2005

Electronic Commerce Fraud: Towards an Understanding of the Phenomenon

Ian MacInnes
Syracuse University

Damani Musgrave
Syracuse University

Jason Laska
Syracuse University

Electronic Commerce Fraud: Towards an Understanding of the Phenomenon

Ian MacInnes, Damani Musgrave, and Jason Laska
Syracuse University, School of Information Studies
imacinne@syr.edu, dpmusgra@syr.edu jmlaska@syr.edu

Abstract

The objective of this paper is to determine the factors that contribute to electronic commerce fraud. We present a model that identifies five causes: the incentives of criminals, the characteristics of victims, the role of technology, the role of enforcement, and system related factors. The Internet has lowered the barriers to entry for criminal enterprises. Victims are unable to determine which sites are real and which ones are fraudulent and lack of reporting further facilitates this type of crime. The lack of enforcement, resulting from inadequate resources and laws, contributes to the lowering of entry barriers to fraudulent businesses. An analysis of FTC cases shows that most crimes are not technologically sophisticated and that greater awareness and experience with this type of schemes people will avoid being victimized.

Introduction and problem statement

This is an exploratory study that aims to identify the factors that lead to electronic commerce fraud. Criminal activity is a multifaceted phenomenon. A framework that integrates the motivating factors was developed. This study is composed of two parts. The first presents a model that is based on research that scholars have done in areas that are related to electronic commerce fraud. The second analyzes the suits filed by the U.S. Federal Trade Commission to map out the crimes and gain a high level view of the type of crime that are committed on the Internet.

This paper differs from previous contributions in that it is the first to explain the problem of electronic commerce fraud. Existing work on the subject has been primarily descriptive. A second contribution of this paper is that it presents a model that integrates all of the factors that others scholars have identified as causes of crime to explain incidents of fraud in electronic commerce transactions. Third, by using Federal Trade Commission cases filed against perpetrators, the paper presents a map of crimes based on technical and non-technical factors to determine the level of sophistication of these offenses.

Electronic commerce has grown rapidly since the early 1990s. According to a report by the Pew Internet and American Life Project, 65% of Internet users in the U.S. have bought products online [1]. This number is likely to increase as more people become familiar with it and through broadband penetration. In the Christmas 2003 holiday, for example, each of the top five product categories experienced double digit growth, with videos and DVDs showing a 46% increase from the previous year and apparel a 40% increase [2].

Electronic commerce does not come without risks. The new medium has attracted people who engage in fraudulent activities. The Internet Fraud Complaint Center (IFCC) of the Federal Bureau of Investigation (FBI) reports that Internet crime has been increasing since the agency began collecting this type of information. From 2001 to 2002 fraud complaints tripled [3]. Table 1 shows the number of IFCC reported cases of fraud by category and by average dollar amount loss.

Table 1: Amount Lost by Fraud Type for Individuals Reporting Monetary Loss

Type of fraud	Percentage of complaints reporting dollar loss	Average (median) dollar loss per typical complaint
Auction Fraud	87	$320
Non-delivery (mdse and payment)	82	$176
Credit/debit Card Fraud	62	$120
Investment Fraud	75	$570
Business Fraud	75	$220
Confidence Fraud	58	$1,000
Identity Theft	15	$2,000
Check Fraud	56	$1,100
Nigerian Letter Fraud	<1	$3,864
Communications Fraud	36	$174

Source: IFFC, Internet Fraud Complaint Center, Washington, DC, 2003.

In spite of the growing incidents of fraud on the Internet there is little scholarly work on the issue. Most of the papers written about the topic have focused on security related to unauthorized access of a company's servers. Surprisingly, fraud related to transactions that have a presence on the Internet is "low tech." Contrary to what one would expect, people who commit these crimes may not even have sophisticated computer skills. Similarly, while we would expect victims to be naïve or uneducated we find that all types of people have been victims of this type of crime. The purpose of this paper is thus to determine the factors that lead to electronic commerce fraud and provide some recommendations to

minimize it. The research questions that guide this study are:

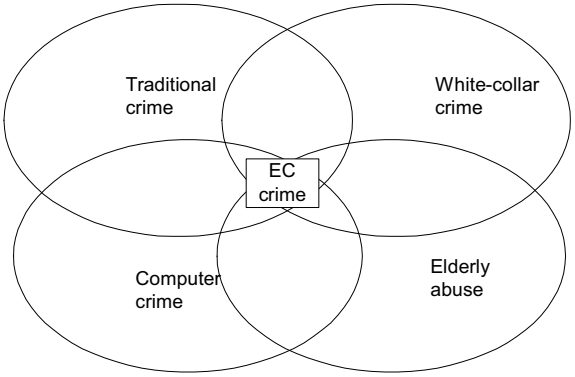
- What are the factors that lead to electronic commerce fraud? Why does it happen?
- In what ways does ICT technology facilitate/inhibit the problem?
- How do victims contribute to the problem?
- How sophisticated are these crimes and the victims they target?

The following sections present the model as well as the scholarly work that has preceded this research and forms the basis of the theoretical framework.

Definitions

Electronic commerce fraud is a relatively new phenomenon but it shares many of the features of traditional crime. Electronic commerce fraud falls at the intersection of several types of crime, as shown in Figure 1.

Figure 1: Antecedents of Electronic Commerce Crime



Like traditional crime, electronic commerce fraud results from a person engaging in an illegal activity that causes harm to someone else. The type of individual, as well as the type of illegal activity and the harm done determine which types of crimes take place.

