Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case

Christine Conradt[1]
Boston University, USA

Abstract

Using the tenets of rational choice theory, routine activities theory, general deterrence theory, social learning theory, and differential reinforcement theory, the Adrian Ghighina case is analyzed to identify causation and motivations of offenders that engage in online auction frauds. The results of this analysis indicate that the most successful prevention strategies will be comprised of multi-faceted approaches that address micro- and macro-level factors including the public education in victimization prevention, increased guardianship in the private sector, reform of traditional law enforcement investigation techniques, increased cooperation between domestic and foreign law enforcement agencies, and heightened public awareness in the apprehension and prosecution of cyber criminals.

Keywords: Adrian Ghighina; cyber crime; online auction fraud; routine activities theory; general deterrence theory; social learning theory; rational choice theory

Introduction

Cyberspace's inherent lack of spatiality and temporality (Choi, 2010) has created new forms of e-commerce that did not previously exist. One of the most prevalent forms of e-commerce is the online auction which allows individuals to buy and sell new and used goods via the Internet to the highest bidder regardless of geographical locations of the buyer and seller. This has revolutionized commerce in a way that could not have happened previously. Prior to online auctions, a seller's pool of potential buyers was limited to the geographic area where the item for sale was kept. Even expanding those boundaries by advertising the item for sale in a newspaper or magazine afforded the seller relatively limited prospects. Online auctions transcend all geographic boundaries not only allowing sellers to locate a multitude of potential buyers genuinely interested in their item (Albert, 2004), but to also take advantage of the increased demand and sell the item at a higher price. Without utilizing the Internet, sellers would not have access to the large pool of buyers, nor would they make as much money per transaction.

With more than 1.3 million transactions taking place daily on online auction sites (Gengler, 2001) the practice of buying and selling online has become firmly woven into the way we now procure personal and commercial goods. It is not surprising, then, that this enterprise has become fraught with criminals hoping to profit from the numerous transactions each day through illegitimate practices. The crime of fraud can be traced back,

[1]Boston University, One Silber Way, Boston, MA 02215, USA. Email: Christine.conradt@gmail.com

according to Drapkin (1989, as cited in Burns, Whitworth & Thompson), to the fourth century B. C. Since then, criminals have found ways to commit new forms of fraud as new opportunities presented themselves. The advent of online auctions has provided offenders unparalleled advantages in locating situations ripe for fraudulent activity, an infinite number of potential victims, anonymity needed to evade capture, and the ability to manipulate a jurisdictional structure designed for traditional crime. The same characteristics that benefit buyers and sellers (the transcendence of geographical borders, the need to use a third party in the transfer of payment, and inherent trust required to accept that an item for sale actually exists and is in the condition stated by the seller), also benefit criminals.

In 2001, the Internet Fraud Complaint Center [IFCC] and Department of Justice [DOJ] launched a massive investigation titled 'Operation Cyber Loss' which exposed over 56,000 U.S. victims and a cumulative loss of over $117 million (Kubic, 2001). One of the several internet fraud schemes investigated during Cyber Loss was online auction fraud. According to the 2009 Internet Crime Report, auction fraud made up 5.7% of the total complaints received (Internet Crime Complaint Center [ICCC], 2009, p. 5). Of all types of online auction fraud, non-delivery of merchandise is the most common according to eBay (Aleem & Antwi-Boasiako, 2011). The ICCC estimates that in 2008, non-delivery of goods and auction fraud constituted 33% and 26% of their annual complaints respectively (Federal Bureau of Investigation [FBI], 2009). These numbers suggest that online auction fraud is one of the most prevalent forms of cyber crime.

Online auction fraud is problematic in more than just the monetary losses suffered by individual victims. Legitimate online auction sites suffer a loss in reputation when criminals use their businesses as a means to commit auction fraud. A negative reputation equates to monetary loss for the company; and according to Nikitkov and Bay (2008), the electronic marketplace in general "will suffer if too many people engage in unethical behavior" (p. 236). There are no simple solutions in combating this problem. Much can be learned, however, by analyzing the causation and motivations of individual offenders that engage in online auction fraud, and then using the knowledge gained as the basis for prevention strategies. This paper analyzes the causational factors and motivations of Adrian Ghighina, who was convicted of multiple incidences of online auction fraud, and proposes prevention strategies based on this case.

