Loyola Consumer Law Review

Volume 14 | Issue 2 Article 5

2002

Remedies for Internet Fraud: Consumers Need All the Help They Can Get

Kristen Weisse

REMEDIES FOR INTERNET FRAUD: Consumers Need All the Help They Can Get

Kristen Weisse*

I. Introduction

Millions of American consumers find themselves victims of Internet fraud every year. Internet fraud affects consumers in two different respects. First, consumers who are victims of fraud suffer a personal financial loss. Second, consumers pay for fraud in their capacity as taxpayers, as it is taxpayer dollars that subsidize government programs designed to remedy and prevent Internet fraud. Attention has finally been turning to the necessity for consumer protection in the wake of a virtual e-commerce explosion.[1]

Consumers are particularly susceptible to Internet fraud because a purchaser cannot bargain with an Internet seller who offers a "take it or leave it" deal.[2] Purchasers agree to unsatisfactory terms, often unknowingly, in order to obtain the merchandise or services they are seeking. In addition, most purchases involve low transaction values.[3] Consumers generally hesitate to spend time, effort, and more money in order to recoup a small monetary loss.

The term "Internet fraud" encompasses all fraudulent acts that are carried out through or made possible by the Internet. Internet fraud plagues consumers in numerous ways, including credit card theft, identity theft, and "cyberjacking," which involves logging on to a website that automatically reroutes the consumer to another site, usually an adult site, and disables the consumer's Internet browser.[4]

---

* J.D. Candidate, May 2002, Loyola University Chicago School of Law; B.A. Political Science, 1995, Loyola University Chicago.

[1] Henry H. Perritt Jr., *Dispute Resolution in Cyberspace: Demand for New Forms of ADR*, 15 OHIO ST. J. ON DISP. RESOL. 675, 697 (2000).

[2] *Id.* at 698.

[3] *Id.* at 699.

[4] Kenneth Sanney, Note, *Cyberjacking, Mousetrapping, and the FTC Act: Are Federal Consumer Protection Laws Helping or Hurting Online Consumers?* 3 VAND. J. ENT. L. & PRAC. 221, 222 (2001).

Any attempt to discuss remedies for all types of Internet fraud would be futile. Rather, this article will focus on remedies available to combat Internet fraud that affects consumers making general merchandise purchases on a day-to-day basis. Part II will detail the types of Internet fraud consumers most commonly encounter. Part III will then examine the currently available remedies, which are, unfortunately, almost nonexistent. Lastly, Part IV will discuss the current debate over Internet regulation and which solution can provide satisfactory answers to consumer problems.

II. Background

In general, "Internet fraud" indicates wrongdoing on the Internet. However, Internet fraud involves much more than wrongdoing. The Federal Trade Commission ("FTC") must prove that conduct rises to the level of fraudulent or deceptive in order to bring a successful action for fraudulent conduct, and recover damages. To prove deceptive practices, for example, the FTC must prove three elements, specifically, that the scheme was: "1) an act likely to mislead; 2) consumers acting reasonably under the circumstances; 3) about a material fact."[5] These elements assist the FTC in differentiating between conduct that is merely dishonest and conduct that is legally reprehensible.

While a variety of deviant acts contain all three of the elements of deception, on a day-to-day basis, consumers primarily fall victim to two types of deceptive practices: sellers who never send merchandise to the purchaser, and sellers who send counterfeit merchandise to the purchaser.[6] Consumers generally encounter these types of fraud in three places: on Internet auction sites, on general merchandise sites, and in their very own e-mail boxes.[7]

---

[5] Kraft, Inc. v. F.T.C., 970 F.2d 311, 314 (7th Cir. 1992) (citing In the Matter of Cliffdale Assocs., Inc., 103 F.T.C. 110, 164-66 (1984)).

[6] *See* Jonathan Rausch, *The Rising Tide of Internet Fraud* (May 2001), *at* http://www.cybercrime.gov/usamay2001_1.htm (last visited Mar. 24, 2002).

