Avatars, Capital Ships, and False Promises: An Analysis of Fraud in Virtual Worlds and its Implications for the Real World

William N. Dilla
Associate Professor of Accounting
Iowa State University

Andrew Harrison
Ph. D. Student in Business and Technology
Iowa State University

Brian Mennecke
Associate Professor of Information Systems
Iowa State University

Diane Janvrin
Associate Professor of Accounting
Iowa State University

We acknowledge helpful comments from an anonymous reviewer.

Contact author:
William N. Dilla
Associate Professor of Accounting
2330 Gerdin Business Building
Iowa State University
Ames, IA 50011 U.S.A.
wzilla@iastate.edu
1-515-294-1685
Avatars, Capital Ships, and False Promises: An Analysis of Fraud in Virtual Worlds and its Implications for the Real World

Abstract

We expand accounting research on fraud by categorizing and analyzing fraudulent acts in virtual worlds. Virtual worlds are computer-generated, immersive environments where players control a character, an avatar, to interact with others online while engaging in social, entertainment, educational, and commercial endeavors. Virtual worlds include unique capabilities such as anonymous interaction through an avatar and engaging and immersive visualizations. They also feature complex, unregulated economic environments. These features may increase the potential for rational individuals to commit fraudulent behavior and also likely encourage trusting beliefs and behaviors on the part of potential victims. To illustrate how and in what circumstances these environments can be used for fraudulent behaviors, we develop a socio-regulatory model to classify cases of virtual world fraud as within or outside social norms and regulations. We then adapt the “fraud diamond” model (Wolfe and Hermanson, 2004) to examine a number of documented cases of virtual world fraud. We discuss how observing virtual world behavior allows examination of the efficacy of explicit or implicit codes of conduct for preventing fraud within organizations, how virtual worlds allow observation of motivations of both the perpetrators and victims of fraud, and how fraud perpetrators use projected identities to commit fraud in virtual and real worlds. This research is important to accountants in organizations and society since we illustrate how virtual worlds can be used as “simulators” of real world fraud behaviors and show how behaviors and attitudes expressed in virtual worlds relate to comparable behaviors in real-world contexts.
Avatars, Capital Ships, and False Promises: An Analysis of Fraud in Virtual Worlds and its Implications for the Real World

My IPO where I raised 50 billion ISK in exchange for the future promise of my stuff was a scam. I'm not parting with all my stuff ... I have a really cool shirt that says on the front, "Social Engineering Specialist" and on the back reads, "Because there is no patch for human stupidity." I wear it a lot.

Curzon Dax, a player who perpetrated a $10,000 fraud in EVE Online. (Dax 2009)

Introduction

What do avatars, capital ships, virtual world banks, and Bernie Madoff have in common? The answer is, interestingly enough, provided in the quote above by a player named Curzon Dax, one of the most renowned fraudsters in online virtual worlds, who hinted at one of the important reasons why fraud occurs. While “stupidity” may have a part to play, what is particularly interesting about this quote is what it tells us about the attitude of the perpetrator; that is, that whether online or offline the attitudes and behaviors of both perpetrators and victims of fraud can’t be “patched.” Stated another way, whether we consider human behavior in “real” life or in virtual worlds like EVE Online, the fact is that fraud will be a common component of market activities and we can learn about fraudulent behavior by examining the attitudes and behaviors of Bernie Madoff in the real world and Curzon Dax in the virtual world.

The ability to learn more about fraud in virtual worlds is particularly important given the proliferation of online venues for commerce and the virtualization of the workplace (Reeves & Read, 2009). In these environments, where users often maintain a cloak of anonymity and
economic transactions are barely regulated, if at all, the potential for fraud is high. Yet, players often succumb to new and innovative tactics for perpetrating fraudulent transactions. Furthermore, these environments offer accounting researchers the opportunity to observe, interact with, and in some cases, manipulate the environment to conduct research to better understand the antecedents of fraud and ways to prevent it from occurring.

EVE Online is one of several virtual worlds where users assume the identity of an avatar and interact, socialize, conduct business, and engage in a variety of goal-directed activities. These activities might include killing a computer-controlled dragon to advance to the next level, engaging in battle with other users to seize their property or land, or building and running a business to sell wares or services. Virtual worlds such as EVE Online, Second Life, World of Warcraft, and others are similar regardless of their structure or rules (i.e., the Terms of Service or TOS) because economies exist where trading of game property or assets for other virtual or in some cases, real-world assets takes place.1

Because of these rich economic environments, virtual worlds provide more than a simple entertainment experience. Indeed, Reeves & Read (2009) argue that virtual worlds incorporate a wide range of substantive real-world work activities. Thus, virtual worlds have the potential to be more than games—they may be powerful environments for developing

1 The literature on virtual worlds (e.g., Bloomfield & Rennekamp, 2009, Reeves & Read, 2009) often makes a distinction between massive multiplayer online role-playing games (MMOGs), or structured games and virtual social worlds, or unstructured games. MMOGs involve structured, mission-oriented narratives, defined character roles, and explicit goals, while virtual social worlds do not (Reeves & Read, 2009, p. 26). Both environments involve real-time interactions between avatars and virtual economies that allow participants to buy and sell virtual goods. In this paper, we refer to any online environment that includes interactions between avatars and a virtual economy as a “virtual world.”
employee skills and improving their work engagement. If virtual worlds are to become part of the work environment, it is important to consider the possibility of virtual world fraud.

Virtual world economies are not limited to the area inside the “walls” of the game, since, in some cases by design and in others in spite of the rules, in-game assets can be converted to real-world currencies. For example, Second Life has been classified as an open game because the TOS allows the conversion of virtual earnings into real currency (Castronova, 2004; Mennecke et al., 2007). In fact, some users of these games have been able to amass substantial amounts of wealth by virtue of their activities (Chung, 2006, Kirkpatrick, 2007). Alternatively, closed games such as World of Warcraft specifically forbid the conversion of in-game assets; yet, unsanctioned markets exist outside of the confines of the game to convert and trade game assets for real currencies. The presence of wealth-building opportunities suggests that motivation exists for dishonest individuals to attempt to achieve gains through fraudulent activities.

We use “deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage” (Dictionary.com, 2011) as a working definition of fraud in this paper. This definition allows for consideration of fraud involving both virtual and monetary assets. Thus, we address fraudulent actions related both to virtual assets that have no corresponding value in the real world (as in closed games) and to virtual assets convertible to real-world assets (as in open games). The definition also allows for differences between virtual and real-world social norms and regulations. We consider actions that may be considered fraud in a virtual world, but not in the real world, and vice versa.
Virtual worlds provide a rich environment for archival studies of fraudulent behavior. They allow one to track the development of social phenomena without interfering with their development (Bainbridge, 2007, Williams, 2010). Further, there are substantial differences in the degree to which virtual worlds are regulated. One can compare behavior in closed games, where the game proprietor ostensibly regulates the economic environment through the TOS, to that in open games, where to date the simulated economic environment is largely unregulated (Carli, 2007; Bloomfield & Rennekamp, 2009; Bloomfield & Cho, 2010). Further, as game proprietors change their rules to prevent fraudulent activity, one can compare behavior before and after the change. This can provide insights into what extent regulation plays in preventing fraudulent behavior.

Yet, application of economic and legal theories can only partially explain how and why fraud occurs in virtual worlds. There are also interesting psychological aspects to consider (Yee, 2006a). Since the virtual world player assumes the identity of an avatar, the parties to a fraudulent transaction do not engage in direct physical interaction. This suggests similarities to other online environments, where fraud perpetrators gain power over their victims through a negotiation process in which they employ various deception techniques such as masking information, disguising information, distracting the victim’s attention away from information, and assuming someone else’s identity (Albrecht et al., 2007, Grazioli & Jarvenpaa, 2003). An important difference between virtual worlds and other online environments is that in most online environments assuming another identity is considered deception, while in virtual worlds assuming another identity is part of the environmental structure. Indeed, Mennecke et al. (2010) propose the virtual world participant’s embodied virtual representation (i.e., the avatar)
as the nexus of activity in social interaction within virtual worlds. This embodiment makes it likely that a virtual world player might engage in acts that they would not commit in the real world (Skaar, 2009; Olivetti, 2010). Examining fraudulent behavior in virtual worlds provides insights into whether and how identity representation influences such behavior.

The observation of fraudulent activity in virtual worlds is of particular interest to accountants in organizations and society for three reasons. First, virtual worlds provide the opportunity to observe the results of behavior in which the economic and social environments differ only along one or a few dimensions (Bloomfield & Rennekamp, 2009). While this brings to mind the opportunity to observe the efficacy of alternative market and regulatory structures in preventing fraud, “field” research in virtual worlds can also be used to determine the efficacy of explicit or implicit codes of conduct in preventing fraud within organizations. This is important, as scant data exists on the efficacy of codes of conduct and other control mechanism in preventing such frauds. Second, studying fraudulent activity in virtual worlds gives one the opportunity to observe the motivations of both perpetrator and victim. The classic “fraud triangle” widely used in accounting research focuses almost entirely on perpetrator characteristics and assumes that the perpetrator is motivated by financial pressure (Loebbecke et al., 1989; Albrecht et al., 2009). However, there are times where the perpetrator’s desire for prestige or control supplements or even replaces financial pressure (Gauthier-Villars & Mollenkamp, 2008). There are also times when the victim’s desire for financial gain or prestige plays an important part in the fraud scheme, and little is known about this phenomenon because victim motivations are rarely mentioned in fraud litigation proceedings. Finally, virtual worlds give us the opportunity to observe whether fraud perpetrators’ beliefs and actions are
consistent across different contexts and environments. Since an avatar is a player’s embodied virtual representation (Mennecke et al., 2010), and his or her true identity is often anonymous to other players, to what extent does this embodiment allow the player to rationalize actions he or she would not otherwise under take in real life? This is an important point to consider—cases in which an apparently honest person has rationalized taking corporate assets have occurred numerous times, but why such rationalizations take place is not well-understood.

In this paper, we first describe the characteristics of virtual worlds and their economics. Second, we develop a two-dimensional classification scheme for fraudulent acts involving virtual worlds and describe a framework for analyzing these acts. It categorizes cases by whether the fraudulent act is considered to be within or outside: (1) virtual world social norms and (2) virtual world regulations. We also describe how the “fraud diamond” outlined by Wolfe and Hermanson (2004) provides a framework for analyzing virtual world fraud. Third, we identify a number of cases of fraud in virtual world environments and categorize them according to our classification scheme. Fourth, we perform an analysis of these cases according to the dimensions of the fraud diamond. Finally, we state the implications of our analysis and make suggestions for future research.