The Adrian Ghighina Case

In 2004, Romanian citizen Adrian Ghighina legally entered the United States and proceeded to work as a "money mule" for a ring of cyber criminals located overseas (FBI, 2011). The ring offered high priced items like cars, motorcycles, and Rolex watches for auction on web sites like Craigslist, AutoTrader.com, and eBay, and then never delivered the goods after obtaining the fees from unsuspecting buyers. Ghighina's role was to accept payment from victims via wire transfer or Western Union and then deposit the funds into accounts he opened under a false identity (FBI, 2011). From 2005 to 2009, Ghighina opened fraudulent bank accounts in Arizona, Florida, New York, Illinois, and Washington, DC (FBI, 2011).

Ghighina was indicted in Florida for visa and wire fraud, convicted, and served 21 months in Florida during which time he was indicted before a federal grand jury in Illinois in April 2008 (Department of Justice [DOJ], 2011). In May 2010, Ghighina was indicted by a federal grand jury in Washington, DC on charges of bank fraud, conspiracy, and

money laundering. In June 2011, Adrian Ghighina pleaded guilty to conspiracy and wire fraud charges for his role and was sentenced to 48 months in prison (FBI, 2011). The total monetary loss to victims in this case is estimated at $2.7 Million (McMillan, 2011).

Ghighina's victims reside in several states and the majority of his co-offenders reside overseas in Romania (DOJ, 2011). According to the DOJ (2011), the investigation in the Ghighina case included assistance from the following agencies: the U.S. Attorney's office in the Northern District of Illinois, the U.S. Attorney's office in the District of Columbia, the Criminal Division's Computer Crime and Intellectual Property Section, the Criminal Division's Office of International Affairs, two FBI field offices, U.S. Immigration and Customs Enforcement's Homeland Security, and the Chicago Police Department.

Theoretical Framework

A myriad of well-informed theories exist about crime in general, but only recently have experts begun to study cyber criminals and cyber crime within the context of these theories. By applying universally recognized theories to Adrian Ghighina specifically, we may begin to understand more about the causation and motivations of offenders that engage in online auction fraud. Routine activities theory, social learning theory, general deterrence theory, and rational choice theory all offer explanations as to why Ghighina chose to participate in this type of deviant behavior; and in general, why, online auction fraud is so common.

Although some argue that as a theory Rational Choice falls short in explaining the nature of expressive crimes (Hayward, 2007), economic behavior is generally analyzed using tenets of rational choice (Brown, Esbensen & Geis, 2010). Online auction fraud is a crime committed primarily for economic gain and therefore rational choice applies in the causation and motivations of offenders. Rational choice theory posits that offenders are rational people who weigh the benefits of engaging in a particular criminal behavior against the risks associated with that behavior (McQuade, 2006). With regards to Adrian Ghighina, there were two primary benefits in engaging in online auction fraud. First, fraudulently selling big ticket items netted substantial financial gains for Ghighina and his co-offenders. Because they opted to "sell" only expensive items, one fraudulent auction transaction yielded thousands to tens of thousands of dollars. For Ghighina, the high monetary yield gained from a single transaction was more attractive than the alternative of conducting multiple fraudulent transactions with lower yields. Increasing the number of transactions meant more time spent opening fraudulent bank accounts and a greater number of victims, both of which could increase the perceived risk of being caught.

The second benefit inherent in online auction fraud is the high concentration of potential victims from all over the country. The effort traditional criminals would expend in selecting a target is practically eliminated in cases of online auction fraud. Ghighina's colleagues located victims by simply posting an item for sale online. The very act of posting an item brings potential victims to the offender as the internet has liberated buyers and sellers from the "geographical, cost, and time constraints of the traditional auction business model" (Tan, 2002, p. 348).

While benefits associated with conducting fraudulent auction transactions online are high, the risks are relatively low. Jurisdictional issues, difficulties in obtaining and preserving evidence, a lack of consistency in how laws are applied to cyber crimes by the court, and offender anonymity inhibit apprehension of offenders that offend online (Choi, 2010; Hinduja & Schafer, 2009). Ghighina's victims were geographically situated in the

U.S. while Ghighina's co-offenders were in Romania, and many victims were located in different states than Ghighina himself which allowed the offenders to take advantage of the limitations associated with geographical jurisdictions. Often, law enforcement officials have trouble connecting crimes taking place in multiple jurisdictions; recognizing the scope of victimization; and organizing a unified response in cooperation with other agencies (Hinduja and Schafer, 2009). In addition, many law enforcement agencies do not have well-funded or highly staffed cyber crimes units to pursue cases (Burns, Whitworth & Thompson, 2004). Ghighina moved from state to state to open fraudulent bank accounts, his victims resided in various jurisdictions, and his co-offenders operated from Romania. Collectively, these factors reduced his risk of apprehension, lowering perceived risk.