[7] *Id.*

A. Internet Auction General Merchandise Complaints

Internet auction fraud is the second most frequently reported type of Internet fraud.[8] This fraud is not limited to any particular type of auction and tends to affect most auction sites.[9] Internet auction fraud may take any number of forms, but generally falls into two categories.[10] First, some sellers misrepresent items, so that a disappointed purchaser receives counterfeit merchandise or merchandise significantly different from the product he ordered.[11] Second, some sellers simply collect payments, and never deliver products.[12] Such incidences of online auction fraud account for approximately ten percent of all Internet fraud.[13]

One of the most popular online auctions is eBay, with over 6.5 million distinct visitors in February 1999 alone.[14] Consumers continue to visit eBay in increasing numbers, attracted by the vast array of goods offered, including collectibles, memorabilia, and electronics.[15] When the buying and selling of merchandise takes place in a non-governmentally regulated space, fraud is sure to abound and flourish, especially because the Internet provides virtual anonymity.

Despite eBay's claim on its website that people are basically good, the following example proves, at a minimum, that auction participants sometimes tell more than "white lies."[16] A Peoria, Illinois

---

[8] Brian Krebs, *ID Theft, Auction Fraud Top FTC Consumer Complaints* (Jan. 23, 2002), *at* http://www.newsbytes.com/news/02/173862.html [hereinafter *Consumer Complaints*]. The most frequently reported type of Internet fraud is ID theft.

[9] *See* Brian Krebs, *FTC Seeks to Stem Online Auction Fraud* (Feb. 14, 2000), *at* http://www.newsbytes.com/news/00/143828.html.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Consumer Complaints*, *supra* note 8.

[14] James M. Snyder, *Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud?* 52 FED. COMM. L. J. 453, 456 (2000).

[15] Verne Kopytoff, *2 Sellers on eBay Arrested/Third Suspect Sought in Online Fraud Case*, S.F. CHRON., Dec. 28, 2000, at B1.

[16] *See* http://www.ebay.com (eBay's website contains a posting reflecting a belief that people are basically good) (last visited Feb. 28, 2002); *see also* Sarah Okeson, *Peorian Logs on to Internet Trouble*, PEORIA J. STAR, June 10, 2001, at A1.

man was "selling" gold and silver coins on eBay.[17] The man did not intend, however, to make good on his eBay dealings.[18] In fact, he had previously "sold" various items over eBay under his own name before eBay terminated his account for misdealings.[19] He later bought out another seller, and "sold" items under his name.[20] This man took over $400,000 from unsuspecting winning bidders who never received anything in return.[21] The prospects for recovery are slim, but victims of the scheme have banded together to make this case public knowledge.[22] Victims have contacted one another, and talked to the press.[23] Some have even visited the seller's home to voice their protests.[24] These victims hope that their experience will serve as a warning to others.[25]

B. Non-Auction general merchandise complaints

While not as prevalent as Internet fraud claims, non-auction general merchandise claims rank among the greatest number of fraud complaints.[26] Non-auction general merchandise complaints, like auction complaints, may be the result of a fraudulent practice, or a mere mistake. Such claims are often similar to auction complaints that involve purchasers who never receive merchandise, or who receive counterfeit merchandise instead of an original. Unlike fraudulent practices that occur in connection with auctions, non-auction fraud may also take the form of an overpriced service, or an untrue or unrealistic delivery date.[27] Non-auction general merchandise

---

[17] Sarah Okeson, *Peorian Logs on to Internet Trouble*, PEORIA J. STAR, June 10, 2001, at A1.

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] Perritt, *supra* note 1, at 6B.

[27] *See Internet Fraud Hearing*, TECH L. J. (1998), *available at* http://www.techlawjournal.com/internet/80210.htm (last visited Mar. 24, 2002).

complaints often stem from one of three places: an unfamiliar website, a familiar website, or an e-mail.[28]

1. Unfamiliar Websites

Consumers have expressed concerns about purchasing from "unfamiliar e-businesses."[29] In fact, one survey conducted by National Technology Readiness found that sixty-seven percent of consumers "are not confident conducting business with a company that can only be reached online."[30] Consumers naturally are skeptical of retailers who can only be reached online, as these retailers may discontinue their websites at any time, or may refuse to respond to consumer complaints. Despite these drawbacks, these sites continue to tempt consumers by offering products or services at extremely inexpensive prices. These sites are able to offer these prices because they most likely do not have, and do not intend to deliver, the goods in accordance with consumer laws, or at all.[31]

