators. These opportunities are closely tied to, and often dependent upon, the abilities of the perpetrator to commit fraud and are inversely related to the victim’s ability to detect fraud.

**Capability**

A perpetrator’s capabilities vary by context; for example, technical skills may be relevant to e-commerce fraud while financial skills will be relevant to investment fraud. Capabilities embody the perpetrator’s perception of their capacity to commit fraud in a specific context (Wolfe and Hermanson 2004), and represent a similar but different component of perceived behavioral control. In TPB, perceived behavioral control is also a reflection of past experiences (Ajzen 1991). As a result, the convergent theory stemming from accounting and criminology also recognizes these two important behavioral concepts, though they are regarded as distinct from one another. When a perpetrator’s capabilities align well with the requirements needed to commit fraud, the less effort it will take for that person to engage in the act. Conversely, the more capable a person is of detecting fraud, the greater the effort that will be needed by the perpetrator to consummate the fraud transaction. The likelihood of fraud occurring is positively related to perpetrator fraud-relevant capabilities. Relevant expertise also increases the probability of success and decreases the perceived effort required for success (Beach and Mitchell 1978).

It is also critical to examine the alignment of opportunity and capability to commit fraud in designing fraud prevention and detection systems (Wolfe and Hermanson 2004). The capabilities to commit fraud can be rooted in various forms of power (Albrecht et al. 1982), though expertise and positional power are the most often used. Technical competency with the information system that facilitates the exchange allows perpetrators to exploit weaknesses in the exchange. Knowledge of economic exchanges and governance structures is useful in the context of investment fraud. Similarly, perpetrators of fraud are often familiar with auditing procedures (Ramos 2003). The ability to communicate and subtly manipulate
the exchange is also useful. Generally, in fraudulent exchanges a combination of these types of skills is used by perpetrators, or a paucity of these skills is exhibited by victims (Albrecht et al. 1982).

**Rationalization**

The rationalization for fraudulent action generally takes the form of a dismissal of rules or a disdain for others. For fraud to occur, the perpetrator must be able to rationalize their intentions prior to action. Frequently, perpetrators feel compelled to commit fraud because they rationalize that they are deserving of the benefits their actions are intended to accrue. Perpetrators often believe that the typical social norms regarding the use of deceit to obtain gain do not apply to them and are able to reconcile their intentions with their personal code of ethics because their moral propensity allows them to act dishonestly in certain contexts (Ramos 2003). Environments where mores suggest that financial success is justified at all costs are also likely to encourage fraud (Choo and Tan 2007).

Behavioral intention in TPB represents the strength of one’s intention to perform a behavior while attitude represents the degree to which one favors or disfavors a behavior (Fishbein and Ajzen 1975). Nevertheless, fraud is a unique context where perpetrators often outwardly display unfavorable opinions of the actions they are committing. It is common for fraudsters to state that they had never intended to defraud others and that they had fully planned to repay (Albrecht et al. 1982). Consequently, we believe that in the context of fraud a perpetrator’s ability to rationalize a fraudulent act is more akin to their true behavioral intention without their expression of intent being subverted by strong social influences and self-delusion. We contend that the degree to which a perpetrator can rationalize fraudulent actions is directly tied to his intention to commit fraud.

**Research Design**

To test the proposed model of interpersonal fraud, a structural equation modeling (SEM) approach is proposed to analyze data collected from a laboratory experiment. SEM was selected for two primary reasons: (1) SEM combines path analysis models with covariance-based factor analysis models, and in the proposed model the measurement of latent constructs and the relationships between them are both critically important, and (2) the extant research that this work builds upon recommends SEM as an appropriate research method (Gefen et al. 2003). A SEM model is well-suited to empirically study how attitudes and intentions are statistically related to behaviors. Fraud is typically studied in a reactive manner in which case studies of fraudulent actions are described after the behaviors have occurred. Legal and social ramifications, as well as a reduced likelihood that the fraudulent action would be successful, make it unlikely that in many real-world scenarios individuals would accurately share their attitudes pertaining to their intentions. Nevertheless, a well-designed experiment can provide statistical evidence describing how attitudes and intentions are developed prior to a fraudulent action and thereby inform a previously under-studied research domain.

In the experiment described in this manuscript, the population of interest includes all people making online transactions, though determining a valid and viable sample from this group can be difficult. Consequently, a specific scenario was developed for exploring interpersonal fraud that included the buying and selling of textbooks online through an auction site (e.g., EBay; see Ba and Pavlou 2002; Pavlou and Gefen 2004). Deceitful exchanges can be complex processes with communicative cues being iteratively exchanged by parties engaged in the exchange (Buller and Burgoon 1996; Carlson et al. 2004), and studying an online auction transaction can mitigate the complex effects of iterative feedback. The misrepresentation of a material good for financial gain is a common form of online auction fraud. To replicate this type of fraud in an experimental setting, a group of participants will develop online profiles for selling books where the creators of the profiles with the highest sales totals will receive a financial bonus. Another group of participants will be tasked with selecting among the sales profiles created by the first group.

The degree to which a book is represented as being in better condition than it actually is in a sales profile created by study participants and the numbers of these fraudulent profiles that are selected for purchase by potential victims form the key dependent variables of interest and indicate the observed amount fraud through the misrepresentation of an asset. An advantage to limiting the scope of the study to the buying
and selling of textbooks include the ability to hold many of the features of the product being sold constant because a textbook can be considered to be largely commoditized (Brynjolfson and Smith 2000). A textbook is nearly identical, with the exception of condition, to other versions of the same textbook. Many other characteristics of the exchange including the price, place, and product can be held constant while the effects of changes in promotion, which are more salient in discussing the misrepresentation of an asset, can be explored. Online textbook purchasing is an activity common to college students, thus a sample taken from this population is a valid representation of and generalizable to others buying and selling similar products online.

Conclusion

This paper outlines a new perspective on how to view fraudulent transactions in the context of social exchange theory and technology adoption research. We offer a two-sided behavioral model that melds research from the information systems field with the fraud-related literature from accounting and auditing. Because of its foundations in these robust literatures, we are confident that this model will be useful in modeling behaviors in the context of fraud.

References