Another factor that reduces perceived risk is the behavior of victims themselves. Victims of online auction fraud sometimes neglect to report their victimization to police because they fear appearing stupid for being victimized (McQuade, 2006); view themselves as partially responsible for their victimization (Choi, 2010); do not believe they will receive restitution for their losses (Schoepfer & Piquero, 2009; Holtfreter, Piquero & Piquero, 2008); or do not know where to report such victimizations (Schoepfer & Piquero, 2009). No available data could be found regarding the actual reporting behavior of Ghighina's victims, but the general underreporting of such crimes could contribute to an offender's perception of risk. Given the low risk of detection coupled with significant monetary benefits, Ghighina's behavior supports the tenets of rational choice theory.

General deterrence theory posits that rational choice theory holds merit and to deter offenders, punishment must be swift, certain, and severe (McQuade, 2006). Because of the aforementioned reasons, the certainty that cyber criminals like Ghighina and his associates will be caught and face punishment is very low. In fact, Ghighina was able to perpetrate his crimes for four years without apprehension. Punishment cannot be meted out until an offender is caught and convicted; if that does not happen, deterrence theory holds that offenders will not be deterred from committing crimes.

In addition, when offenders of online auction fraud are convicted, punishment is rarely severe. In general, white collar criminals are treated with more leniency than traditional offenders (Friedrichs, 2010). Ghighina received only four years in prison for a crime spree that lasted the same length of time and netted approximately $2.7 Million. In comparison, former Bank of America manager Pamela Cobb who pleaded guilty to bank fraud after stealing nearly $2 Million from bank customers, faces up to a $1 Million fine, 30 years in prison, and may be forced to make restitution (CBS News, 2012). Cobb's crime is similar to Ghighina's in that she fraudulently victimized multiple individuals, pleaded guilty, and netted an amount in the low millions range, but the sanctions she faces are more severe than those received by Ghighina.

Ghighina's punishment was not only lenient in comparison to Cobb's, but it was also not swift. He had already served 21 months of his sentence in Florida before he entered pleas on his Washington, DC and Illinois charges. The cooperation necessary between all of the law enforcement agencies and various U.S. Attorneys' offices impeded the adjudication process making swift punishment nearly impossible. In Ghighina's case, none of the three necessary elements for crime deterrence, according to General Deterrence Theory, were present.

Routine activities theory puts forth that crimes happen when motivated offenders come in contact with suitable targets under a lack of capable guardianship (McQuade,

2006). Three factors, according to Routine Activities Theory, increase victimization risk: exposure to offenders, deviant behavior, and target attractiveness while the presence of guardianship acts as a protective factor (Spano & Frielich, 2009). This theory explains why Ghighina's victims were victimized.

Motivated offenders are drawn to online auctions because of the prevalence of suitable, or attractive, targets (consumers who are willing to bid on, and purchase high, ticket items online regardless of where they are geographically located) and the absence of guardianship (online auction sites allow sellers to create accounts without a thorough background check). In-person auctions require that the item for sale be present. In Ghighina's case, the items sold often did not exist; existence of an item is unverifiable in cyberspace due to the internet's wide geographical reach. The nature of online auctions dictates that a buyer must trust the seller is actually selling the item he/she claims to possess. This type of trust is not necessary at in-person auctions where the item being sold physically exists in the same location as the potential buyer. Those that Ghighina's victims trusted that if they paid the fee, the auctioned item would be delivered. Not all consumers demonstrate this level of trust. Those that do not harbor this level of trust tend to refrain from procuring goods through online auctions. Therefore, victims of Ghighina and other offenders increase their exposure to potential offenders the more frequently they purchase goods through online auction sites.