Electronic commerce fraud falls at the intersection of different types of crime. Some electronic commerce related crimes also listed in the common definitions of white-collar crime include false claims and statements as well as credit and lending institution fraud [4]. Research in this area has recognized that white-collar crime is not the exclusive realm of top executives. There are corporations that set up questionable businesses, forming what Phillip Schrag has called the "commercial underworld"– "small and medium-sized firms that operate on the fringes of the law" [5]. This is a type of business that normally preys on vulnerable people who, through pressure tactics and credit offers, pay for cheap merchandise and home repairs that are delivered unsatisfactorily if at all. High income individuals have also fallen prey to this type of scheme. A common example is to sell a luxury vacation property that does not exist [6].

Electronic commerce can also be associated with elderly abuse. There are many people take advantage of vulnerable groups like the elderly, who often suffer from physical or mental impairments [7]. To a certain extent the level of sophistication of computers has led many more people to become vulnerable in the same way that elderly people are. Technology is moving at a faster pace than society is able to learn and a savvy criminal can take advantage of people's lack of understanding of these means to gain at their expense.

Because electronic commerce fraud takes advantage of technology it is considered an Internet or computer crime. In the book Fighting Computer Crime, Donn Parker describes a crime committed by Mike Hansen, a computer scientist who helped develop a backup system for the wire transfer function of the Federal Reserve. While he worked on the project he interviewed several people and became knowledgeable about the system. He obtained the number of the interoffice settlement account and the telephone authorization code. One day he called the international banking department from a public phone. He wanted to make a $10.2 million dollar transfer. He provided a wrong account number, which the clerk corrected, giving him the correct one, enabling him to successfully transfer the money to Russalmaz, the Soviet government diamond brokerage house. He was later caught with the diamonds in his possession. As Parker describes, many people would not have considered this a computer crime as only a telephone was used. Parker nonetheless argues that this was a computer crime because the perpetrator accessed a computer terminal without authorization and used his computer skills, knowledge, and access to gain the necessary information [8]. There are thus many electronic commerce crimes where the computer was not the instrument to commit the crime but, following Parker's logic one could justify them as computer crimes as well.

More recently the United States Department of Justice lists the following crimes: (1) use of a computer to facilitate a crime; (2) Internet gambling; (3) cyberstalking and harassing speech; (4) unlawful conduct on the Internet; (5) child pornography; and (6) sale of

prescription drugs over the Internet [9]. Electronic commerce thus is unique as it does not fall into any of the categories described above.

For the purpose of this study we define electronic commerce crime in a similar manner to the OECD [10]: it consists of fraudulent and deceptive commercial practices that cause potential or actual harm to consumers by using or taking advantage of their vulnerabilities and of information technologies. These include misrepresentations of material fact, failing to deliver products or services that have been paid for, as well as charging or debiting consumer's financial, telephone, or other accounts without authorization.

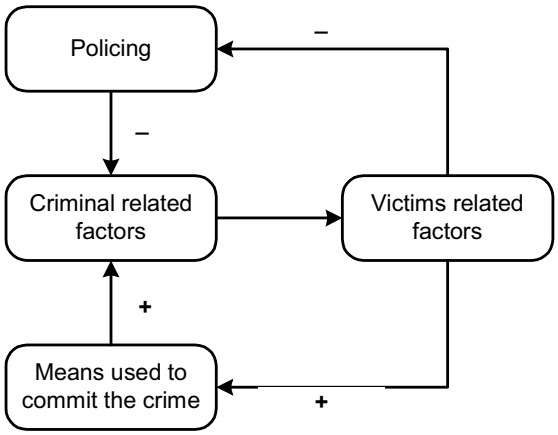
Theoretical context: pieces of a model

Because of the complexity and extent of criminal activity most studies in the area focus on a narrow aspect of the problem. This type of study has provided great insight into the minds of the criminals [11], the vulnerabilities of the victims [7], the weaknesses of law enforcement agencies [5], [12], [13], [14], and the role of instruments that helped to commit the crime[11]. Given the narrow focus of these studies there is rarely an effort to present a systemic view of the problem even tough many of them have it implied. To our knowledge this is the first study that focuses on electronic commerce fraud. It differs from those contributions in that it benefits from prior work to develop a systemic view of the problem where each of the parts is considered to be part of the problem and, if correctly addressed, part of the solution as well.

This study argues that individuals who engage in criminal activities regarding electronic transactions have made economic calculations that are similar to those of a businessperson. They have identified a profitable segment and potential customer base. Using the right technology and outlets they could generate promising income with little risk or adverse consequence. Taking this business model approach to electronic commerce crime, the next five sections present each of the pieces of the model.

The model is composed of four major elements, the perpetrator, the victim, policing that can prevent fraud, and the means used to commit illegal acts. We believe that these four components with their associated factors are related to each other and combined from yet another factor that we call *systemic feedbacks,* which can be positive or negative. Figure 2 presents each of the four components with the associated factors. The following section will explain each of the components in more detail.

Figure 2: Model of Systemic Effects of Electronic Commerce Fraud



The development of the framework benefited from the use of triangulation as a methodology to help determine the factors leading to electronic commerce fraud. We relied on three types of sources. Scholarly work on the subject for traditional and online fraud to help us identify generally accepted factors leading to fraud. Aggregate statistics from the Internet Fraud Complaint Center and the National Consumers League were a third source of data. Federal Trade Commission court cases were a fourth source of data. These involved 301 lawsuits against people or companies that used the Internet to conduct illegal activities from 1994 to 2003.