**Characteristics of virtual worlds**

**Characteristics of virtual world players**

While the popular press and even some academic literature perpetuates a stereotype of Internet and video game players as adolescents who prefer to engage in violent games (e.g., Holtz & Appel, 2010), Yee’s (2006b) survey of Massively Multiplayer Online Role-Playing Game
(MMOG) players suggests a very different picture. While 85 percent of Yee’s (2006b) respondents were in fact male, his results contradict the stereotype of virtual worlds as an adolescent environment with the average age of respondents being 26.6 (with a median of 25) and an age range of 11 to 68 (with an inter-quartile range of 19 to 32). Furthermore, he found that 50 percent of respondents worked full-time while only 22 percent were full-time students. By way of comparison, the population of Second Life users is somewhat more balanced by gender at approximately 55 percent male with a higher average age of 32 (Rosedale, 2008).

When we consider that most players in virtual worlds are working adults and that these individuals utilize discretionary time to engage in virtual world activities, it is important to consider the motivation that “drives” virtual world users. Yee (2006b) identifies five factors that motivate individuals to participate in MMOGs (See Table 1). The five factors, relationship, manipulation, immersion, escapism, and achievement, can each individually or in combination influence users to participate in one or more virtual world activities. We consider each of these as having potential to enable fraudulent behaviors, however, some of these factors such as manipulation and achievement appear to be more important in motivating perpetrators while relationships and achievement might be more influential in causing victims to be defrauded. In addition, factors such as immersion and escapism might function as tools that can be used to facilitate fraud. For example, one important relationship between immersion and escapism motivations and the structures and capabilities afforded by virtual worlds is the player’s ability to project a unique identity into the virtual space. In the next section we discuss the potential role that this ability to project such an identity has in influencing fraudulent behaviors.

Insert Table 1 about here.
**Projection of identity into the transactions space**

Users of virtual worlds “inhabit” virtual spaces using an embodied representation called an avatar to represent their presence and interact or carry out transactions with others in the space (See Figure 1). Avatars can take on many embodied representations, such as idealistic humanoid forms (elves, dwarfs, a superhero, etc.), animals (bears, dogs, aliens, etc.), or inanimate objects (e.g., a spaceship, a credit card, etc.). Further, players often choose avatars that bear little resemblance to their physical self, even being of the opposite gender (Levine, 2007). These representations can have an important influence on how the user perceives other social actors and how he or she behaves.

A user’s perception of presence, or being in the virtual world space, will be influenced by several factors, such as his or her readiness to suspend disbelief, the degree of physical or psychological immersion, the quality of the media, the presence and appearance of virtual objects, and the physical surroundings of the user. The presence or absence of other embodied avatars increases the user’s sense of presence (Biocca, 1997; Biocca et al., 2003; Mennecke et al., 2010). Furthermore, this sense of engagement is important because it will lead to greater involvement in the virtual world space and specifically with the other avatars (i.e., people) present in that space (Nah, et al., 2010a; Nah, et al., 2010b).

The result of embodiment in a virtual world is that users are likely to feel closer to others they interact with and as a result they are likely to trust them more than they would if they were using other media to interact. This higher level of trust is important because it will
likely offer opportunities for exploitation and trust violations. Trust is a critical antecedent in
most online interactions, particularly in encounters that involve transactions and exchanges
such as purchasing or selling goods or services (Gefen et al. 2008; Kaplan and Nieschwietz,
2003). As a medium that has the potential to promote trust through virtual proximity and
embodied representations, virtual worlds have the potential to create trusting attitudes in
users that may lead to potential opportunities for fraudulent behavior. Our position is that the
virtual world’s unique characteristics foster user attitudes that can lead to fraudulent behavior
through simulation of real-world social norms.

*Characteristics of the transactions space*

Each virtual world proprietor sets the rules by which a user’s projection is allowed to
interact with other social actors in that world’s virtual space. There is much diversity among
virtual worlds in terms of transaction space features. Castronova (2004) identifies two types of
games: closed and open. Closed games like World of Warcraft have TOS that allow in-game
trade of goods and services, however, in-game assets remain the property of the proprietor and
have no legitimate real-world value. As a result, closed game TOSs specifically forbid users to
convert virtual assets into real-world currency. In open games like Second Life, the TOS allows
or encourages trade inside of the game by granting players intellectual property rights to their
self-created virtual assets. Players may also trade in-world assets for assets outside of the game
using a currency exchange, such as Second Life’s LINDEX. Because game assets can be
converted into real-world currency, it is possible for individuals to earn substantial real wealth by participating in unstructured games (Freedman, 2008; Papagiannidis et al., 2008).

**Categorizing and analyzing fraudulent actions in virtual worlds**

**A socio-regulatory model of virtual world fraud**

Social norms within and across different virtual worlds vary significantly and often are quite unique relative to the “real world.” Behaviors like theft or assault might be condoned or encouraged in some worlds, while such behaviors would be considered serious offenses in others (McCarthy 2006). For instance, engaging in piracy and theft from other players to fund one’s exploits is accepted and even encouraged in EVE Online (Drain, 2010b). Indeed, EVE Online distributes to new players an official guide to becoming a pirate (MMM Publishing, 2006), extolling the exciting nature of the experiences piracy offers. In contrast, other games have explicit codes of conduct spelling out social norms that are closely aligned with real-world norms (Habbo Hotel, 2009; RuneScape, 2011; Second Life, 2011).

Similarly, regulatory policies vary across virtual worlds. The most important regulatory policy with respect to virtual world fraud is whether a game is closed or open to the transfer of virtual to real assets. Theft of virtual assets is often within the social norms of a game such as

---

2 The open / closed distinction exists along a continuum. For example, EVE Online, an otherwise closed game, allows limited trading of the game’s currency (Inter-Stellar Kredits or ISK) for game time, which has a real-world value (Drain 2010a). Sixty-day game time codes purchased for cash can be converted into Pilots License Extensions (PLEX), which become items in the game. The PLEX can then be traded to other players for the game’s currency, creating a legitimate way to buy ISK. Likewise, players with ISK to spare can buy PLEX from the market and redeem them for game time.
EVE Online, but the conversion of ill-gotten virtual assets to real currency is against the game’s TOS and is likely to result in a player’s suspension.

Because social norms and regulations vary across virtual worlds, we offer a socio-regulatory model of fraudulent behavior in virtual worlds that takes norms and regulations into account (Figure 2). This model is adapted from the literature on corporate social responsibility where economic, legal, and ethical motivations form a set of overlapping domains and behavior is motivated by a combination of economic self-interest, regulatory compliance, and normative social influences (Carroll, 1991; Schwartz & Carroll, 2003). Because of the analogous relationships between these constructs, we re-label ethical motivations as social norms and legal motivations as regulation. Furthermore, because our focus is on fraud, we replace the economic self-interest component of the Schwartz and Carroll (2003) model with the construct of fraudulent behavior.

Insert Figure 2 about here.

**Categories of virtual world fraud**

The model shown in Figure 2 suggests a categorization of fraudulent actions in virtual worlds along two dimensions: the *social norms* and *regulatory policies* of the virtual environment inhabited by the party or parties affected by the act of deception. The fraudulent actions can be either within or outside the social norms or regulatory policies of the virtual world, resulting in four possible categories. We classify an action as being outside the social norms of a virtual world if the actions of the perpetrator would be widely regarded by that virtual community as inappropriate behavior. In these situations, the perpetrator is likely to
leave the virtual world due to the social ramifications and reputational risks caused by their actions. In contrast, if the behavior would be overlooked, ignored, or celebrated by the average member of the virtual community, it is considered to be within the social norms of that community.

We classify an action that results in censure or suspension by the virtual world’s proprietor as outside virtual world regulatory policies. Further, if the proprietor initiates real-world legal proceedings against the perpetrator or cooperates with authorities in a criminal investigation, we assume that the fraudulent action was also considered to be outside virtual world regulatory policies. Behavior that does not result in suspension or any other type of disciplinary action by the virtual world proprietor is considered to be within the virtual world’s regulatory policies.

**Analyzing fraud in virtual worlds with the “fraud diamond”**

The fraud triangle has been widely used by practitioners to facilitate fraud risk assessments (e.g., AICPA, 2002) and by academics to describe and analyze the factors leading to fraud (e.g., Loebbecke et al., 1989; Hogan et al., 2008). The fraud triangle defines three elements that must be present for fraud to occur: (1) a perceived pressure or motivation, (2) a perceived opportunity, and (3) the ability of the perpetrator to rationalize the fraud as acceptable (Albrecht et al., 2009). More recently, Wolfe and Hermanson (2004) have argued that practitioners should also consider the capability of a potential perpetrator to commit fraud, resulting in a four-cornered “fraud diamond.” Because of the importance of perpetrator capability in committing fraud in virtual worlds, we use the fraud diamond as a basis for our analysis of virtual world fraud cases.
Panel A of Figure 3 displays the components of the fraud diamond and outlines their application to virtual world fraud. First, a virtual world player must have a motivation to commit fraud. As in the real world, this motivation may arise from personal financial pressures or simply from the desire to accumulate assets (i.e., greed). In addition, two of the motivational factors offered by Yee (2006b) appear to be important: achievement and manipulation. Individuals with strong achievement motivations may engage in fraudulent activity to accumulate in-game assets or commit a complex fraud to demonstrate how clever they are. Those with strong manipulation motivations may engage in fraudulent activity in order to dominate other players or the game operators.

Second, an individual must perceive that they have the capability to commit fraud. Three types of capabilities appear to be important in this context. First, perpetrators may have sufficient technical knowledge to commit fraud through actions such as exploiting weaknesses in programming code or by using an automated program (i.e., a bot) to illegally generate or steal in-game assets. Second, they may understand how to exploit weaknesses in rules governing virtual world organizations or economic institutions in order to commit fraud. Finally, perpetrators may have the ability to manipulate their victims into erroneously believing that they are worthy of being trusted. These capabilities are not mutually exclusive—more than one may be present in a given case of fraud.

Third, perpetrators in virtual worlds must be able to rationalize that their fraudulent behavior is worth the risk. They may rationalize that their activities are not unethical because
they do not violate a game’s explicit formal rules. However, other game players may consider an individual’s actions to be fraudulent if they violate either real or virtual world social norms. A virtual world player may also rationalize committing fraud because he or she believes that other players are inferior and therefore deserve to be exploited (e.g., Dax, 2009). Further, a player might rationalize fraudulent behavior if they believe that they can hide behind the embodiment of their avatar and escape any sort of real-world consequences.