Pratt, Holtfreter, and Reisig (2010) point out that while Routine Activity Theory suggests that victims engaging in deviant behavior are more likely to be victimized (Karmen, 2010), victims of online auction fraud are typically involved in legitimate, lawful behavior at the time of victimization. Because of this, simply engaging in procuring items from online auction sites is a high-risk behavior compared to individuals that do not buy items via online auctions (Pratt, Holtfreter, & Reisig, 2010). In essence, although it is not unlawful, the behavior of buying items through online auctions is not the norm. According to the National Consumers League, only one-third of adults that engage in online activity have ever purchased an item using an online auction site (National Consumers League, n.d.). Because the majority does not, purchasing through online auctions could be considered behavior inconsistent with the norm. In addition, although cyberspace lacks a geographical location, the "deviant place factor" concept, which "calls attention to exact [high-risk] locations rather than the general lifestyle of particular individuals" (Karmen, 2010, p. 97) could apply in this case, which would support Routine Activities Theory. Ghighina's victims were attractive because of: their willingness to purchase expensive items online, their geographic locations obfuscated jurisdictional issues for law enforcement, and their willingness to use money orders or wire transfers as methods of payment rather than an escrow service.

The single most important protective factor, according to Routine Activities Theory, is capable guardianship. Without capable guardianship to ensure that Ghighina and his co-offenders actually had the item in their possession, victims had no way of knowing that the item did not exist. The auction sites Ghighina and his colleagues used did not have the guardianship required to prevent victimization. Guardianship of online auctions comes in three forms: self-regulation of the online auction houses, consumer protection organizations, and government regulation through the Federal Trade Commission's Bureau of Consumer Protection (Snyder, 2000). While guardianship does happen in all three forms, many of the more effective fraud prevention strategies are cost-prohibitive. In 2002, 90% of all internet crime complaints to the National Internet Fraud Watch

Information Center were attributed to online auction frauds (National Consumers League, 2003), implying that existing forms of guardianship are largely ineffective. Online auction scams originating from Romania, similar to those perpetrated by Ghighina, are prevalent enough that the FBI's Internet Crime Complaint Center [IC3] specifically lists Romanian auction fraud as a specialized category of online auction crimes on its website (Internet Crime Complaint Center, n.d.). While the FBI's attempts to inform the public of these schemes and offer a place to report them is a form of guardianship, not enough is being done to prevent victimization.

Social learning theory expounds upon Edwin Sutherland's Differential Association Theory which puts forth that criminal behavior is learned through close contact with others that behave in a criminal manner (Akers, 2002). According to social learning theory, cyber criminals learn how to commit their crimes from other people through imitation initially, and then reinforcement of the behavior by those individuals (McQuade, 2006; Akers, 2002). At this time there is no documentation to shed light on how Adrian Ghighina became involved with his Romanian co-offenders, but we can examine how Ghighina's criminal behavior was reinforced. As the "mule," Ghighina was instructed how to transfer funds using bank accounts he opened with fraudulent identification to complete the transactions set up by a ring of cyber criminals that operated from his home country of Romania. In Ghighina's case, we can see social learning theory at play in two ways: Ghighina's behavior was learned through intimate contact with other criminals and his behavior was reinforced. Ghighina's home country of Romania is important in this sense. Many of these types of cyber-frauds originate in Romania and of all crimes associated with Romania, online auction fraud is believed by the FBI to be the most common (FBI, 2009; FBI, n.d.). The prevalence of this particular crime suggests that the criminal subculture in Romania perceives online auction fraud as a viable way to exploit the weaknesses inherent in online auctions and illegally obtain money. The ring-leaders teach others how to successfully complete the actions associated with their role. In Ghighina's case, this was obtaining fraudulent identification and opening fraudulent bank accounts. Ghighina was making 20 – 40% per fraudulent transaction he completed (DOJ, 2011); an obvious reward for his behavior. Each time an offender succeeds in perpetrating a scam and collecting money, the experience reinforces his confidence in his abilities to repeat the crime. Because of this, other online auction offenders are not likely to cease their behavior on their own.

Prevention Strategies

Clearly, online auction fraud is a serious problem with far-reaching ramifications. If prevalence is any indication, current methods of preventing and adjudicating this type of crime appear to be ineffective. Prevention strategies must be based in sound theories supported by empirical evidence. From a theoretical perspective, we can examine causation and motivations of offenders like Ghighina to create comprehensive prevention strategies that include micro- and macro-level deterrents, enforcement guidelines, and sanctions.