Each of the three researchers independently analyzed this data. Each developed a framework from the patterns that they were able to identify in the four sources of data. The final framework resulted from the combined analysis of the researchers.

Criminal related factors

A large body of research exists regarding criminals and the factors that lead them to engage in illegal activities. In this section we exclude street and violent crimes as the vast majority of electronic transaction related crimes are done without physical presence and are not violent in nature. The factors that lead these individuals to conduct criminal activities more closely resemble those of white-collar crimes.

In general academic work, scholars have identified four main contexts that can explain why people commit crimes: 1) biological; 2) psychological; 3) sociopsychological; and 4) sociological. Although these have been used to explain violent crime and street crime, some of these factors can also be applied to non-violent criminal activities. Sutherland, the first scholar to identify the problem of white-collar crime, argued that psychological factors do not cause this type of crime: "[t]he criminal behavior of businessmen cannot be explained by… feeblemindedness or emotional instability.

We have no reason to think that General Motors has an inferiority complex or that Aluminum Company of America has a frustration-aggression complex …" Sutherland nonetheless argues that personality factors cannot be entirely ruled out [15]. A personality difference could lead someone to engage in criminal activities while another similarly place executive would reject them [5].

In the book Crime and the Mind Bromberg concludes from analyzing several of his patients that the personality traits of white-collar crime are similar to those of a banker that was convicted of financial manipulation [16]. They are realistic, relatively uncompromising, independent, and unaware of their strong tendency towards recklessness. On a deeper level they have a "certain rigidity of character expressed openly in stubbornness, independence and lack of compromise. Egocentricity and an unconscious feeling of omnipotence shown through [their] character structure." [5].

Considering that most examples of electronic commerce crime are related to a business, however bogus, the individuals behind them have a clear profit motive. As was modeled by Deadman and Pyle [17] criminals, regardless of other drivers, weigh the forces of reward against risk. Moreover, people in general may juxtapose the rewards – the income obtained from carrying out the crime – they might see from a certain decision against the risks involved with enacting upon that decision – the costs of punishment if caught. The criminal expects to be rewarded for his actions, as is evident from the types of electronic commerce crime, such as false product sales, a phony web business, modem hijacking, and false promises.

Because electronic commerce crimes have a technological component it is clear that individuals that that are engaged them it possess some level of technical understanding. Just as a pickpocket will have some degree of silence of foot and speed of hand, so will the cyber criminal have a degree of skill with computers and the Internet. The criminal's ability may be in subterfuge, embedding meta-links in webpages so that searches will pull up unsolicited ads. The ability may come from experience with Ponzi schemes such that the criminal is aware of how to maximize profits while minimizing costs and thus, exploiting customers to the highest potential. A simpler level of ability would fall under incorporating spam emails as another channel to advertise a false product. Many companies who practiced this type of illegal business had other channels before using the Internet. However, the rapid acceptance of email into the mainstream has given these companies a large market of ready viewers.

Victim related factors

While there has been considerable research about criminals less is known about the victims. Studies of crime have generally focused on victims of violent crime and less is known about victims of economic transactions. The limited scholarly work that exists in this area is related to the difficulty of finding the victims. in many cases the victims of organizational crimes do not know that they have been victimized in the first place [5]. They also do not know where to direct complaints when they discover a problem. In this respect Coleman writes: " people who eat food with carcinogenic ingredients, buy short-weighted products, or breathe contaminated air seldom know with any degree of certainty that they have been the victims of a crime. Still, the regulatory agencies receive a large volume of complaints from business, special-interest groups, and the general public. The problem is that those complaints tend to be concentrated in few narrow areas where the harm is most obvious…" [5].

Although he was referring to white-collar crimes, the situation is similar for electronic transactions. There are many products of questionable quality that are sold on the Internet. For example the American Urological Clinic marketed Viagara-like products for $39.45. These included products under the names Alpostaglandin®, The Celldanaphil-pc System, Prosta-Gen®, Väegra®, and Urophil. They claimed that their products had been developed by legitimate medical enterprises and that they had a 68 to 94 percent chance of eliminating impotence [18]. Similarly the American College For Advancement in Medicine promoted online its non-surgical EDTA "chelation therapy" which they claimed was effective in the treatment of atherosclerosis[19]. As can be appreciated from these examples, many of the products that were offered to consumers on the Internet take advantage of the inability of consumers to verify claims. Online transactions thus experience asymmetric information problems, where the seller possesses more information about the object to be exchanged than the buyer. As Nelson [20] explains, many products and services possess "experience" attributes that cannot be evaluated until after purchase when the person has had the opportunity of consuming them. This is particularly true when the price of a good is low enough, the personal cost of doing a quality inspection is not justified [20].

In a traditional physical setting, as described by Ba and Pavlov, potential buyers have the opportunity of getting to know about the quality of a product by "kicking the tires" [21] but in an online setting where buyers never meet, this

is not a real possibility and buyers thus have to rely on written descriptions and in some cases digital photos of the items offered for sale [22]. Under such circumstances sellers may be tempted to make inaccurate or incomplete descriptions of their online product offerings [21].