Finally, the virtual world perpetrator must perceive that there is an opportunity that makes it possible for them to commit fraud. As shown in Panel B of Figure 3, we expand the opportunity element of the fraud diamond into two sub-factors: environmental factors and victim characteristics. The professional and academic accounting literature tends to focus on environmental factors such as lax internal controls, ineffective corporate governance, or lack of adequate regulatory oversight (Hogan et al., 2008). Victim characteristics are mentioned infrequently in this literature, even though research suggests that fraud perpetrators choose their tactics to take advantage of their victims’ known or perceived weaknesses (Johnson et al. 1993, Grazioli and Jarvenpaa 2003). An advantage of studying fraud in virtual worlds is that these environments provide the investigator with the possibility of simultaneously examining perpetrator and victim characteristics, as these are both widely discussed in news articles and online forums addressing virtual worlds.

We identify three types of environmental factors related to virtual world fraud. The first group of environmental factors involves in-game regulatory policies, which includes both a “hard” and a “soft” set of governance structures that may influence fraudulent behaviors. Specifically, “hard” factors include virtual world programming code, which defines and
encapsulates explicit and implicit rules and constraints of “game play” by specifying what is and is not allowed. Hard factors define whether and how items such as code weaknesses might be exploited to commit fraud. Alternatively, “soft” factors include the governance and internal control structures developed by virtual world organizations and proprietors and are manifest in the game’s TOS and other in-game regulations. By extension, a third factor is present to limit fraud when a game’s proprietor implements monitoring activities designed to detect illegal in-game activity.

The second group of environmental factors concerns real-world regulatory policies and centers around the inconsistent definition and application of the law to virtual worlds. For example, actions that are considered legal in a virtual world may be illegal in the real world, and vice versa. These inconsistencies arise because of a number of reasons, but several prominent factors include the lack of legal precedent concerning virtual assets, perceptions about the value or ownership of virtual assets (e.g., authorities may be unwilling to prosecute cases of virtual world fraud), and inconsistent regulations concerning virtual assets that exist across jurisdictions.

The third group of environmental factors involves social norms such as the set of informal rules that might emerge within a given virtual environment. In some games such as World of Warcraft, players are quick to report unethical behavior, whereas in games such as EVE Online, a certain level of unethical behavior is encouraged (McCarthy 2006). Social norms include the possibility that an individual may assume alternate virtual identities to conceal their actions. For example, the use of alternate identities (alts) is widely accepted in Second Life unless a participant uses their alts to commit fraud, which is against both the virtual world’s
social norms and its TOS (Second Life, 2010). Finally, social norms may include player resistance against proprietor attempts to impose stricter game regulations.

   Victim characteristics include their motivation, misplaced trust, and lack of knowledge. Investors’ motivation to earn above-average rates of return is often a characteristic in real-world frauds such as the Madoff case (Economist, 2008). Similarly, a virtual world player with a strong achievement motivation (Yee, 2006b) is likely to be susceptible to fraudulent solicitations that promise easy advancement or accumulation of virtual assets. Further, individuals who possess strong relationship motivations might be likely to put misplaced trust in fraud perpetrators. Finally, individuals who lack knowledge about their environment or the game structure may be susceptible to fraud. Players who are unaware of safeguards over economic activity (e.g., market regulations), corporate governance structures, online security practices, and formal or informal game rules are more likely to become fraud victims compared to those who are more knowledgeable about these environmental factors.

Cases of fraud in virtual worlds

Methodology for Case identification and selection

   We used Internet-based searches as our primary strategy for locating information about virtual world fraud for three reasons. First, research examining fraudulent behavior in virtual worlds is not well developed. Therefore, a more traditional literature review of academic literature would result in insufficient information for our analysis and Internet searches would provide more current news sources covering a wide spectrum of environments and behaviors. Second, as a relatively new environment for fraud, virtual worlds lag behind other Internet
platforms in terms of both detection and response. Therefore, we would expect that most information about fraud would be detected by searching “unconventional” sources such as forums or game periodicals. Finally, most virtual world fraud tends to be of a smaller scale (i.e., less than $10,000) than traditional corporate fraud cases and is therefore less likely to show up on the “radar” in traditional sources (e.g., IC3, 2010).

We supplemented searches of conventional article indices (i.e., ABI/Inform, Google Scholar, and LexisNexis) with searches of Internet resources likely to contain information about virtual world fraud (i.e., massively.com, Technorati, and virtual world message boards). We used the keywords “virtual,” “virtual world,” “virtual fraud,” “fraud,” “virtual theft,” “theft,” “con,” and “scam.” Cases used for our analysis were corroborated through multiple news articles, legal documents, research papers, blogs, or original posts made by participating individuals or organizations. Often, virtual fraudsters would recollect and publicize their exploits in a boastful memoir, which made it easier to document the case’s background, user motivations, and outcomes. We included cases that could be traced back to an edited news source, legal documents, or a first-person account of the incident in the analysis and deleted cases that were hypothetical or vaguely described. In accordance with the methodology used by Grazioli and Jarvenpaa (2003), we used the following criteria to filter the cases:

- Two parties were in a conflict of interest
- An exchange took place that dealt with the possession or acquisition of virtual world assets
- The deceiver made a misrepresentation that gave him or her an unfair advantage over the target
- We found clear indications that the case actually occurred.

We did not include cases that were too vaguely described to accurately categorize in our framework.

We developed a brief description of each case, then determined whether the perpetrator’s actions were considered to be within or outside social norms for the virtual world where the fraud occurred and whether they were within or outside the virtual world’s regulatory policies. If the information was available, we converted the value of the theft to U.S. currency for comparison purposes. Finally, we determined the fraud diamond components relevant to the fraud to the extent possible given the available information.

We deemed three types of cases closely related to virtual world fraud to be outside the scope of our analysis. The first type include cases where a perpetrator claimed to have virtual world assets to sell online, but failed to deliver the assets after receiving money from the victim (Collington, 2010; Holisky, 2010). While these cases involve virtual assets, all the interaction between the perpetrator and the victim took place online outside of a virtual world. As such, these cases fall into the broader category of consumer deception on the Internet (Grazioli & Jarvenpaa, 2003; Nikitkov et al., 2011). Second, we did not examine cases that used virtual worlds to launder money derived from illegal activities (Monroe, 2007; Muttik, 2008). Virtual world money laundering is a serious and significant criminal activity; however, the funds only pass through the virtual world—the criminal activities that generate the funds (e.g., selling illegal drugs) or for which the funds are used (e.g., terrorism) occur in a real-world environment. Finally, we excluded cases that used game software to place malware on a user’s computer in order to gain access to sensitive data such as bank account information (Muttik,
2008). As with money laundering, this is a potentially serious criminal activity; however, addressing this problem requires technical solutions that are beyond the scope of this paper. In summary, we excluded cases involving real assets where fraud or other criminal acts take place in the real world.

Tables 2, 3, and 4 display information about our identified cases of virtual world fraud, classified by whether the fraudulent acts are considered inside or outside virtual world norms and inside or outside virtual world regulatory policies. We identify one case where the perpetrator’s actions were regarded within both virtual world norms and regulatory policies (Table 2), five cases where their actions were regarded as outside virtual world norms, but within regulatory policies (Table 3), and 11 cases where their actions were regarded as outside both virtual world norms and regulatory policies (Table 4). We did not identify any cases where the perpetrator’s actions were regarded as within social norms, but outside regulatory policies.

Insert Tables 2, 3, and 4 about here.

**Within both social norms and regulatory policies**

Table 2 outlines the details of the one case of fraud we identified where the perpetrator’s actions were considered to be within social norms and regulatory policies for the virtual world where the actions occurred. It involved destruction of the Band of Brothers (BOB) organization in EVE Online through an act of virtual corporate espionage (Egan, 2009b; Graham, 2009). A disgruntled BOB director defected to GoonSwarm, a rival organization. Once assured of a safe place within the rival, he exploited a control weakness to disband BOB and steal nearly
all of its assets, apparently taking BOB’s in-game currency for himself and transferring the organization’s capital assets to GoonSwarm.

Given the size and importance of the two organizations in the EVE Online environment, this coup has been likened to “Apple dissolving Microsoft” (Graham, 2009). The director’s actions are considered well within the norms of EVE Online, where usually unacceptable behaviors such as theft and deceit are not only condoned, but are considered valid tactics for competitive actions (Drain, 2010b). Because there are no game rules forbidding theft of assets from individuals or organizations in EVE Online, the theft was also within the game’s regulatory policies.

**Outside social norms, but within regulatory policies**

Table 3 shows the cases which involve fraud that was outside the virtual world’s normally accepted behavior, but did not violate official regulatory policies. All of the cases in this category have characteristics that parallel real-world banking and investment scams. They all involve individuals or virtual world institutions (i.e., banks or investment funds) that managed to gain investors’ trust. Once trust was garnered and the investors had handed over their assets for what they thought was a lucrative opportunity, perpetrators stole the assets. While there were no direct formal or legal sanctions against these perpetrators, several cases resulted in the perpetrator being forced to leave the virtual world because of social stigmas associated with their actions. A notable exception is the case of alleged misappropriation of capital raised in the Second Life CAPEX by corporate CEOs (Bloomfield & Cho, 2010). Investors were unable to take either informal or formal sanctions against the CEOs because these players were able to operate with anonymity.
Outside social norms and outside regulatory policies

Table 4 lists the cases in which activities were considered to be outside the social norms and regulatory policies of the virtual world in which they occurred. Nearly all of the cases in this category are classified as outside virtual world regulations for one of two reasons. Seven cases involve conversion of closed game virtual assets into real assets, which is against these games’ TOS. Five cases involve deception strategies executed outside virtual world boundaries, such as worms, Trojan horses, and phishing sites. These are against both virtual world and real-world regulations. Only two cases fall outside these two categories. The perpetrator in the Final Fantasy XI theft of assets (Brewer, 2008; Welsh, 2008) was manipulated into sharing his login credentials with the perpetrator. The Second Life auction deception case (Anderson, 2006; Cheng, 2007; Craig, 2006; Reuters, 2007a; Walsh, 2006) involved what the game’s proprietor deemed to be unauthorized early access to a land auction.

Socio-regulatory differences between virtual and real environments

Regulatory policies are socially constructed and ultimately derived from social norms (Edelman & Suchman, 1997) and as a result, virtual and real-world regulatory policies influence one another. New or unanticipated actions occurring within or mediated through a virtual world can result in real-world legal actions (Barrett, 2009; Sophos, 2005; Sophos, 2007). In some cases, actions occurring within the virtual world are perceived as violations of real world laws (Knight, 2005b), while in others, virtual world actions are considered to be outside the

---

3 The total number of cases mentioned (12) adds up to more than the total of 10 in this category, as some cases involve both conversion of closed game assets and deceptions executed outside virtual world boundaries.
scope of real world laws (Brewer, 2008; Finlayson, 2005; Welsh, 2008). Additionally, virtual
world players are not always governed by the same legal polices as a result of the
geographically dispersed nature of virtual world participation, causing confusion in interpreting
jurisdictional authority.