Protecting consumers from online auction fraud is no simple task, but according to Kyung-shick Choi (2010), we can address prevention by examining the routine activities theory and its three components: the presence of motivated offenders, the presence of suitable targets, and the lack of capable guardianship. To reduce the number of motivated offenders, the crime of online auction fraud must be made to appear less attractive by

either increasing the risk associated with the crime or reducing the reward. Because of the popularity of e-commerce and online auctions, it is safe to assume that the availability of rewards will stay constant. Therefore, we should focus on decreasing the number of motivated offenders by effectively increasing their perception of risk.

Apprehending and prosecuting cyber criminals more consistently is one way to increase a potential offender's perception of risk. Given the number of agencies involved and the length of time it took to identify and capture Adrian Ghighina, it is evident that work must be done in this area. Unfortunately, law enforcement is inadequately equipped to deal with cyber crime in general and online auction fraud specifically due to a variety of reasons (Burns, Whitworth & Thompson, 2004) including underreporting, jurisdictional issues, and the general anonymity of online users. In addition, nearly 47% of law enforcement agencies have no computer crime division and of those that do, 93% are staffed with fewer than six people (Burns, Whitworth & Thompson, 2004). Much of the investigation of internet fraud falls to the Department of Justice and the FBI, specifically the IFCC which has had some success in apprehending cyber criminals. Allocating adequate resources to local law enforcement agencies as well as the FBI and DOJ, and earmarking funds to be used specifically for cyber crime divisions would likely result in more thorough investigations and a higher rate of arrests. These agencies must employ individuals with highly sophisticated computer skills to work closely with the security departments of online auction sites like eBay. Encouraging agencies to collaborate more effectively through the use of computerized systems both domestically and with international law enforcement agencies to track cyber criminals across borders should also be a primary focus.

Reducing the number of suitable targets will also prevent online auction fraud victimization, according to Routine Activities Theory/lifestyles theory (Choi, 2010). According to Chua and Wareham (2008), educating the potential buyer of online auctioned goods offers the greatest benefits in reducing crime because simply apprehending one offender does not deter the infinite number of other offenders. This can be accomplished, in part, by educating the public on how to avoid internet scams and accurately detect fraud (Collins, 1998).Online auction sites are in a position to play an integral role in educating users. Mandating that new users watch a short tutorial video that explains illegal activities and lists best practices of online auction buying prior to setting up a buyer or seller account would increase awareness. In the case of Ghighina, victims could have prevented their victimization had they refused to pay for their items via bank transfer and insisted on using an approved escrow company or other third-party payment system.

Capable guardianship happens in various forms. Digital guardianship implemented by the auctions sites themselves is the first step in reducing fraud. Building digital mechanisms into computer systems that flag suspicious activity and refer the user to a live investigator employed by the site could prevent victimization. The implementation of suspect screening mechanisms that educate auction users about the person they are buying from/selling to as suggested by Chang and Chang (2010) or advanced frameworks with filtering procedures that can accurately identify fraudsters that create seller accounts (Chang and Chang, 2011) are technology-based forms of digital guardianship that exist, but are not frequently used by auction sites. Forcing sellers to provide identification when opening accounts instead of opening accounts anonymously would also increase early fraud detection (Aleem & Antwi-Boasiako, 2011) and therefore, increase perceived risk. Optimal pricing rules and the increased availability of legitimate escrow service providers

as trusted third parties is another way to increase the perceived risk for potential offenders (Hu, Lin, Whinston & Zhang, 2004). Alert systems within the auction house's system could also be of assistance in detecting fraud. For example, offenders like Ghighina often instruct victims to pay for goods via bank or wire transfer instead of using the approved third party payment system. An item that is sold on the site but is not attached to a third party record of payment should generate an alert. This form of guardianship is preferable even though it requires auction sites to carry the burden and cost of employing investigators, which could result in increased costs passed on to the users.

Capable guardianship can also come in the form of government oversight. Government regulation, according to some, carries potentially negative ramifications. Some experts advocate government-imposed regulation on auction sites (Chua & Wareham, 2008; Gavish & Tucci, 2008) like penalties for auction houses that do not maintain complete records of auction bids, authenticate items to be sold, or require proof of identity to create seller accounts (Albert, 2004).Making auction sites financially responsible to provide a site as secure as possible for its customers may act as an incentive to implement fraud detection systems that are available but that auction houses view as an unnecessary expense.