Individuals that engage in these types of crimes are taking advantage of the asymmetries in information that exist in the sale of these products. They benefit from "practical anonymity," where the customer knows that the company has a name and appears to be a legitimate business but in reality they are unaware of who they really are and the criminal nature of their business. This is further aggravated by additional deceiving practices that they include in the promotion of their products. For example they take advantage of legitimate products and associated them with their own illegitimate ones. SmartScience Laboratories, for example, sold via their website a product called JointFlex, a series of over the counter pain creams claimed to contain glocosamine and chonodroitin sulfate, two legitimate substances, which when applied topically provided more pain relief, but this was not true.

The victims of electronic commerce fraud, contrary to what conventional wisdom would suggest, are not simply poor, uneducated, physically or mentally impaired individuals such as the elderly. The Internet and the trust that people put in websites has enabled some to easily deceive people at all levels of income and education. People's vulnerabilities and concerns provide criminals with a large pool of potential "customers." Some have taken advantage of people's concern for the environment. The OneSource Worldwide Network sold on the Internet and elsewhere the EarthSmart Laundry CD for $80. The plastic disc that was sent to consumers was purportedly filled with "structured water" that cleaned as well as conventional detergents but with much lower environmental impact [23].

They have taken advantage of people's charitable inclinations. The Mentor Network, for example, set up a pyramid scheme where individuals paid $24 to join and another $30 a month thereafter for a minimum of one year. Of that amount they claimed that they sent $7.50 to a bona fide charitable organization that assists needy children in foreign countries while $15 was paid to consumers as recruitment bonuses and promised high monthly returns [24].

They have taken advantage of people's medical concerns by selling all types of products that claim to cure Alzheimer's Disease, and HIV/AIDS [25]. Others claimed to mitigated Attention Deficit Hyperactivity Disorder (ADHD)[26], and chronic or degenerative diseases including multiple sclerosis, emphysema, tuberculosis and spinal cancer [27].

Individual consumers are not the only ones vulnerable to the deceptive practices of companies that have established operations online. Small businesses are also vulnerable market niches for criminal entrepreneurs. They have set up operations that claim to offer additional revenues to small business clients by many products such as selling free-standing kiosks with accepting cash designed to allow customers to access the Internet for a fee. They have given phony references and made unreasonable earnings claims [28]. One offered digital photo sticker vending machines which also claimed unreasonable revenue claims [29].

There are also more sophisticated electronic commerce fraud schemes that use technology in a much more sophisticated manner. In the late 1990s, for example, a pornographic website offered its visitors additional free images if they downloaded a program. When executed the Audiotex Connection program silenced the speakers, disconnected the individual from their ISP and connected them to an international ISP that charged $2 per minute. As well, an Australian company, Internic Technology, developed a copy of the legal InterNIC site where it sold domain names for $250 instead of the $100 charged by InterNIC. They forwarded the application to Network Solutions and kept the difference [30].

In the previous section it was stated that electronic commerce fraud resembled elderly abuse. The trust that many people put on Internet sites and the inability to determine if a product is working has made detection more difficult. Even with full mental abilities, basic human weaknesses have made common individuals and small companies vulnerable to the criminal creations of others.

To add to the complexity and lack of understanding of the problem many of these crimes are unreported. According to Shover: "[a] great deal of white-collar crime goes unreported for the simple season that many of its victims are unaware they have been victimized. Unlike robbery, burglary, and other street crimes, acts of white-collar crime frequently do not stand out in victims' experiences; they characteristically have the look of routine legitimate transactions"[4]. Aside from the difficulty of recognizing that they have been victims of crime they also fail to report because they share part of the responsibility, believing that "they should have been more careful in the first place, victims often feel a sense of embarrassment and shame, and prefer that others not learn what happened to them" [4]. By understanding this type of crimes and being aware of the capabilities of technologies people can begin to recognize and report these crimes.

Policing factors as a deterrent to electronic commerce crimes

Criminals are influenced by a number of factors including reward and risk. Many people juxtapose the

rewards they might see from a certain decision against the risks involved with acting upon that decision. The electronic commerce crimes identified here are clearly subject to this type of calculation. With each crime, whether it is a false product sale, a phony web business, modem hijacking, or a other false promise, there are certain rewards that the criminal can expect to gain from participating in the crime. There is also a risk of being caught.

The law determines whether an activity is illegal or not. White-collar criminals consider law and enforcement is determining the probability of being caught. People weighing whether or not to engage in an illegal activity are likely to have a high probability of being successful. There are several factors that play in their favor.

First, electronic commerce fraud often falls in grey areas of the law. For example, the U.S. Food and Drug Administration does not regulate herbal or natural products, even when they make unsubstantiated health claims. It is thus impossible for people to determine the validity of those claims and it is sometimes debatable whether the company is committing a crime because they face no regulatory oversight.

Second, resources to fight these types of crimes are more limited than those allocated for street and violent crimes. This is because the organizations in charge of enforcement, in the case of electronic commerce it is the Federal Trade Commission, are often regarded as being too bureaucratic and members of Congress consider self-regulation as the first course of action [5]. Most federal agencies can only enforce rules through civil or administrative actions. They can initiate a hearing before an administrative law judge or file a lawsuit in a civil court. If they determine that the case warrants criminal prosecution they can recommend this to the Justice Department, which then makes the final decision [5].