Table 5 and Figure 4 summarize cases that shift between categories when analyzed in a
virtual versus real-world socio-regulatory context. There are two types of classification changes.
The Band of Brothers case (Egan, 2009b; Graham, 2009) shifts from being classified within EVE
Online’s social norms and regulatory policies to classified outside real-world social norms and
regulatory policies. Double-crossing a colleague to destroy the organization that both parties
invested time and energy to develop is outside most individuals’ real-world social norms, yet
such behavior is allowed and encouraged in EVE Online (Drain, 2010b). Similarly, an individual
stealing corporate assets is against real-world norms, but acceptable within EVE Online’s TOS.
Even so, the classification of deceptive actions as within EVE Online’s social norms is not always
clear-cut. Unlike other large frauds where perpetrators were forced to or voluntarily left the
game, the Band of Brothers perpetrator was able to remain in EVE Online only because he had
sought the protection of a rival organization before destroying the Band of Brothers and
stealing its assets.

The remainder of the cases listed in Table 5 are situations that involve shifts from
classification outside virtual world regulatory policies to within real-world regulatory policies. In
most of these cases, the distinction arises because conversion of virtual assets into real
currency is against the game’s TOS. These actions are outside of the regulatory policies of the
virtual worlds in which they occur, however, conversion of virtual into real assets generally does not violate current real-world laws and the perpetrators seldom face legal consequences. This divergent classification shows the importance of evaluating virtual behaviors in the both virtual and real-world socio-regulatory contexts to understand how virtual regulations and social responsibilities are related to their real-world counterparts.

The sole exception is the Second Life land auction dispute (Anderson, 2006; Craig, 2006; Walsh, 2006; Cheng, 2007). Marc Bragg, the alleged perpetrator, filed a lawsuit against Second Life proprietor Linden Lab claiming that the shutdown of his account and seizure of his virtual assets was illegal. Bragg asserted that according to Second Life’s TOS, rights to virtual property owned by Second Life residents belong to the players. A Pennsylvania judge agreed to hear the lawsuit on the grounds that Linden’s TOS did not allow Second Life participants an effective means of resolving disputes with the proprietor (Reuters, 2007a). The case was eventually settled out of court (Reuters, 2007b). Due to the confidentiality of the settlement, real-world law regarding the conversion of assets illegally obtained within an open game such as Second Life remains ambiguous.

Case analysis

Perpetrator motivations

Perpetrator motivations in four out of six of the cases classified as within virtual world regulatory policies (Tables 2 and 3) appear to be achievement, manipulation, or a combination of both (Yee, 2006b). Perpetrators in these cases appear to misappropriate virtual funds so they can improve their status and power in the game. In at least two cases, it appears that the
perpetrator had a strong desire to manipulate others. EVE Intergalactic Bank (EIB) scam perpetrator Cally and investment fraud perpetrator Curzon Dax both left detailed accounts of their exploits, explaining that a substantial part of their motivation was the enjoyment they received from fooling other players who they believed to be inferior (i.e., gullible, less intelligent, or less skilled) (Google Video, 2006; Dax, 2009).

In two cases classified as within virtual world policies, the perpetrators’ motivations seem to mimic real-world motivations for committing fraud. First, managers in the Ginko Financial case (Alphaville Herald, 2007; Second Thoughts, 2007; Talbot, 2008) were apparently motivated by greed—virtual assets accumulated by the bank and skimmed from investors could be converted to real assets. Second, indirect evidence suggests that CEOs of firms trading on the Second Life CAPEX who retained invested funds were also motivated by greed (Bloomfield & Cho, 2010). While it is not clear whether the CEOs entered the market with the express intention of skimming investor funds, it is plausible that some individuals became motivated to commit fraud once they became aware of how to accumulate substantial assets in this fashion.

Finally, it appears that perpetrator Bad Bobby of the Titans4U case (Drain, 2010c; Geere, 2010; Lau, 2010) may have been motivated by both achievement and greed. Bobby’s initial plan seems to have been to accumulate funds to support his own game play, however, he eventually accumulated EVE Online virtual assets worth $45,000, which represented sufficient funds to purchase 214 years of game time (Polo, 2010). This suggests that Bobby continued to be motivated to accumulate additional assets for personal benefit (i.e., greed).

Perpetrators appear to have been motivated by the possibility of accumulating real assets in eight out of the eleven cases classified as outside virtual world regulatory policies
Achievement appears to have been a motivation in two out of the remaining three cases classified as outside virtual world regulatory policies. Initially, the perpetrators in the Outwar click fraud case were reported to have sold the IP addresses of infected machines to would-be spammers, however, it turned out that their motivation for the phishing attack was merely achievement within the game (Leyden, 2004). It also appears that the perpetrators who used phishing to steal virtual furniture in Habbo Hotel (BBC News, 2007; Sophos, 2007) were motivated by in-game achievement. Finally, it is not clear whether the perpetrator in the Final Fantasy XI case (Brewer, 2008; Welsh, 2008) was motivated by in-game advancement or financial greed because the available news accounts do not state whether the stolen items were converted into real assets.

Perpetrator capabilities

Perpetrators in all the cases classified as within virtual world regulatory policies understood how to exploit weaknesses in rules governing virtual world organizations or economic institutions in order to commit fraud. There are two cases where the perpetrator’s ability to manipulate others was also an important factor. Curzon Dax understood very well that potential victims would trust a game figure well-known as an entrepreneur and entertainer (Egan, 2009c; EVE Online Forum, 2010). He used this fame to lure investment into a “special” fund, in a manner similar to the way Bernie Madoff enticed victims through his personal
relationships and reputation (Economist, 2008). Titans4U fund manager “Bad Bobby” was able to use his reputation as a fund manager to convince other company directors to allow the sale of shares which eventually gave him control over the fund’s assets (Drain, 2010c). In contrast, in the cases where virtual world banks or the Second Life CAPEX was used to commit fraud, perpetrators remained relatively anonymous and did not directly manipulate their victims.

Eight of the cases involving behavior classified as outside virtual world regulatory policies involve technical capabilities. As mentioned earlier, five out of the 11 cases in this category involve deception strategies executed outside virtual world boundaries, such as worms, Trojan horses, and phishing sites. Another three involve exploiting weaknesses in virtual world programming codes. Of the remaining three cases in this category, two involve perpetrators manipulating victims into believing they could be trusted and one involves knowing how to exploit a weakness in a virtual bank’s governance structure.

**Perpetrator rationalization**

In some cases, perpetrators rationalized that if there were no rules expressly forbidding their actions, there was nothing wrong with what they did. Ginko Bank CEO Nicholas Portacarrero openly stated that his bank did nothing wrong (Alphaville Herald, 2007; Second Thoughts, 2007). He also denied any responsibility for the bank’s collapse, instead blaming the failure on Linden Lab’s decision to shut down Second Life casinos. In the Second Life auction fraud case, Marc Bragg claimed that because the game proprietors made it possible to access land auctions before they were open to the public, there was nothing wrong with his actions (Craig, 2006).
The impact of rationalization on a perpetrator’s likelihood to commit fraud is difficult to assess in a game such as EVE Online, where deceit and theft are acceptable behaviors (Drain, 2010b). In this environment, rationalization appears to consist of deciding whether one’s actions are going to be considered “normal” behavior or whether they fall outside the game’s social norms. In many respects, this is analogous to the real world where certain fraudulent actions involving low value assets might be unlikely to result in prosecution but social norms preclude the perpetrator from engaging in the behavior (e.g., one would be unlikely to be prosecuted for defrauding a friend of $50 but such an action would negatively affect the friendship).

In two cases, perpetrators rationalized their actions because they perceived themselves to be intellectually superior and thought their victims deserved to be fooled. EIB CEO “Cally” released a video stating his rationalizations (Google Video, 2006). Similarly, Curzon Dax posted a message stating that he had become bored with the game and decided to pull off one final scam to take advantage of other players he considered to be ‘stupid’ (Dax, 2009).

The exact role of virtual world embodiment in enabling virtual world participants to rationalize their actions appears to vary from case to case. Some perpetrators provide misinformation or otherwise maintain a cloak of anonymity to separate their online activity from their real-world identity. For example, Ginko Bank perpetrators Hinoserm Rebus and Nicholas Portocarrero were apparently alternate characters controlled by the same individual (Alphaville Herald, 2007) and CEOs of firms trading on the Second Life CAPEX enjoyed considerable anonymity (Bloomfield and Cho, 2010). In fact, it is only rarely that a real-life
individual behind an avatar such as EIB executive Cally “outs” themselves to admit their fraudulent actions (Google Video, 2006).

**Opportunity**

*Environmental factors*

*Virtual world regulatory policies*

Programming weaknesses or “bugs” do not seem to be a significant long-term factor in providing an opportunity for virtual world fraud. Proprietors have moved quickly to fix weaknesses in game code, such as those that allowed players to produce fraudulent currency in EverQuest 2 (Knight, 2005a; Terdiman, 2005) and allowed an individual to use a bot to beat up and rob virtual characters in Lineage 2 (Knight, 2005b). Further, when these exploits are used they generally do not have long-term consequences. One exception to this is the Second Life land auction case (Anderson, 2006; Craig, 2006; Walsh, 2006) where Marc Bragg sued Linden lab to reclaim his confiscated assets (Cheng, 2007; Reuters, 2007a, 2007b). Given that the settlement details are not public, one might presume that Linden Lab was forced to cede assets (real or virtual) back to Bragg.

The lack of effective virtual organization governance or internal controls appears to be a factor in all cases where fraud was classified as within virtual world regulatory policies. This is also true of the EBAnk theft case in EVE Online, which is classified as outside regulatory policies because it involved the conversion of stolen virtual assets into real currency (BBC News, 2009; Egan, 2009a). In most of these cases, internal controls were weak or simply did not exist. In others, such as the Band of Brothers (Egan, 2009b; Graham, 2009) and Titans4U (Drain, 2010c) cases, these entities developed what appeared on the surface to be strong governance
structures, however, the perpetrators were able to find and exploit control weaknesses to steal the organizations’ assets.

When the frauds mentioned above were committed, the virtual worlds involved did not regulate investments in virtual corporations, banks, or other institutions. Subsequent regulatory responses have differed across virtual worlds. EVE Online has steadfastly refused to develop significant financial regulation, even as substantial frauds continue to occur (Egan, 2009a). Indeed, EVE Online players tend to view the opportunity to interact in a more or less lawless environment as one of the game’s attractive features (Drain, 2010b; McCarthy, 2006). On the other hand, Second Life began to regulate banks in early 2008 (Second Life, 2007) and shut down banks that did not comply (Semuels, 2008).