One example of an unfamiliar website experience with negative results is the case of a couple that purchased over $86,000 in goods on CyberRebate.com on credit cards, and never received the corresponding rebates.[32] CyberRebate.com offered a variety of electronics and general merchandise goods at high prices.[33] The site attracted consumers because the company would then send consumers rebates of up to one hundred percent.[34] CyberRebate.com filed for Chapter 11 bankruptcy on May 16, 2001, before it paid many consumers their guaranteed rebates.[35] Both "Cyberrebate Rebate Recover Alliance" on MSN.com and "CyberRebate-Support4Lost-

---

[28] Rausch, *supra* note 6.

[29] Mozelle W. Thompson, *The Challenges of Law in Cyberspace – Fostering the Safety and Growth of E-Commerce*, 6 B.U. J. SCI. & TECH. L. 1, 26 (1999).

[30] *Id.*

[31] Okeson, *supra* note 17, at A1.

[32] Paul Cox, *CyberRebate Closure, Credit-Card Firms Leave Thousands of Buyers in the Lurch*, WALL ST. J., June 5, 2001, *available at* 2001 WL-WSJ 2865519.

[33] *Id.*

[34] *Id.*

[35] *Id.*

Rebates" on Yahoo! provide forums where approximately two thousand consumers who lost money on CyberRebate.com can share stories and air their grievances.[36] This case is an example of the temptation of low prices and the fraudulent practices that a consumer may encounter when purchasing inexpensive products on unfamiliar websites.

2. Familiar Websites

Superficially, it may appear to be a case of fraud when a consumer orders an item online from a regional or national department store chain, and the retailer overcharges the consumer, or never delivers the merchandise. Certainly, well-known retailers may be guilty of engaging in deceptive practices, and the FTC has approached retailers with such allegations.[37] On average, large regionally or nationally known retailers gross consistent profits, and maintain consistent customer bases. By engaging in fraudulent or deceptive practices, these sellers stand to lose customers and profits, which they depend on. In determining whether a familiar website is engaging in fraud, it is important to examine the occurrence in light of the legal elements of deception, and most notably the elements of "likely to mislead" and "about a material fact."[38] Because retailers often do not intend to mislead or deceive their customers, most acts do not rise to the level of deception or fraud. A retailer with a significant customer base, both on- and off-line, has it's reputation and goodwill to protect, and is unlikely to be an Internet fraud offender.

When a major retailer does perpetrate fraud, it often takes a subtle and even unrecognizable form. For example, the FTC investigated the Apple Computer Company, not because it sold fake products, or failed to deliver merchandise, but because it charged

---

[36] *Id.*

[37] *E.g.*, Federal Trade Commission, *Pet Express Settles FTC Charges* (Dec. 10, 2001), *at* http://www.ftc.gov/opa/2001/12/petxpress.htm (last visited Mar. 24, 2002); Federal Trade Commission, *Juno Online Services Settles FTC Charges Over Internet Service Advertisements* (May 15, 2001), *at* http://www.ftc.gov/opa/2001/05/juno.htm (last visited Mar. 24, 2002); Federal Trade Commission, *Playgirl.com Operators to Pay $30 Million to Settle FTC Charges* (Nov. 5, 2001), *at* http://www.ftc.gov/opa/2001/11/crescentstlmt.htm (last visited Mar. 24, 2002).

[38] *Kraft, Inc.*, 970 F.2d at 314 (citing *Cliffdale Assocs., Inc.*, 103 F.T.C. at 164-66).

customers for a free service.[39] Between 1992 and 1996, Apple advertised a program called "Apple Assurance," which guaranteed free technical support for all Apple computer owners for the duration of their ownership of the computers.[40] However, in October 1997 Apple began to charge owners of its computers $35.00 for technical support.[41] The FTC took no formal action against Apple, as Apple agreed to discontinue charging customers for its Apple Assurance program, and to reimburse those who already paid for the program.[42] Whether Apple's actions would have risen to the level of fraud or deception is uncertain, but any time an implication of fraud is present, it is most often in the best interest of a large company, such as Apple, to settle the claim and keep its customers satisfied.