Third, the penalties, which can be effective in deterring economic crime, are often lenient. Of the electronic commerce related cases that the Federal Trade Commission has filed before civil courts and administrative hearings, the vast majority of sanctions involve consumer redress, which entails the return of the funds that were acquired illegitimately. This is generally done by freezing the assets of the offenders. Other sanctions include prohibiting defendants from engaging in this type of illegal activity. In many instances, the case is settled and rarely does anybody face imprisonment.

Another agency, the Federal Drug Administration, is limited in its enforcement powers. For example, it cannot forbid the distribution of a drug just because it has hazardous side effects as there are many drugs that are effective in the treatment of serious diseases that have serious side effects. Similarly the FDA does not test drugs coming to market. The companies that develop and manufacture the products instead do these. The Consumer Product Safety Commission, which is in charge of issuing regulations with the intention of protecting customers from unsafe products, is unable to prevent the sale of dangerous products, the normal course of action is to intervene after injuries or deaths have already occurred [5].

Fourth, government agencies have their budgets approved by Congress, and thus want to be seen as doing their job. The pressure to perform combined with limited resources often causes them to have to decide between persecuting important but time-consuming cases that could potentially alienate powerful corporate interests or pursuing less important claims that will more easily result in a list of convictions that will impress congressional oversight committees [5].

Fifth, the government has generally ignored white-collar crimes in favor of more visible street and violent crimes. Crime control has been at the center of partisan politics because voters seem to care deeply about this issue. As Tonry argues " Critics claim that Republicans and other conservatives cynically heightened public anxieties about crime by stressing it relentlessly in campaigns and legislative chambers and then promised to assuage those anxieties by promoting harsh penalties. There is considerable evidence to support this claim. Heightened political and media attention to crime and drugs issues nearly always precedes increases in the percentages of Americans who name crime or drug abuse as "America's most pressing problem" [31].

The problems that agencies face make electronic commerce fraud fall in the outer limits of the law made which prompted Kedrosky to make an analogy "between cyberspace and the 19th century frontier "boom town" where there is little law and unrestrained capitalism reigns supreme",[32]. Because of the low probability of being caught and then relatively mild punishment that these individuals face, there are great incentives for people to engage in this type of business.

Means related factors

Many of the crimes that are committed using the Internet as a tool could have as easily been done through the phone or mass media outlets. Many of the pyramid schemes and false product offerings that are appearing on the Internet have existed in other media for many years. Ponzi schemes that are becoming so common on the Internet have existed for decades[33]. There are several factors that contribute to the proliferation of these illegal

businesses. Many of them are related to the inherent characteristics of the Internet.

First it is an international network where an increasing number of people are connected. In the United States where most of the crimes identified by the FTC occur, 128 million people, 64% of the population, have Internet access [34]. Compared to traditional media outlets a criminal can access a wider portion of the population at a much reduced price. Even though national television broadcasting reaches a larger segment of the population, these "interactions" correspond to short one-way segments that are available at a relatively high price. Other media outlets are much more fragmented and most target local areas. The Internet, in contrast, has a constant presence at a fraction of the cost. The potential audience is larger than that of a city. There is also access to an audience outside of the United States.

Anonymity and practical anonymity are other factors that contribute to people being defrauded. A growing number of people are relying on the Internet for information. While people are aware that not all the information provided on the Internet is accurate, it is not easy to distinguish legitimate from illegitimate sources. Hittle points out that "[i]ronically, anonymous messages on the Internet are not always false. A study presented at the 1998 Summer Symposium on Accounting Research suggested that anonymous forecasts appearing on the Internet were better predictors of the performance of technology companies than were the traditional analysts' forecasts appearing in the electronic First Call Network" [35]. Without the public being able to discern between truthful or deceiving information, many fall prey to the skills of criminals. It is not surprising that these types of crimes are often called crimes of trust.

In addition to real anonymity there is also something that we call practical anonymity. This refers to the existence of sites that identify themselves with names and may even provide an address. Even though they provide this information it is not possible to determine if that company or organization is legitimate. In the physical world one can visit the location of the business while on the Internet finding out whether or not a company is real will require research that most people do not do. Such research is often not worth the effort when the price of a good is low enough than the personal cost of a quality inspection exceeds it [20].

Software to develop webpages is becoming increasingly easy to use. People can make sophisticated and professional looking webpages, which is facilitated by the ease with which one can obtain an exact copy an entire webpage by simply copying the code [35].

Grazioli and Jarvenpaa created several fake webpages as part of a study. Students were not able to distinguish between legitimate and fake ones. Only eight of the 80 participants in the study successfully identified a fraudulent site[36]. An individual unaware of the types of scams that have been developed on the Internet may not question the validity of a site with a professional look and confidently make a transaction.

The lack of face to face contact is another factor that allows criminals to more easily lull users into believing suspect claims. The creation of virtual communities, and the corresponding decrease in the level of participation in real world communities, may decrease the propensity to question the plausibility of claims and schemes. Among perpetrators of fraud, there appears to be a reduction in impediments to such acts. The ability to deal on a faceless basis, at the click of button, with individuals throughout the world, may facilitate misleading and deceitful acts. This may be the apotheosis of advanced capitalism, where commodities are exchanged in cyberspace, often for the mere purpose of exchange or sometimes for nothing at all [37].