Those opposed to government regulation suggest a multi-pronged solution that includes buyer education, insurance policies, and increased transparency (Gavish & Tucci, 2008). They feel government-imposed regulation and oversight should be considered as a last resort as it almost always has negative consequences, restricting the freedom of online sellers and auction companies in ways that the limited benefits (a minor reduction in crime) do not outweigh the costs and inconvenience. Increased transparency through government regulation and legislation can go too far and violate the privacy of legitimate sellers and buyers as well. Insurance policies, and the cost of that protection, may offset the savings of buying online and deter customers or reduce profit margins which are already typically low for individual sellers. Increasing capable guardianship in the private sector by encouraging individual auction sites to create more thorough methods of qualifying buyers and sellers, and improving banking systems to prevent the opening of fraudulent accounts may pose fewer negative consequences than government regulation. Simply requiring auction sites to post their fraud-deterrent strategies for the potential consumer or voluntarily submit to an approval rating system by a panel of fraud-prevention experts would give consumers more information in making decisions regarding which sites to use. Theoretically, sites that dedicate more resources toward fraud prevention and can therefore provide a safer experience for consumers would receive higher ratings which would then encourage consumer use. Ultimately, the increase in business could potentially offset their costs in providing such protection.

According to deterrence theory, increasing the sanctions associated with these types of crimes should help (McQuade, 2006). While prevention is a more cost-effective approach than judicial action (Albert, 2008), there is a need for reform in how online auction fraud cases are processed. Consistency in the judicial arena with regards to processing and sanctions would more effectively deter potential offenders. Similar types of fraud not committed online tend to receive more severe sanctions than online auction fraud. As posited by differential reinforcement theory, punishments must be equitable and fairly imposed. An increase in capable guardianship, allocating more resources to cyber crime units, and enlisting cooperation from agencies in other countries will increase the certainty of being caught. Encouraging victims to come forward and educating them on how to report victimizations will also increase certainty as more crimes are reported.

Increasing the certainty of being caught by the various means previously discussed will also increase the offender's perceived risk. Rational choice theory supports the notion that increasing offender risk will reduce crime (McQuade, 2006). As capable guardianship is increased through more effective oversight by the auction sites, better awareness and willingness to report fraud by individuals, increased rates of arrests and prosecutions by the criminal justice system, and more severe sanctions put forth by legislation, offenders will be more careful about choosing targets. Fewer targets will exist as public education on fraud prevention increases. These changes will affect offender choices and presumably reduce victimization. For example, fraudulent accounts, like those of Ghighina and his co-offenders, are very often associated with a history of selling high-ticket items (Chiu, Ku, Lie, & Chen, 2011); data mining techniques exist that detect these types of accounts and flag them as suspicious. These forms of guardianship are effective as a means of increasing the certainty of apprehension.

According to social learning theory, breaking up cyber crime rings, particularly in countries where these rings are prevalent, should limit offenders' opportunities to teach others how to commit the crimes successfully. In Ghighina's case, it is unlikely that the ring in Romania will now stop engaging in online auction fraud simply because Ghighina is no longer operating. He will be replaced with another "mule" who will be instructed on how to get away with his role in the crime. Cooperation between domestic and foreign agencies will result in casting a wider net to apprehend these criminals. When foreign agencies work together, the cyber criminal's ability to circumvent law enforcement based on jurisdictional boundaries is reduced. While it is not clear whether Romanian officials assisted in the arrest of Ghighina, Romania's Inspector General of Police publicly stated that Romania's cooperation with International Criminal Police Organization- International Police [INTERPOL] to reduce cross-border crimes is a priority (INTERPOL, 2012). In a collaborative investigation between Romanian Police and the DOJ in 2011, 117 search warrants were executed by Romanian authorities, yielding arrests of more than 100 Romanian individuals suspected of online auction fraud (DOJ, 2011b).

Publicizing the successes of international law enforcement agency cooperative efforts is an important aspect as well. Media campaigns publicizing the global arrests and prosecution of criminals engaging in online auction fraud in countries where rings are prevalent will also reduce the number of new offenders willing to become "mules."