3. Unsolicited E-mails

Many consumers receive numerous e-mails from unknown authors in their e-mailboxes every day as a result of "spamming." Spamming occurs when a seller of a product or service sends out a blanket e-mail to numerous e-mail addresses.[43] Many of these e-mails are generally from "sellers" perpetrating fraud.[44]

One example of how spamming can result in fraud involves a seller who sent out a mass e-mail advertising a brand new Playstation

---

[39] Federal Trade Commission, *Apple Computer Settles FTC Charges That its "Apple Assurance" Program Was Deceptive* (Jan. 26, 1999), *at* http://www.ftc.gov/opa/1999/9901/appassu.htm.

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] Thompson, *supra* note 29, at 13.

[44] *Id.* In fact, not only do individuals attempt to "sell" merchandise by way of e-mail, but they may also engage in other schemes. They may indicate that the e-mail is confirmation of an order. The e-mail claims that merchandise was ordered and paid for by the consumer's credit card. If there is a problem with the order, the e-mail directs the consumer to call the phone number provided in the e-mail. The phone number may appear to reach a U.S. location, when in fact, the number is to a far-away location, often an island, which costs $10.00 per minute or more. The perpetrators of this scheme make money on the telephone charges the consumer incurs.

II game console for sale.[45] A 14-year-old boy who had been looking for a Playstation II received the e-mail. [46] The boy jumped at the chance to purchase the game system for such a low price, as he had seen the console selling for much higher prices.[47] In his e-mail, the man claimed that he was a college student who needed the money to pay his rent.[48] The boy and his mother found this to be a viable explanation and wired the $420 purchase price to the man, who promised to send the Playstation II via overnight delivery.[49] The Playstation II never arrived.[50] The boy's mother contacted state police, the state attorney general's office, and Western Union in an attempt to track down the seller.[51] Finally, she turned to local police, but there was little hope of tracking down the seller, and even less likelihood of recovering the $420.[52]

The individuals involved in the Apple Computer mishap were reimbursed and made whole through threatened legal action by the FTC. CyberRebate.com customers and the boy who paid for a Playstation II were not so lucky. If fraudulent practices continue to succeed via the Internet, with no available recourse or remedy for consumers, consumer confidence in the Internet will soon sharply decline.

III. Available Remedies

The remedies available to individual victims of Internet fraud are few. Due to the sheer volume of Internet fraud victims, and the fact that many of these transactions involve small dollar amounts, few legal mechanisms exist to recover that money.

The FTC has brought some of the most successful remedial actions against perpetrators of fraud over the Internet. Many consumer

---

[45] Aimee Green, *As Online Fraud Increases, Local Police Train to Help Victims*, PORTLAND OREGONIAN, July 26, 2001.

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

organizations have a link on their websites to the FTC website, so that a consumer can file a complaint online, by phone, or by mail.[53] In fact, most consumer and government agencies concerned with consumer welfare have some type of posting on their websites that lists ways in which consumers may minimize Internet fraud. Yet, the only suggestion for those who have already been defrauded is to file a complaint with the FTC. While the FTC receives all of these claims, it never acts on many of them.[54] In determining whether to bring a suit, the FTC takes into account various considerations.[55] These considerations include, but are not limited to, whether there is a significant detriment to consumers, whether the behavior constitutes a pattern or practice rather than an isolated incident, and whether a law enforcement action is viable.[56]

In terms of individual actions, a defrauded consumer may institute a traditional legal action against the seller by filing a complaint in court. This remedy is limited, however, to cases in which 1) the contact information of the seller is known, and 2) the seller lives in or has sufficient contacts with the state in which the action is filed so a court in that state would have jurisdiction over the claim.[57] Moreover, the purchaser may need an attorney to file the claim, depending on the amount sought, as an attorney is not required in small claims court. There is, of course, no guarantee that the purchaser will have sufficient evidence to ensure a victory in court. Therefore,

---

[53] *E.g.*,Consumer.gov, *at* http://www.consumer.gov (provides a link to a complaint form, as well as the FTC's address at 600 Pennsylvania Avenue, Northwest, Washington, D.C., 20580) (last visited Feb. 28, 2002); *see also* The National Fraud Information Center, *at* http://www.fraud.org (last visited Feb. 28, 2002); The National Consumers League, *at* http://www.natlconsumersleague.org (last visited Feb. 28, 2002); The Internet Fraud Complaint Center, *at* http://www.ifccfbi.gov (last visited Feb. 28, 2002); The Federal Trade Commission, *at* http://www.ftc.gov (last visited Feb. 28, 2002).