Another important aspect of virtual world regulation involves the TOS agreements for closed games that prohibit the exchange of game assets for real-world assets. It is not clear how effective these provisions are in deterring fraud given that we identified seven cases where the perpetrator either was known to or apparently had converted stolen virtual assets to real assets. These provisions set up an interesting “end-game” problem where, for example, a virtual world player who has grown tired of a game and does not care if they get thrown out for illegal conversion of stolen goods will not be deterred from committing one last fraudulent act in that game.

Finally, efforts to monitor player behavior vary across virtual worlds. Some games have mechanisms for detecting, reporting, and sanctioning fraudulent in-game behavior (McCarthy, 2006). For example, World of Warcraft has rules of etiquette that are tough and strictly enforced. Malicious players in this game tend to be quickly discovered and exiled. Second Life
has an extensive set of procedures for dealing with abuse (Second Life, 2011). Abusers can be identified through other players’ reports or through Second Life’s monitoring mechanisms (Talbot, 2008). On the other hand, unethical behavior is accepted and even encouraged in EVE Online (Egan, 2009a; Drain, 2010b). Indeed, efforts to rein in EVE Online player behavior have been considered controversial (McCarthy 2006).

Real world regulatory policies

There are effective sanctions for individuals who use real-world techniques such as computer worms and identity theft to steal virtual assets. Since there is established law regarding these actions, these individuals can be and often are punished (e.g., Sophos, 2004, 2005, 2007). Game proprietors appear willing to cooperate with the law in such cases and in some cases have launched their own internal investigations to detect offenders. For example, Jagex, the proprietor of RuneScape, has been aggressively pursuing “phishing thieves” and cooperating with authorities in the US and UK to ensure their arrest (Ward, 2009).

While game proprietors and law enforcement often cooperate to investigate and punish acts of deception that include an out-of-game element, the picture is very different for fraudulent acts that occur within virtual worlds. As far as we know, there have been no formal legal consequences in any of the cases we describe involving theft of virtual assets in virtual environments. Attempts to recover stolen virtual assets under U.S. law have been unsuccessful (Brewer, 2008). To date, the only countries known to consider theft of virtual assets a property crime are China and South Korea (Brewer, 2008; Carli, 2007).

Social norms

The fact that social norms vary across virtual worlds has been discussed already. Thus, it is not surprising that a number of the cases we identify occurred within EVE Online, a virtual
world where deceit and theft is accepted and encouraged. Regardless of official game rules, players have their own informal enforcement procedures. Even in games such as EVE Online, players may refuse to interact with or find other ways to punish an individual who engages in egregious fraudulent activity, such as placing a bounty on the offender (EVELopedia 2011). This phenomenon helps to explain why Curzon Dax voluntarily left EVE Online after disclosing his investment fraud (Dax, 2009) and why the individual who destroyed the Band Of Brothers alliance had to seek the protection of a rival organization (i.e., an action equivalent to a criminal fleeing to another country to avoid extradition) (Egan, 2009b; Graham, 2009).

To illustrate how social norms may affect perpetrator behavior, we again consider the EIB (EVE Online) and Ginko Financial (Second Life) bank cases. The cases are similar in that they both involve depositors being promised high rates of return but subsequently losing their money when the banks were not able to make good on these promises. Nevertheless, the demonstrated attitudes of the perpetrators are different in these cases. EIB operator Cally (Dentara Rast) produced a video admitting to and even bragging about the scam (Google Video, 2006). Ginko Financial manager “Nicholas Portacarrero” is more circumspect about his role, blaming the bank run on the 2007 Second Life gambling ban. Portacarrero even claims that what he did was not fraud, since he fully disclosed to depositors all the risks associated with the bank (Second Thoughts, 2007). The difference in demonstrated attitudes appears to be due to the fact that EVE Online is considered to be a lawless and unregulated environment, while Second Life tends to be more regulated and the social norms are generally less supportive of fraudulent behaviors.
There are instances where game proprietors’ regulatory initiatives clashed with the prevalent norms of the players. In such cases, modifications in game rules and user agreements can lead to unanticipated consequences. For example, Marc Bragg successfully sued to challenge his suspension from Second Life for alleged auction fraud and his confiscated virtual assets were presumably returned (Reuters, 2007b; Talbot, 2008). More recently, a group of Second Life players filed a class-action lawsuit (Archinaco, 2010) over the recent decision by Linden Lab to open-source its software platform in an effort to become more service-oriented (Lazarus, 2010; Sutter, 2010). The lawsuit alleges that previously developed virtual land with an estimated cash value between $50 and $100 million became worthless at the time of the change in policy. The plaintiffs claim that the game’s proprietor committed fraud by repeatedly emphasizing that users would have indefinite ownership of any property purchased online. These two cases demonstrate that game proprietor actions designed to protect themselves or players can have unintended and possibly severe legal consequences.

**Victim characteristics**

*Motivations and misplaced trust*

As with perpetrators, victims are likely to have strong achievement motivations that may cause them to be susceptible to fraud. Just as gullible real-world investors can be lured into a Ponzi scheme by the promise of large or consistent returns, an achievement-motivated player will be attracted to a virtual investment that promises to increase their asset balance or status in the game. Individuals with a strong relationship motivation are also likely to become virtual world fraud victims because they are likely to trust perpetrators with whom they develop a rapport. This suggests an asymmetry between perpetrator and victim.
characteristics—the manipulative perpetrator’s avatar poses as a character with strong relationship needs (e.g., Curzon Dax) in order to take advantage of a victim or victims with a strong relationship motivation (Egan, 2009c; EVE Online, 2010).

Lack of knowledge

Many players in virtual worlds are susceptible because they lack knowledge of market institutions, regulations, or exploits. Users apparently are likely to place their trust in virtual world characters that have a reputation or a prestigious position. As a consequence, investments in companies which do not have safeguards that would be “standard” protections in the real world (e.g., audited financial statements or internal control reports) are commonplace (Bloomfield & Cho, 2010). This lack of knowledge exists not only in individual players who are victimized, it is often expressed in the poorly designed organizational structures that players construct. As with unregulated banks in the early part of the twentieth century, naivété on the part of organizational officers in virtual world institutions has resulted in poorly designed safeguards and auditing structures that have opened these organization to threats of exploitation (Drain, 2010c; Graham, 2009; Ocampo, 2009).

Carelessness or ignorance of basic computer security features can also leave virtual world players open to fraudulent activity (Bossler & Holt, 2010). A player who gives logon information to others, enters his or her credentials and other sensitive information into a suspicious game website, or responds to phishing e-mails is almost certain to become a fraud victim. Players’ experience with and knowledge of virtual world social norms also has an important influence on their likelihood to become a victim. For example, an experienced EVE
Online player is likely to be aware of the potential for petty theft through griefing activities, and would be less likely to fall victim to these schemes than a novice.

**Individuals versus groups**

The fraud diamond does not make a distinction between fraud committed by single individuals versus groups. However, nearly all the cases of fraud we examined were committed by individual perpetrators. Fraudulent acts performed by individuals are consistent with most cases of real-world occupational fraud or theft of corporate assets. However, this is inconsistent with the more widely studied phenomenon of fraudulent financial reporting, which is usually orchestrated by small teams of top executives or in some cases by middle managers acting under the direction of executives (Albrecht et al., 2009).

We observed only two cases where multiple game players colluded to commit fraud in a virtual world. The first is the “Band of Brothers” case (Egan, 2009b; Graham, 2009). Even though the actions needed to destroy the Band of Brothers from inside the organization were fairly simple, the perpetrator knew he needed a safe haven to retreat to if he were to stay in the game. Therefore, collusion with an interested party was necessary to execute this fraud. Second, Bloomfield and Cho (2010) find evidence suggesting that large investors may have been colluding in the Second Life stock markets to lure smaller investors in and later misappropriate their assets.

The fact that we found so little evidence of fraud perpetrated by groups is somewhat surprising given the culture in games such as EVE Online where alliances are commonly formed to engage in warfare (Egan, 2009b). Members of these groups often engage in petty acts of deception known as griefing where, for example, they might entice a player to join their gang,
steal his assets, and subsequently expel them. Nevertheless, we did not find evidence of more substantial or complex acts of fraud being perpetrated by alliances.

**Observations, implications, and future research**

This review and analysis has important implications for practice and future research. In this section, we describe three of the most significant observations that we made as we analyzed these cases and discuss the real-world implications and future research opportunities associated with each area.

**Design of environments for fraud prevention**

First, observing the constructed environments of virtual worlds provides insights into improving the design of real-world environments for the prevention and detection of fraud. The most salient comparison of environments available from our case analysis is that between EVE Online and Second Life. Despite significant financial scandals in its virtual economy, EVE Online members have resisted regulation of financial institutions such as banks. On the other hand, the proprietors of Second Life have implemented numerous regulations in response to a string of fraudulent events.

The CEO of EVE Online’s EBank maintains that her financial institution can remain viable in this unregulated virtual world through self-regulation and building depositor trust (Egan, 2009a). However, it is uncertain how EVE Online financial institutions can be successful in a game well-known for lawless behavior, where players seem to tolerate financial losses as if they were a cost of doing business (Ten Ton Hammer Network, 2009). Time will tell, but if EBank and
similar institutions can survive and succeed in EVE Online, they could provide a model for
designing financial institutions in emerging economies with lax economic regulation.

An interesting aspect of regulation in Second Life is the legal resistance that the game’s
proprietors have met with when players felt that their virtual property rights were being
threatened (Archinaco, 2010; Talbot, 2008). A real-world parallel to this phenomenon is how
corporate and trade organizations resisted the imposition of internal control requirements in
the periods prior to and following passage of the Sarbanes-Oxley Act (Shapiro & Matson, 2008).
Furthermore, it is not uncommon for personnel within organizations to resist attempts at
improving controls when, for example, they believe a new procedure is too time consuming or
a monitoring technique such as scanning e-mails is perceived as invasive of personal privacy
(Torpey et al., 2010). Resistance to internal control procedures is an important issue that has
received little attention in the academic literature. Virtual world environments provide
researchers with the opportunity to closely observe behavior related to these issues and to
potentially design realistic simulated environments to test when and how changes in
regulations or controls might lead to resistance.