Conclusion

Online auction fraud is one of the most prevalent and problematic cyber crimes today. Its effects reach far beyond the individual victim and impact the public trust in private online auction sites as well as the institution of e-commerce as a whole. Adrian Ghighina is proof that, despite efforts to collaborate with international law enforcement agencies, the criminal justice system is ill-equipped to handle this type of criminal. Traditional perspectives regarding punishment, jurisdiction, investigational techniques, and victimization do not adequately address the complex nature of Ghighina's multilayered fraud and the nature of online auctions as a component of e-commerce.

By studying individual cases like Ghighina's from a theoretical perspective, causation and motivations of offenders can be identified and addressed on a larger scale. Universal prevention strategies, rooted in accepted theories of crime can also be formed. Micro-theories provide insight to the individual motivations of the offender while macro-level

theories provide relevant information regarding the nuances of e-commerce, potential victims, and online auction processes in general. Through the identification of motivations and causation, empirically-based multi-approach prevention strategies can be formed and subsequently tested. Potentially effective prevention strategies include: educating internet users about the safest methods of buying and selling online; increasing the offender's perceived risk of being caught through legislative and law enforcement reform, and media support of cyber crime arrests; exploring private and public sector efforts at creating capable guardianship; increasing sanctions; and promoting better cooperation among domestic and foreign law enforcement agencies. A multi-faceted strategy that addresses micro- and macro-level factors will ultimately be essential in preventing and reducing this type of crime.

References

Akers, R. L. (2002). A Social Learning Theory of Crime. In S. Cote (ed). *Criminological Theories: Bringing the Past to the Future* (pp. 135 - 144). Thousand Oaks, CA: Sage Publications, Inc.

Albert, M. R. (2004). E-Buyer Beware: Why Online Auction Fraud Should Be Regulated. *American Business Law Journal,* 39(4), 576-643.

Aleem, A., & Antwi-Boasiako, A. (2011). Internet auction fraud: The evolving nature of online auctions criminality and the mitigating framework to address the threat. *International Journal of Law, Crime and Justice,* 39(3), 140-160

Burns, R. G., Whitworth, K. H., & Thompson, C. Y. (2004). Assessing Law Enforcement Preparedness to Address Internet Fraud. *Journal of Criminal Justice*, 32(5), 477-493

CBS News. (30 March 2012). Ex-Bank of America manager admits stealing $2 Million from customers. Retrieved on 15th April 2012 from http://www.cbsnews.com/8301-504083_162-57407100-504083/ex-bank-of-america-manager-admits-stealing-$2-million-from-customers/

Chang, W., & Chang, J. (2010). An Online Auction Fraud Screening Mechanism for Choosing Trading Partners.2010 2nd International Conference on Education Technology and Computer. Retrieved on 15th April 2012 from http://ieeexplore.ieee.org.ezproxy.bu.edu/stamp/stamp.jsp?tp=&arnumber=5529945

Chang, W., & Chang, J. (2011). A novel two-phased modeling framework for early fraud detection in online auctions. *Expert Systems with Applications*, *39*(9), 11244 – 11260.

Chiu, C., Ku, Y., Lie, T., & Chen, U. (2011). Internet auction fraud detection using social network analysis and classification tree approaches. *International Journal of Electronic Commerce*, 15(3), 123-147.

Choi, K. (2010). *Risk Factors in Computer-Crime Victimization*. El Paso, TX: LFB Scholarly Publishing LLC

Chua, C. E. H., & Wareham, J. (2008). Parasitism and Internet Auction Fraud: An Exploration. *Information and Organization*, *18*(4), 303 - 333

Collins, S. (10 Feb 1998). Fraud on the Internet: Scams Affecting Consumers. Committee on Governmental Affairs United States Senate. Washington, DC.

Brown, S. E., Esbensen, F., & Geis, G. (2010). *Criminology: Explaining Crime and Its Context (7th ed)*. New Providence, NJ: Matthew Bender & Company, Inc.