Systemic factors

Each of the four factors described above contribute to electronic commerce fraud on their own, but the combination of all of them further increases the probability of an individual engaging in these types of activities without many risks. The Internet has substantially reduced barriers to entry for criminals. Inherent features of the network, such as anonymity and low costs, make it easy for individuals to defraud others with little effort. Criminals can set up phony websites as well as send thousands of e-mails that market bogus products and services. While the international nature of the network has facilitated entry, the resources for enforcement have reduced as well. The size of the network as well as lack of resources and effective regulatory tools makes it difficult to prosecute cases. Even in those circumstances where criminals have been found and a case against them has been filed, the penalties and sanctions are often limited to confiscation of what the illegally obtained. This is not enough to create an effective deterrent. An analysis of the cases that the FTC has prosecuted shows that the same types of crime are repeated over and over again. There are perhaps a few differences in execution but the basics are same. This indicates that criminals have found profitable enterprises and are able to reestablish businesses that take advantage of the returns that come with lax enforcement, easy to use technology, and naïve consumers that believe messages that are professional in appearance. The victims themselves become another factor in the system that contributes to the incentives to set up this type of operation. The victims' own weaknesses, desperation, and inability to verify the information further lowers barriers for the criminal.

In the framework shown in Figure 2, there are two arrows that come from the victim. One connects to the enforcement box and the other to the means box. If the

victim reports the crime then it can enhance the policing effort and potentially reduce the amount of fraud committed. If the victim does not report the crime then this weakness on the part of the victim becomes another means/tool that the criminal takes advantage of in committing the crime.

Analysis of crimes

The previous section presented a framework that identified the causes that contribute to the development of fraudulent business enterprises. The model helped to answer three of the four research questions established at the beginning of this project. The last question nonetheless remains to be answered. While the model was able to explain the factors that contribute to electronic commerce fraud it is necessary to determine the level of sophistications of these crimes and the technical and non-technical tools that are used in these activities.

At a conference on cybercrime that took place at the Yale Law School in March 2004, we conducted informal interviews to determine if there was data that could be analyzed for this study. Talks with individuals from Interpol, government officials from other countries in charge of cyber crime, and scholars that specialized in the subject commented that there is little data on Internet fraud. The reason they provided for this is because it is difficult to detect and it is commonly not reported [38].

Given the lack of data, the analysis in this section is based on the list of cases that the Federal Trade Commission has filed before administrative and civil courts from 1994 to 2003. These correspond to 301 cases, of which a sample of 75 was selected at random for analysis. The number of cases corresponds to a 10 confidence interval at a 95% confidence level. Each of the cases was scored based on the categories in Table 2.

Once the cases were scored based on this criteria a series of ratios were created to map the cases based on the technical and non-technical features of the crime.

The technical ability of the criminal versus the technical savvy of the victim scores were combined to create the first ratio. These two components are in opposition. For every step that the criminal can take to become more enabled, the victim can take a step to become less of a victim. By creating a ratio, and placing the Technical Ability of the Criminal (A) over the Technical Savvy of the Victim (S), the first electronic commerce fraud ratio (A/S) is created.

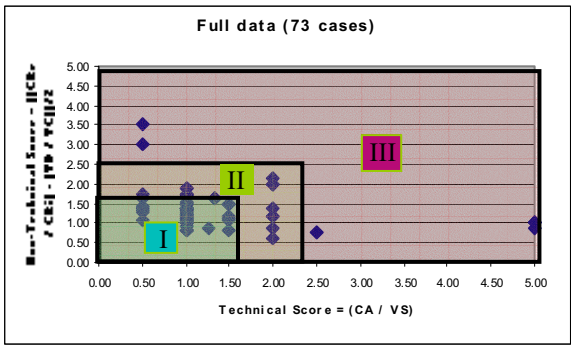
Of the two non-technical scores the first corresponds with the expected reward versus the perceived risk to the criminal. Because these two components are at odds in the cyber criminal's decision-making, they are placed together to form the second force ratio. Expected Reward to the Criminal (Re) is placed over Perceived Risk to the Criminal (Ri) and thus we have (Re/Ri)

The final electronic commerce fraud force ratio is the Victim's Desire for the product or service (D) placed over the Cost (C) that the victim must pay in order to satisfy that need. Thus, the ratio is (D/C). Of all the ratios that were created, the last two pairs are clearly non-technical, while the first pair is clearly technical. In order to graph the technical scores against the non-technical, we take the average of the last two force pairs, thus producing the following:

Technical Coordinate = (A / S)
Non-technical Coordinate = ((Re / Ri) + (D / C)) / 2

By running this calculation on each score, it is possible to present the results in a graph that provides a new way of looking at electronic commerce fraud. 73 cases were scored using the method described above and have are plotted in Figure 3 to provide a graphical representation of the sample of electronic commerce crimes. Please note that the technical component is on the x-axis and the non-technical component is on the y-axis

Figure 3: Categorization of Federal Trade Commission Cases



Several of the cases cluster around the coordinate (1.00, 1.00). This point is important because it represents a balance between each measure. For example, a result of 1.00 in the technical ratio shows that the criminal used a technological method that was not highly sophisticated and the victims could have detected it if they had been more experienced. The criminal might have created a convincing webpage that caused people to send money to a false charity. This is a relatively simple demonstration of technical ability on the part of the criminal, and involves little savvy on the part of the victim. Thus, both parties showed the same level of technical skill.