Yee (2006a) and Lehdonvirta (2005) both suggest that individuals might self-select into
virtual worlds that include more or less regulation based on their motivation for playing online
games. It is also possible that executives and rank-and-file employees might self-select into real
world organizations and industries based on the regulatory environment and the tolerance for
bending social norms or regulations. While accountants have studied self-selection into the
public accounting profession (Scofield et al., 2004), we are not aware of research studying self-
selection into positions responsible for financial reporting. Obtaining a better understanding of
what motivates players to participate in certain virtual worlds may help us to understand whether individuals involved in financial reporting scandals self-selected into their companies because of their tolerance for unethical behavior or whether they were later socialized into accepting such behavior after joining these organizations.

**Perpetrator and victim motivations**

An analysis of cases of virtual world fraud allows a more in-depth view into fraud perpetrator and victim motivations than can be afforded through conventional archival and experimental research. It is only rarely that one sees a real-world fraud case that does not involve monetary gain, such as the trading scheme that Jerome Kerviel executed at Société Generale in an attempt to prove himself superior to the bank’s elite traders (Gauthier-Villars & Mollenkamp, 2008). Obtaining a better understanding of non-monetary incentives for fraud can help organizations improve their fraud prevention techniques. Virtual world environments allow one to isolate perpetrator motivations, such as the desire for achievement and need to manipulate others, from the more widely studied motivations of responding to financial pressures or increasing one’s personal wealth.

Real-world evidence often provides little information about victim motivations, as the focus in published documentation such as legal complaints and court decisions is on the perpetrator’s actions. Do investors become fraud victims because of their ignorance of fraud “red flags” and their susceptibility to personable, well-known perpetrators? Or, is their desire for social achievement and increasing personal wealth an equally important factor in their decision to get involved in fraudulent investments? Further knowledge about these issues might help in the design of protective mechanisms for retail investors. As our cases
demonstrate, we can learn about investors’ motivations by studying fraudulent events in virtual worlds.

Yee’s (2000b) large-scale approach to surveying the attitudes of virtual world players holds promise for learning more about victims of virtual world fraud. One could survey these victims to obtain information about what led them to invest in virtual assets that promised high rates of return. Because of the relative anonymity of virtual world players and the ease of approaching players online, it may be easier to survey virtual fraud victims than victims of real-world fraud. In fact, while most perpetrators and victims in real world fraud cases are reluctant to openly discuss their involvement in fraud, our cases demonstrate that both victims and perpetrators openly discuss their experiences, motivations, and tactics associated with fraud. One might question the validity of collecting data from virtual world participants because the assets lost in virtual fraud schemes often have little or no real value, but players generally consider their lost virtual assets to have a substantive value because of the time and effort spent in creating these assets.

**Effects of identity representation on players’ actions**

Finally, one of the interesting common themes we see in the cases we examined is that identity representation in virtual worlds represents an important moderating factor that influences whether and how fraud is undertaken by perpetrators. As is the case with “real-world” fraud, perpetrators often represent themselves in a way that is quite different compared to their true identity. Part of carrying out a fraud often may involve building and embodying a new identity that is aligned with what is needed to manipulate victims into cooperating with the perpetrator.
Because an inherent feature of most virtual worlds is the formation of a unique identity that is generally represented using a pseudonym, an “enhanced” embodied representation, and a synthetic ambiance, perpetrators have a unique and in many respects, ideal forum for assuming whatever persona is needed to engage in fraud. The phenomenon of virtual world embodiment potentially offers useful insights to researchers into how fraud perpetrators adopt alternate identities in order to gain their victims’ confidence. For example, despite avatar Curzon Dax’s reputation in the EVE Online community as an entertainer, financier, and builder of elaborate battleships, the player behind the avatar was actually motivated by his desire to derive pleasure from scamming others (Dax, 2009; Egan, 2009c; EVE Online Forum, 2010).

Significant literature in communications and information systems documents how mediated communication can be used to manage impressions, filter out social cues, and affect the outcomes of communication tasks (e.g., Jarvenpaa & Leidner, 1999; Markus, 1994; Valacich, 1993; Walther, 1996; Walther, et al., 2010). Indeed, some of the research in these areas has focused on deception and the role of media in enabling these acts or, alternatively, the detection of same (Boyle, Kacmar, & George, 2008; Buller & Burgoon, 1996; Carlson & George, 2004; Carlson et al., 2004; George & Robb, 2008; Whitty, 2002). In spite of this, with few exceptions (e.g., George et al., 1995) much of this literature has been overlooked by accounting scholars because these “deception” studies are often not framed in the specific domain of fraud. Given this, much can be learned from this literature about how interpersonal behaviors, attitudes, perceptions, and representations (e.g., embodied representations such as avatars) influence victims. Virtual worlds, which enhance the perpetrator’s ability to assume new identities, represent an ideal “laboratory” for studying these phenomena.
Conclusions

Virtual worlds hold substantial promise for studying the conditions that lead to the committing of fraud and the mechanisms for preventing it from occurring. They are able to provide information on issues where obtaining archival or conventional experimental data is difficult or infeasible. These include examining alternative regulatory and control mechanisms for fraud prevention, in-depth examination of fraud perpetrator and victim characteristics, and consideration of how fraud perpetrators use alternate identities to take advantage of others.

Further, as virtual worlds become part of the workplace, the possibility of fraudulent activity within these new work environments becomes very real. With the exception of the “Band of Brothers” case, all the cases examined in this paper involve fraud committed against individuals outside an organization, however, virtual worlds in the workplace raise the possibility of occupational fraud committed within or against an organization. Reeves & Read (2009, pp. 221-222) suggest this may occur because of unregulated in-game economies or poorly defined in-game rules. We further suggest that workers’ embodiment as avatars may mediate these factors to further contribute to the possibility of virtual occupational fraud. Thus, the need to learn more about virtual world fraud is important as organizations develop virtual worlds as a work environment.

Our analysis of existing cases of reported virtual world fraud and how virtual world fraud is similar to and different from real world fraud represents only a starting point for examining the implications of this phenomenon for practice and research. The experimental methods advocated by Bloomfield and Rennekamp (2009) for studying accounting-related phenomena, such as embedding controlled experiments in a segment of a virtual world and field
experiments where one creates an alternative institution in a virtual world and observes
players’ behavior, are also potentially useful methods for investigating fraud-related issues.
However, these methods are primarily designed to test economic theories. In order to fully
examine the phenomenon of virtual world fraud and its implications for the real world, we
encourage accounting and other researchers to consider the role of the psychological and social
factors that influence fraud and that have been shown to be relevant influences on user
behavior in virtual worlds. Yee (2006b) has shown that gathering information from virtual world
players on user attitudes is fairly easy by embedding surveys in websites or within the game
environment itself. While Yee’s (2006b) research focuses on generalized user characteristics,
such as demographics and player motivations, his approach could easily be adapted to focus on
more specific issues such as fraud.

Despite the promise of archival, experimental, and survey techniques for studying fraud
in virtual worlds and its implication for the real world, we encourage researchers to proceed
with a degree of caution. Attempts to make a simple mapping from a specific virtual world to
real world phenomenon can result in erroneous conclusions. As our comparison of socio-
regulatory classifications in the virtual and real world indicates, actions considered outside
social norms and regulations in the virtual world may be within norms and regulations in the
real world, or vice versa. Williams (2010) recently laid out a framework for mapping virtual to
real world phenomena in communication research. Scholars interested in using virtual worlds
to study fraud are well-advised to follow a similar approach before embarking on the use of this
potentially powerful research tool.
References


<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relationship</td>
<td>Desire to interact with others, willingness to form meaningful relationships that are supportive in nature, willingness to disclose real-life problems and issues.</td>
</tr>
<tr>
<td>Manipulation</td>
<td>Objectify other users and manipulate them for one’s personal gain and satisfaction. Enjoy deceiving, scamming, taunting, and dominating other users.</td>
</tr>
<tr>
<td>Immersion</td>
<td>Enjoy being in a fantasy world and being “someone else.” Enjoy storytelling aspects of virtual world and creating “history” for their avatar.</td>
</tr>
<tr>
<td>Escapism</td>
<td>Use the virtual world to temporarily avoid, forget about, and escape from real-life stress and problems.</td>
</tr>
<tr>
<td>Achievement</td>
<td>Desire to become powerful in the context of the virtual environment through the achievement of goals and accumulation of items that confer power.</td>
</tr>
</tbody>
</table>
Table 2
Case involving behavior regarded as within virtual world social norms and within virtual world regulatory policies

Panel A: Case Descriptions

<table>
<thead>
<tr>
<th>Reference</th>
<th>Case</th>
<th>Estimated loss in US dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egan (2009b), Graham (2009)</td>
<td>Band of Brothers (BOB): A disgruntled director collapsed the BOB alliance and transferred its assets to a rival organization. The director sought the protection of a rival organization. Once assured of a place within the rival, he exploited a corporate governance weakness to steal nearly all the BOB assets and transfer them to the rival. Scheme likened to “Apple dissolving Microsoft.”</td>
<td>$4,600</td>
</tr>
</tbody>
</table>

Panel B: Motivation, capability, and rationalization

<table>
<thead>
<tr>
<th>Case</th>
<th>Motivation</th>
<th>Capability</th>
<th>Rationalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band of Brothers (BOB)</td>
<td>Disgruntled director wanted to take action against his colleagues.</td>
<td>Perpetrator’s director-level status gave him control over the BOB assets.</td>
<td>Lack of respect for others and willing to take actions against his fellow directors once he had the protection of a rival corporation.</td>
</tr>
</tbody>
</table>

Panel C: Opportunities

<table>
<thead>
<tr>
<th>Case</th>
<th>Environmental factors</th>
<th>Victim characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band of Brothers (BOB)</td>
<td>Weak corporate governance structure. EVE Online encourages acts of espionage or theft.</td>
<td>Misplaced trust. Power unevenly distributed in a few top individuals, causing dysfunction among organization members. Rank and file members were apparently unaware of situation.</td>
</tr>
</tbody>
</table>
## Table 3
Cases involving behavior regarded as outside virtual world social norms, but within virtual world regulatory policies