Department of Justice. (17 Feb 2011). Romanian Man Pleads Guilty for Role in International Fraud Scheme Involving Online Auction Websites. Retrieved on 15th April 2012 from http://www.justice.gov/opa/pr/2011/February/11-crm-206.html

Department of Justice. (15 July 2011). Organized Romanian Criminal Groups Targeted by DOJ and Romanian Law Enforcement. Retrieved on 15th April 2012 from http://www.justice.gov/opa/pr/2011/July/11-crm-926.html

Federal Bureau of Investigation. (30 June 2009). Online Auction Fraud. Retrieved on 15th April 2012 from http://www.fbi.gov/news/stories/2009/june/auctionfraud_063009

Federal Bureau of Investigation. (29 June 2011). Romanian Man Sentenced to 48 Months in Prison for Role in International Fraud Scheme Involving Online Auction Websites. Retrieved on 15th April 2012 from http://www.fbi.gov/chicago/press-releases/2011/romanian-man-sentenced-to-48-months-in-prison-for-role-in-international-fraud-scheme-involving-online-auction-websites

Friedrichs, D.O. (2010). *Trusted Criminals: White Collar Crime in Contemporary Society (4th ed)*. Belmont, CA: Wadsworth Cengage Learning

Gavish, B., & Tucci, C. L. (2008). Reducing Internet Auction Fraud. *Communications of the Association for Computing Machinery*, *51*(5), 89-97

Gengler, B. (2001). Web Fraud Costs Consumers $117 Million. *Computer Fraud & Security*, 7, p. 5

Hayward, K. (2007). Situational crime prevention and its discontents: Rational Choice Theory versus the "culture of now." *Social Policy & Administration*, *41*(3), 232 – 250.

Hinduja, S., & Schafer, J. A. (2009). US cyber crime units on the world wide web. *Policing: An International Journal of Police Strategies and Management, 32*(9), 278 – 295.

Holtfreter, K., Piquero, N. L., & Piquero, A. R. (2008). And justice for all? Investigators' perceptions of punishment for fraud perpetrators. *Crime, Law and Social Change*, *49*(5), 397 - 412

Hu, X., Lin, Z., Whinston, A. B., & Zhang, H. (2004). Hope or Hype: On the Availability of Escrow Services as Trusted Third Parties in Online Auction Environments. *Information Systems Research*, *15*(3), 236 – 249.

International Criminal Police Organization- International Police [INTERPOL]. (13 Jan 2012).

Visit by Romania's General Inspector of Police to INTERPOL emphasizes role of international law enforcement cooperation. Retrieved on 15th April 2012 from http://www.interpol.int/News-and-media/News-media-releases/2012/PR004

Internet Crime Complaint Center. (2009). 2009 Internet Crime Report. Retrieved on 15th April 2012 from http://vista.bu.edu/webct/RelativeResourceManager/Template/course_documents/metcj610_W02_2009IC3Report.pdf

Internet Crime Complaint Center. (n.d.). Internet Crime Schemes. Retrieved on 15th April 2012 from http://www.ic3.gov/crimeschemes.aspx/#item-2

Karmen, A. (2010). *Crime Victims: An Introduction to Victimology*. Belmont, CA: Cengage Wadsworth Learning

Kubic, T. T. (23 May 2001). Congressional Testimony before the House Committee on the Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection. Retrieved on 15th April 2012 from http://www.fbi.gov/news/testimony/internet-fraud-crime-problems

McQuade, S. (2006). *Understanding and Managing Cyber crime*. Boston, MA: Pearson Education Inc.

McMillan, D. (17 Feb 2011). Romanian Pleads Guilty to Role in $2.7M EBay Scam. *PC World*. Retrieved on 15th April 2012 from http://www.pcworld.com/businesscenter/article/220048/romanian_pleads_guilty_to_role_in_27m_ebay_scam.html

National Consumers League. (2003). 2001 Internet Fraud Statistics. Retrieved on 15th April 2012 from http://www.fraud.org/internet/2001stats.htm

National Consumers League. (n.d.). Online auctions: an in-depth look. Retrieved on 15th April 2012 from http://www.nclnet.org/personal-finance/121-online-auctions/279-online-auctions-an-in-depth-look

Nikitkov, A., & Bay, D. (2008). Online Auction Fraud: Ethical Perspective. *Journal of Business Ethics,* 79, 235-244

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209-215.

Snyder, J. M. (2000). Online auction fraud: are the auction houses doing all they should or could to stop online fraud? *Federal Communications Law Journal*, *52*(2), 453-472.

Spano, R. and Frielich, J.D. (2009). An assessment of the empirical validity and conceptualization of individual level multivariate studies of lifestyle/routine activities theory published from 1995 to 2005. *Journal of Criminal Justice*, *37*(3), 305-314.

Tan, H. S. K. (2002). E-Fraud: Current Trends and International Developments. *Journal of Financial Crime,* 9(4), 347 – 354.