The same can be seen on the non-technical side. A criminal may believe that he can obtain considerable

revenues through a particular type of fraud. He must then consider the risks. Looking at the graph, while still taking into account the ratios we averaged, it is possible to see that the risks did not substantially outweigh the rewards. On the other side of the average, we also see that the level of desire that victims felt was often close to that of the costs.

Scores at the coordinate (1.00, 1.00) can be considered balanced. In concrete terms, we can say that these are crimes where criminals did not greatly outsmart victims, rewards were not greatly out of line from risks, and victims were not coerced into costly deals without substantial desire on their part.

For the next area that we consider, we move out (0.80 , 0.80) from the central point. This gives us a region from 0.20 to 1.80, the sector I area in Figure 3. We selected this area because it provided a natural break for the data. It is in this region that we find the majority of the crimes and thus the most common infractions. It should be pointed out here that, because we scored on a scale of 1 to 5, there will be no points in the region between 0 and .20.

Within the region of 0.20 through 1.80, we see many different types of crimes. Many of the crimes in this area are not far from balanced. The criminal may have enticed the victim with a pyramid scheme that cost only hundreds of dollars and promised thousands, or used a fancy website to persuade the victim to submit private information. This first level of imbalance demonstrates that the majority of electronic commerce crimes are relatively simple. Criminals do not often show a great deal of technical abilities in the effort of outsmarting victims, nor do they often take substantial risks without commensurate reward. The crimes in this sector are thus not very sophisticated but the criminals have taken some time to make their operation look professional or legitimate. Victims in the crimes represented in this sector do not seem to be technologically savvy and are likely to fall prey to these schemes.

The second region that we will consider is ($\in$.16, $\in$.16) from the central point, and excludes the previous regions. This is the sector II band in Figure 3. This is once again a natural break for the data. Here we see crimes where the balance is further away from normal. An example would be an adult site that collects visitor information and then bills that victim without their knowledge or approval. Here, we see a simple degree of technical ability – the criminal made a website that collects client information using cookies stored on the victim's machine. The victim is not aware of the crime, and thus could not have prevented it at the time. Crimes in this area involve a criminal that has more knowledge of the technology than the victim. The use of technology nonetheless does not mean that they are able to more easily deceive an unsuspecting online customer. In fact the use of the technology itself led to easier detection after the crime had been committed. The reward of billing victims without their knowledge may be great, but the risk is greater. This is because the victims could see the unsolicited charges on their credit and debit card statements and take action. Due to this greater imbalance between the forces, it is difficult though not impossible to succeed with crimes in this band.

The final region encompasses the rest of the graph and corresponds to sector III in Figure 3. Crimes in this area are extremely difficult to execute. They may involve a known company, thus sparking the highest level of trust from victim. Such a crime is extremely rare, as few mainstream companies will engage in obvious criminal activity. Another example of a red band crime is a chain letter scheme where victims sent $50 due to a promise that they would receive $50,000 within three months. Such a crime can be extremely difficult to achieve because it can be difficult to convince victims of such ridiculous claims. Red band crimes are the farthest out of balance and thus, for the criminal, can be both the most dangerous and the most profitable. These crimes can also be more harmful to victims and cause them to lose faith in electronic commerce.

It is thus not surprising that most instances of electronic commerce fraud are more subtle and require little technical sophistication on the part of the criminals.

Conclusion

This paper determined the causes of electronic commerce fraud. We created a model from the scholarly work that preceded this study that identifies five causes of fraud. One of these is a systemic cause that could either aggravate or alleviate the problem. It is clear that the Internet has lowered the barriers to entry for criminal enterprises. At the same time it has provided new tools and the victims are often not able to determine which sites are real and which are fraudulent. Criminals prey on desires and vulnerabilities. The lack of enforcement due to limitations of law and resources as well as lack of reporting, contributes to the lowering of barriers for criminals to enter this type of business. The analysis of cases shows that, for the most part, these crimes are not technologically sophisticated.

Greater technological sophistication leaves a traceable mark. Similarly, the crimes with the greatest profit potential are also difficult to execute because the claims or the tools to deceive are also extreme and not easily believable. This paper supports the view that people are often unable to determine whether a site or an e-mail is legitimate. Governments can potentially help to reduce the instances of E-commerce fraud by raising awareness and encouraging people to report suspicious types of business. Because of the difficulty that people have in identifying these fraudulent sites a web page listing the common characteristics of these schemes with examples can help people avoid falling prey to these fraudulent organizations. Greater enforcement should also contribute

to increase the costs of the crime and thus minimize this type of activity.

References

[1] L. Rainie, Pew Internet and American Life Project, Washington, DC, 2004.

[2] Named in That Tune, in *Brandweek, Vol. 45*, 2004, p. 16.

[3] IFFC, Internet Fraud Complaint Center, Washington, DC, 2003.

[4] N. Shover, White Collar Crime, in *The Handbook of Crime and Punishment* Ed.: M. Tonry, Oxford University Press, New York, NY, 1998, pp. 133-158.

[5] J. W. Coleman, *The Criminal Elite*, St. Martin's Press, New York, NY, 1985.

[6] D. R. Simon, D. S. Eitzen, *Elite Deviance*, Ally and Bacon, Boston, MA, 1982.

[7] R. S. Wolf, K. Pillemer, *Helping Elderly Victims*, Columbia University Press, New York, NY, 1989.

[8] D. M. Lormel, *The Police Chief* 2001, *68*, 66.

[9] Computer Crime and Intellectual Property Section (CCIPS), Department of Justice, http://www.cybercrime.gov/crimes.html.