### Panel A: Case Descriptions

<table>
<thead>
<tr>
<th>Reference</th>
<th>Case</th>
<th>Estimated loss in US dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Video (2006), McCarthy (2006), Pollack (2006)</td>
<td><strong>EVE Intergalactic Bank (EIB):</strong> Perpetrator “Cally” had full control over a bank in EVE Online and lured depositors with promises of high rates of return. After operating for several months, he suddenly closed the bank and kept the game currency in his personal account. Cally pretended to be dead in real life with the result that other key bank personnel were slow to react.</td>
<td>$175,000</td>
</tr>
<tr>
<td>Alphaville Herald (2007), Second Thoughts (2007), Hsu (2008), Semuels (2008), Talbot (2008)</td>
<td><strong>Ginko Financial:</strong> Alternate characters Nicholas Portocarrero and Hinoserm Rebus controlled a bank in Second Life that was operated as a Ponzi scheme promising a 40 percent rate of return. When there were insufficient funds being deposited to cover customers’ withdrawals, depositors staged a run on the bank. Bank management responded by offering customers essentially worthless “perpetual bonds,” thus, customers were unable to recover their assets.</td>
<td>$750,000</td>
</tr>
<tr>
<td>Dax (2009), Egan (2009c), Ten Ton Hammer Network (2009), EVE Online Forum (2010)</td>
<td><strong>Curzon Dax:</strong> EVE Online character Curzon Dax started with a large, apparently legitimate investment scheme. He lured investors into a subsequent fraudulent scheme by contacting people on his initial investor list and working out private deals where each person thought that they were going to fund a &quot;shortage&quot; in the IPO in exchange for a highly coveted and expensive customized virtual battleship. Dax dissolved the fraudulent investment scheme upon leaving the game and distributed all the ill-gotten assets to another player.</td>
<td>$45,000</td>
</tr>
<tr>
<td>Bloomfield and Cho (2010)</td>
<td><strong>Second Life CAPEX:</strong> Firms which raised large amounts of capital in the Second Life Capital Exchange (CAPEX) and where ownership was concentrated among a small group of investors paid smaller returns to investors. This evidence suggests that firm CEOs who raised large amounts of capital appropriated invested assets for their own use. The CEOs may have colluded with large investors to take advantage of smaller investors by making it appear as if the firms were an attractive investment option.</td>
<td>unknown</td>
</tr>
<tr>
<td>Reference</td>
<td>Case</td>
<td>Estimated loss in US dollars</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Drain (2010c), Geere (2010), Lau (2010), Polo (2010)</td>
<td>Titans4U: Perpetrator “Bad Bobby” stole all the assets of this large EVE Online investment fund by exploiting weaknesses in the fund’s governance structure. Assets of the fund were under the control of five trustees, however, Bobby convinced the trustees to create more shares under the guise of increasing the number of trustees. In reality, Bobby himself gained access to the new shares and promptly used that power to eject the other trustees from the organization and steal all of its assets.</td>
<td>$45,000</td>
</tr>
</tbody>
</table>
### Table 3 (continued)
Cases involving behavior regarded as outside virtual world social norms, but within virtual world regulatory policies

**Panel B: Motivation, capability, and rationalization**

<table>
<thead>
<tr>
<th>Case</th>
<th>Motivation</th>
<th>Capability</th>
<th>Rationalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVE Intergalactic Bank (EIB)</td>
<td>In-game achievement and manipulation of others.</td>
<td>Knowledge of lack of bank controls and able to exploit this situation.</td>
<td>Lack of respect for others. Perpetrator admitted in a video that he thought scamming people was amusing and explained that he was “not a nice person.”</td>
</tr>
<tr>
<td>Ginko Financial</td>
<td>Financial pressure as bank had recently lost main source of funds and had liabilities to depositors without cash flow to cover these.</td>
<td>Knowledge of lack of bank controls and able to exploit this situation.</td>
<td>Belief that violating rules was acceptable. Perpetrator publicly claimed that he was not doing anything wrong.</td>
</tr>
<tr>
<td>Curzon Dax</td>
<td>Desire to manipulate others and pull off a big scam before leaving the game.</td>
<td>Knowledge of how to devise a complex investment scheme. Ability to manipulate victims since perpetrator was well-known and popular in game.</td>
<td>Lack of respect for others as perpetrator believed that he was intellectually superior to victims.</td>
</tr>
<tr>
<td>Second Life CAPEX</td>
<td>Not clear if greed was a motivation from the start or if CEOs decided to hold on to funds once they started accruing.</td>
<td>Knowledge that lack of internal controls and external regulations provides a means to retain funds in an unregulated market.</td>
<td>May have believed violating rules was acceptable as there were no specific regulations forbidding this type of activity.</td>
</tr>
<tr>
<td>Titans4U</td>
<td>Appears that initial plan was to support game achievement, however, amount of assets stolen has considerable real-world value, suggesting greed was also a factor.</td>
<td>Had a record of successful investment schemes and the knowledge to override what had appeared to be a strong governance structure.</td>
<td>Belief that violating rules (i.e. fraudulent acts) is acceptable in EVE Online, as other players expressed admiration.</td>
</tr>
</tbody>
</table>
### Table 3 (continued)
Cases involving behavior regarded as outside virtual world social norms, but within virtual world regulatory policies

#### Panel C: Opportunities

<table>
<thead>
<tr>
<th>Case</th>
<th>Environmental factors</th>
<th>Victim characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVE Intergalactic Bank (EIB)</td>
<td>No controls over banking in EVE Online and ineffective controls within the bank itself. Confusion resulting from the perpetrator pretending he had been killed in real life.</td>
<td>Achievement motivation as victims expected to receive high rates of interest.</td>
</tr>
<tr>
<td>Ginko Financial</td>
<td>No financial regulation within Second Life at the time. Bank’s operations not transparent to customers. Perpetrator used two alternate avatars to mask identity.</td>
<td>Achievement motivation as victims expected to receive high rates of interest.</td>
</tr>
<tr>
<td>Curzon Dax</td>
<td>Structure of investment company looked as if it had strong controls, but was easily exploited. Social norms in EVE Online allow for fraudulent acts.</td>
<td>Victims thought they were receiving a ship for temporarily funding a “shortage”. Misplaced trust in perpetrator as he was considered a celebrity within the game.</td>
</tr>
<tr>
<td>Second Life CAPEX</td>
<td>Lack of market regulation in Second Life. Difficult to punish CEOs for holding on to investor funds because their identities are not known.</td>
<td>Lack of knowledge about risks of investing in an unregulated market. Not aware than many firms in the market were controlled by a single individual.</td>
</tr>
<tr>
<td>Titans4U</td>
<td>Structure of investment company looked as if it had strong controls, but was easily exploited. Social norms in EVE Online allow for fraudulent acts.</td>
<td>Corporation trustees and other market participants had misplaced trust in perpetrator. Trustees did not understand principles of effective internal control.</td>
</tr>
</tbody>
</table>
Table 4
Cases involving behavior regarded as outside virtual world social norms and outside virtual world regulatory policies

**Panel A: Case Descriptions**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Case</th>
<th>Estimated loss in US dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leyden (2004), Sophos (2004)</td>
<td><strong>Outwar</strong>: A gang of teenagers from the U.K., Canada, and the U.S. distributed the Randex worm to generate clicks and accumulate points in the Outwar role-playing game. Perpetrators were thought to have sold the IP addresses of infected machines to would-be spammers, but it turned out that their motivation for the phishing attack was merely achievement within the game. Two of the perpetrators were tried and given suspended sentences due to their status as minors.</td>
<td>Not known</td>
</tr>
<tr>
<td>Finlayson (2005)</td>
<td><strong>Legend of Mir 3</strong>: This case concerns two Chinese players of the game. The victim lent the perpetrator a “dragon sabre” that he had won during game play. Once in possession of the sword, the perpetrator sold it for the equivalent of $1,080 US. The victim stabbed the perpetrator to death as retaliation for the theft. The fraud victim was sentenced to life in prison for the stabbing.</td>
<td>$1,080</td>
</tr>
<tr>
<td>Knight (2005a), Terdiman (2005)</td>
<td><strong>EverQuest 2</strong>: A group of players exploited a weakness in the game’s code to produce large amounts of game currency and sell it for cash. Game administrators quickly noticed the increase in exchange activity and shut it down. The perpetrators were subsequently ejected from the game. This activity had both real (i.e., exchange of currency for cash) and virtual (i.e., inflation in the game currency) consequences.</td>
<td>$70,000</td>
</tr>
<tr>
<td>Knight (2005b)</td>
<td><strong>Lineage 2</strong>: A Japanese man used an automated program (i.e., a bot) to “beat up and rob” virtual characters in this game. After collecting the defeated players’ virtual goods, the perpetrator exchanged the stolen goods for real cash. The perpetrator was arrested by Japanese police after some of the players who had lost rare virtual goods noticed them for sale on a popular online auction site.</td>
<td>unknown</td>
</tr>
</tbody>
</table>
Table 4 (continued)
Cases involving behavior regarded as outside virtual world social norms and outside virtual world regulatory policies

<table>
<thead>
<tr>
<th>Reference</th>
<th>Case</th>
<th>Estimated loss in US dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sophos (2005)</td>
<td>Korean MMOG hacking: A gang of suspected cyber-thieves used Trojan horses and other techniques to obtain Korean game players’ login credentials. The perpetrators would use the stolen credentials to access and steal victims’ in-game assets. The perpetrators were detected and arrested in part because of Korean officials’ interest in prosecuting crimes related to MMOGs.</td>
<td>unknown</td>
</tr>
<tr>
<td>Anderson (2006), Craig (2006), Walsh (2006), Cheng (2007), Reuters (2007)</td>
<td>Second Life land auction: Second Life participant Marc Bragg bought virtual land below market price. He was able to link to the URL of the auction site before the land went up for actual auction and bid on the virtual property, thus obtaining it for a price well below market value. Game proprietor Linden Lab froze Bragg’s account and confiscated his property. Bragg sued Linden on the grounds that its procedures for settling account disputes were unfair. Linden settled out of court, restoring Bragg’s Second Life account and virtual property rights.</td>
<td>$8,000</td>
</tr>
<tr>
<td>BBC News (2007), Sophos (2007)</td>
<td>Habbo Hotel: A group of Dutch teenagers set up fake websites to lure the game’s players into giving up their login credentials. The perpetrators used the credentials to access the players’ accounts and steal virtual furniture, which they moved into their own Habbo rooms. The oldest (17 years) member of the group was arrested.</td>
<td>$6,000</td>
</tr>
<tr>
<td>Brewer (2008), Welsh (2008)</td>
<td>Final Fantasy XI: The victim shared his password with the perpetrator, under the assumption that the perpetrator would take care of the victim’s virtual items while he was absent. The perpetrator used the password to steal about $3,800 worth of virtual items from the victim. The victim reported the theft to local police, who refused to investigate since no real assets were involved. Appeals to the game’s proprietors for restitution were also unsuccessful, as the victim had violated the game’s TOS by sharing his password and the perpetrator had also violated the TOS by unauthorized use of another player’s account.</td>
<td>$3,800</td>
</tr>
</tbody>
</table>
Table 4 (continued)
Cases involving behavior regarded as outside virtual world social norms and outside virtual world regulatory policies