[10] OECD Guideline for protecting consumers from fraudulent and deceptive commercial practices across borders, OECD, Paris, France, 2003.

[11] D. B. Parker, *Fighting Computer Crime*, Charles Scribner's Sons, New York, NY, 1983.

[12] J. Braithwaite, Restorative Justice, in *Handbook of Crime and Punishment* Ed.: M. Tonry, Oxford University Press, New York, NY, 1998.

[13] L. W. Sherman, American Policing, in *The Handbook of Crime and Punishment* Ed.: M. Tonry, Oxford University Press, New York, NY, 1998.

[14] C. McCoy, Prosecution, in *The Handbook of Crime and Punishment* Ed.: M. Tonry, Oxford University Press, New York, NY, 1998.

[15] E. Sutherland, *White Collar Crime*, Dryden Press, New York, NY, 1949.

[16] W. Bromberg, *Crime and the Mind: A Psychiatric Analysis of Crime and Punishment*, Macmillan, New York, NY, 1965.

[17] D. Deadman, D. Pyle, An Economic Model of Criminal Activity, in *Illicit Activity* Eds.: Z. MacDonald, D. Pyle, Dartmouth Publishing, Burlington, VE, 2000, pp. 15-37.

[18] American Urological Clinic, et al. Civil No. 1:98-CV-2199 (JOS), in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, www, 2003.

[19] American College for Advancement in Medicine, Docket No. C-3882, in *Commission Enforcement Actions Involving the Internet and Online Services*, http://www.ftc.gov/bcp/internet/cases-internet.pdf ed., Federal Trade Commission, 1999.

[20] P. Nelson, *Journal of Political Economy* 1970, *72*, 311-329.

[21] S. Ba, P. A. Pavlou, *MIS Quarterly* 2002, *26*, 243-268.

[22] M. Albert, *American Business Law Journal* 2002, *39*, 575-643.

[23] FTC v. OneSource Woldwide Network, Inc 3-99 CV 1494-L, in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, 1999.

[24] FTC v. The Mentor Network, Inc. Civ No. SACV96-1104 LHM (EEx), in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, 1996.

[25] FTC v. Western Dietary Products Co. (Western District at Seattle) Civil Action No. C01-0818R, in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, 2001.

[26] In the Matter of Natural Organics, Inc., Docket No. 9294, in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, 2000.

[27] FTC v. Western Botanicals Inc., in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, 2001.

[28] FTC v. Hart Marketing Enterprises Ltd. Inc. et al. Civil No. 98-222-CIV-T-23E, in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, 1998.

[29] United States v. PVI, Inc., Civ. No. 98-6935, in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, 1998.

[30] Internic.com, in *Commission Enforcement Actions Involving the Internet and Online Services*, Federal Trade Commission, 1997.

[31] M. Tonry, Crime and Punishment in America, in *The Handbook of Crime and Punishment* Ed.: M. Tonry, Oxford University Press, New York, NY, 1998, pp. 3-27.

[32] P. Kedrosky, in *The Wall Street Journal*, 1998, p. A22.

[33] Charles Ponzi, in *word iQ Encyclopedia*, 2004.

[34] P. Harwood, L. Rainie, Pew Internet and America Life Project, Washington, DC, 2004.

[35] B. D. Hittle, *Federal Communications Law Journal* 2001, *5*, 165-196.

[36] S. Grazioli, S. L. Jaryenpaa, *Ieee Transactions on Systems Man and Cybernetics Part a-Systems and Humans* 2000, *30*, 395-410.

[37] E. McGoun, *Critical Perspectives on Accounting* 1997, *8*, 97-124.

Table 2: Coding System

Technical Factors		
	(Technical) Ability of the Criminal	(Technical) Savvy of the Victim
1	Used an email	Unable to resist an unsophisticated method
2	Used a website	Unable to resist a convincing email or webpage (not a hijacked webpage) or other demonstration of simple web ability
3	Demonstrated strong use of the web (e.g. complex website, site spoofing)	Unable to resist a hijacked webpage or spoofed email address or other demonstration of strong web ability
4	Hijacked software (web pages) or created minor applications	Unable to resist a hidden, but not invisible act of control or misrepresentation
5	Hijacked hardware or created extensive applications	Unable to resist an invisible web tag, embedded subroutine, or other shadowy Subterfuge
Non Technical Factors for the Criminal		
	(Non-Technical) Reward to the Criminal	(Non-Technical) Risk to the Criminal
1	Intangible reward (e.g. pride, bragging rights)	Safe
2	Thousands of dollars	Not very obvious crime
3	Three to tens of thousands of dollars	Mild misrepresentation of products, services, privacy policy, charges, rewards or identities
4	Hundreds of thousands of dollars	Gross misrepresentation or products, services, privacy policy, charges, rewards and/or identities
5	Millions of dollars or more	Extremely transparent - the lie will be discovered quickly (e.g. non-delivery)
Non Technical Factors for the Victim		
	(Non-Technical) Cost to the Victim	(Non-Technical) Desire of the Victim
1	$0-$9	No desire for product
2	$10-$99	Little desire – just trying it out
3	$100-$499	Could benefit from money, service or product
4	$500-$4999 and/or repeated cost of up to $99	Strong feeling of need for money, service or product
5	Over $5000 and/or repeated cost of up to $499	Desperately believe they need the money, service or product