<table>
<thead>
<tr>
<th>Reference</th>
<th>Case</th>
<th>Estimated loss in US dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barrett (2009)</td>
<td><strong>World of Warcraft:</strong> The perpetrator designed a phishing site that mimics an official World of Warcraft page to steal players’ login credentials. The site offered players a free trail mount, an asset that is difficult to acquire. The stolen credentials were used to loot players’ accounts of virtual goods.</td>
<td>unknown</td>
</tr>
<tr>
<td>BBC News (2009), Egan (2009a), Ocampo (2009)</td>
<td><strong>EBank:</strong> Bank CEO “Ricdic” stole a portion of the bank’s assets by exploiting an internal control feature which gave each bank director absolute control over a portion of the bank’s assets. Ricdic was not punished within the game for taking the virtual currency. Rather, his avatar was banned since the game’s TOS forbids the direct exchange of game currency for real assets. The bank was not put out of business, since it had adopted the fractional reserve system used by modern U.S. banks, which requires the institution to keep a minimum amount of cash on hand.</td>
<td>$6,100</td>
</tr>
<tr>
<td>Ward (2009)</td>
<td><strong>RuneScape:</strong> Perpetrators were alleged to be using phishing e-mails to collect players’ login credentials. As with similar schemes, they used the credentials to steal victims’ virtual assets. The article reported one arrest in Britain, and hinted that other arrests would be likely, as the game’s proprietor is taking steps to investigate and prosecute in-game fraud.</td>
<td>unknown</td>
</tr>
</tbody>
</table>
Panel B: Motivation, capability, and rationalization

<table>
<thead>
<tr>
<th>Case</th>
<th>Motivation</th>
<th>Capability</th>
<th>Rationalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outwar</td>
<td>Generate clicks to build in-game assets for achievement in the game.</td>
<td>Technical knowledge to build and use a worm.</td>
<td>Not known.</td>
</tr>
<tr>
<td>Legend of Mir 3</td>
<td>Convert stolen item to cash.</td>
<td>Ability to manipulate victim since he had earned victim’s trust through prior cooperative play.</td>
<td>Not known.</td>
</tr>
<tr>
<td>EverQuest 2</td>
<td>May have initially been for in-game achievement, but recent introduction of an in-game currency exchange may have provided motivation in the form of real assets.</td>
<td>Technical knowledge of how to exploit a “bug” in the game’s software.</td>
<td>Not known.</td>
</tr>
<tr>
<td>Lineage 2</td>
<td>Convert stolen items to cash.</td>
<td>Technical knowledge to develop a bot that could defeat other players.</td>
<td>Not known.</td>
</tr>
<tr>
<td>Korean MMOG hacking</td>
<td>Convert stolen items to cash.</td>
<td>Technical knowledge to perform large-scale password theft and denial of service attacks</td>
<td>Not known.</td>
</tr>
<tr>
<td>Second Life land auction</td>
<td>Second Life land has substantial value as an in-game asset or when converted to cash, suggesting a motivation of greed.</td>
<td>Technical knowledge to change the ID in a URL for a public auction for one that was not yet listed.</td>
<td>Believed that Linden Lab was at fault for allowing him access to the auction.</td>
</tr>
</tbody>
</table>
Table 4 (continued)
Cases involving behavior regarded as outside virtual world social norms and outside virtual world regulatory policies

<table>
<thead>
<tr>
<th>Case</th>
<th>Motivation</th>
<th>Capability</th>
<th>Rationalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Habbo Hotel</td>
<td>Perpetrators wanted to increase in-game assets. Achievement seems the most likely motivation, however, adding furniture in the game also satisfies immersion and escapism motivations.</td>
<td>Technical knowledge to develop a phishing site which could steal passwords.</td>
<td>Not known.</td>
</tr>
<tr>
<td>Final Fantasy XI</td>
<td>Not known whether motivation was to accumulate virtual assets for achievement or for conversion into real assets.</td>
<td>Ability to manipulate victim as a result of trust developed through mutual game play and acquaintance.</td>
<td>Not known.</td>
</tr>
<tr>
<td>World of Warcraft</td>
<td>Appears that perpetrators wanted to illegally convert virtual goods to cash.</td>
<td>Technical knowledge to design phishing sites indistinguishable from legitimate sites.</td>
<td>Not known.</td>
</tr>
<tr>
<td>EBank</td>
<td>Financial pressure due to mounting family medical bills and other debts in real life.</td>
<td>Knowledge of how to exploit a weakness in the bank’s corporate governance structure.</td>
<td>Theft of virtual assets allowed within EVE Online TOS but not clear how perpetrator rationalized conversion of virtual assets into cash.</td>
</tr>
<tr>
<td>RuneScape</td>
<td>Appears that perpetrators wanted to illegally convert virtual goods to cash.</td>
<td>Technical knowledge to design a phishing site and get access to botnet computers.</td>
<td>Not known.</td>
</tr>
</tbody>
</table>
Table 4 (continued)
Cases involving behavior regarded as outside virtual world social norms and outside virtual world regulatory policies

**Panel C: Opportunities**

<table>
<thead>
<tr>
<th>Case</th>
<th>Environmental factors</th>
<th>Victim characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outwar</td>
<td>At the time, game assets were accumulated by clicking on advertisements.</td>
<td>Lack of knowledge of need for proper antivirus protection.</td>
</tr>
<tr>
<td>Legend of Mir 3</td>
<td>Lack of legal precedent as police did not consider the situation to be a prosecutable crime at the time and sword was not considered a legitimate asset despite perpetrator having sold sword for over $1,000.</td>
<td>Misplaced trust as victim trusted that perpetrator would borrow and return the sword. Later, victim trusted that perpetrator would pay him for sword which was sold.</td>
</tr>
<tr>
<td>EverQuest 2</td>
<td>Programming weakness in game code was exploited by perpetrators. Exploits are against EverQuest social norms, but the perpetrators did this anyway.</td>
<td>Not known.</td>
</tr>
<tr>
<td>Lineage 2</td>
<td>Game monitoring countermeasures did not detect bot activity.</td>
<td>Not known.</td>
</tr>
<tr>
<td>Korean MMOG hacking</td>
<td>Immense popularity of online games in Korea. Proprietors had not fully implemented methods for detecting and preventing fraudulent activity.</td>
<td>Players not aware of the need to protect their login credentials.</td>
</tr>
<tr>
<td>Second Life land auction</td>
<td>Second Life did not properly control access to non-public auctions. Second Life TOS did not explicitly prohibit this type of behavior.</td>
<td>Not known.</td>
</tr>
<tr>
<td>Habbo Hotel</td>
<td>The game’s proprietor allows players to purchase virtual furniture for their “rooms.”</td>
<td>Players not aware of the need to protect their login credentials.</td>
</tr>
<tr>
<td>Final Fantasy XI</td>
<td>No U.S. laws addressing theft of virtual assets. Victim did not monitor his account on a timely basis.</td>
<td>Misplaced trust as victim trusted perpetrator to care for virtual assets while he was unavailable to.</td>
</tr>
<tr>
<td>Game</td>
<td>Motivation and Lack of Knowledge</td>
<td>Trust and Regulation</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>World of Warcraft</td>
<td>There are few widely used or understood mechanisms for distinguishing real game websites from fake ones.</td>
<td>Achievement motivation as victims were enticed by the promise of a new mount, an expensive game item. Lacked knowledge to distinguish a game sponsored site from fake site.</td>
</tr>
<tr>
<td>EBank</td>
<td>Lack of regulation of financial institutions in EVE Online and lack of controls at bank.</td>
<td>Misplaced trust as victim trusted perpetrator and believed that bank controls would function effectively</td>
</tr>
<tr>
<td>RuneScape</td>
<td>Game proprietor had only begun to warn players about and investigate this type of fraud.</td>
<td>Lack of knowledge to distinguish a game sponsored site from fake site or to realize that their computers had been infected by a virus.</td>
</tr>
</tbody>
</table>
Table 5
Cases with different classifications under virtual and real world norms or regulations

<table>
<thead>
<tr>
<th>Reference</th>
<th>Case</th>
<th>Loss in US Dollars</th>
<th>Virtual world classification</th>
<th>Real World Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egan (2009b), Graham (2009)</td>
<td>Band of Brothers</td>
<td>$4,600</td>
<td>Within social norms, within regulatory policies</td>
<td>Outside social norms, within regulatory policies</td>
</tr>
<tr>
<td>Finlayson (2005)</td>
<td>Legend of Mir 3</td>
<td>$1,080</td>
<td>Outside social norms, outside regulatory policies</td>
<td>Outside social norms, within regulatory policies</td>
</tr>
<tr>
<td>Knight (2005a), Terdiman (2005)</td>
<td>EverQuest2</td>
<td>$70,000</td>
<td>Outside social norms, outside regulatory policies</td>
<td>Outside social norms, within regulatory policies</td>
</tr>
<tr>
<td>Knight (2005b)</td>
<td>Lineage 2</td>
<td>unknown</td>
<td>Outside social norms, outside regulatory policies</td>
<td>Outside social norms, within regulatory policies</td>
</tr>
<tr>
<td>Brewer (2008), Welsh (2008)</td>
<td>Final Fantasy XI</td>
<td>$3,800</td>
<td>Outside social norms, outside regulatory policies</td>
<td>Outside social norms, within regulatory policies</td>
</tr>
<tr>
<td>BBC News (2009), Egan (2009a), Ocampo (2009)</td>
<td>EBank</td>
<td>$6,100</td>
<td>Outside social norms, outside regulatory policies</td>
<td>Outside social norms, within regulatory policies</td>
</tr>
</tbody>
</table>
Figure 1. Transaction space and the interactions between actors and their identities.
(adapted from Papagiannidis et al., 2008)
Figure 2. A socio-regulatory model of virtual world fraud.
Figure 3. Virtual fraud framework.

Panel A: The “fraud diamond” (adapted from Wolfe & Hermanson 2004)
Panel B: Opportunities for virtual world fraud

Environmental factors

- Virtual world regulatory policies
  - Programming weaknesses or “bugs”
  - Virtual organization governance and controls
  - Terms of service (TOS)
  - Monitoring player activity
- Real-world regulatory policies
  - Lack of legal precedent concerning virtual assets
  - Authorities’ unwillingness to prosecute when virtual world fraud does not involve a real-world crime
  - Inconsistent rules across jurisdictions concerning virtual assets
- Social norms
  - Informal in-game culture
  - Multiple player identities
  - Player resistance to and litigation against proprietor actions

Victim characteristics

- Achievement or relationship motivations
- Misplaced trust
- Lack of knowledge of:
  - Safeguards over economic activity
  - Corporate governance structures
  - Online security practices
  - Formal and informal game rules
Figure 4.
Comparison of socio-regulatory classifications in the virtual and real world.