[54] Don Oldenburg, *Getting Help on ID Theft*, WASH. POST, Nov. 7, 2001, at C12.

[55] *See, e.g.*, The American Franchisee Association, *available at* http://www.franchisee.org/government.htm (last visited Feb. 27, 2002). While this site is devoted to franchise actions, it examines the issue of fraudulent or deceptive practices. Whether these practices are committed by a franchisor or an online auction participant or retailer, the elements are the same, as are the case selection criteria.

[56] *Id.*

[57] Jeffrey A. Modisett & Cindy M. Lott, *Cyberlaw and E-Commerce: A State Attorney General's Perspective*, 94 NW. U. L. REV. 643, 649-50 (2000).

whether it is spent on an attorney or filing fees, the purchaser takes a risk by filing an action, if it is even possible due to jurisdictional issues. The purchaser could therefore end up losing more money than the initial loss.

A non-traditional means of resolving a fraud claim is through online dispute resolution ("ODR") mechanisms.[58] There are a variety of ODR sites to choose from.[59] One may choose from public, private, nonprofit, and profit programs.[60] In addition, some sites are free or low-cost, while others operate on a sliding-scale basis depending on the value of the dispute.[61] Other sites saddle consumers with initiation and hourly fees that consumers must pay by credit card.[62] Finally, some sites are automated, while others mix online and offline methods including "mediation, arbitration, and cyberspace juries."[63]

eBay utilizes an online mediation service, SquareTrade, as a mechanism for resolving disputes.[64] SquareTrade provides a forum in which parties may resolve trade disputes.[65] To begin the process, a consumer must file a complaint on SquareTrade.[66] SquareTrade then creates a secure page dedicated to the dispute, and contacts the

---

[58] Lucille M. Ponte, *Throwing Bad Money After Bad: Can Online Dispute Resolution (ODR) Really Deliver the Goods for the Unhappy Internet Shopper?*, 3 TUL. J. TECH. & INTELL. PROP. 55, 60 (2001).

[59] *Id.* at 65-86. Three sites that facilitate the negotiation of monetary settlement disputes are CyberSettle.com, *at* http://www.cybersettle.com (last visited Mar. 24, 2002), clickNsettle.com, *at* http://www.clicknsettle.com (last visited Mar. 24, 2002), and SettleSmart.com, *at* http://www.settlesmart.com (last visited Mar. 24, 2002). Two sites offering mediation services are SquareTrade, *at* http://www.squaretrade.com (last visited Mar. 24, 2002) and Internet Neutral, *at* http://www.internetneutral.com (last visited Mar. 24, 2002). A site offering online arbitration is Resolution Forum, Inc., *at* http://www.resolutionforum.org (last visited Mar. 24, 2002). Finally, one can employ a free modified online jury at iCourthouse.com, *at* http://www.i-courthouse.com (last visited Mar. 24, 2002).

[60] Ponte, *supra* note 58, at 65.

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] *Id.* at 76.

[65] *Id.*

[66] *Id.*

opposing party via e-mail.[67] The opposing party, should he choose to participate, may respond via e-mail, or may post a message on the secure page.[68] This phase of dispute resolution, "Direct Negotiation," does not involve a mediator, but rather presents the opportunity for dialogue between the parties.[69] These communications may clarify a dispute, uncover a misunderstanding, or even lead to a resolution without mediator assistance.[70] According to SquareTrade, parties resolve eighty-five percent of disputes in the Direct Negotiation phase for free.[71] If parties are still in disagreement, however, the parties may request a mediator who, for a twenty-dollar fee, will recommend a solution based on principles of fairness.[72]

A mediator acts only to facilitate negotiation and conciliation between parties.[73] A mediator has no authority to render or enforce a judgment.[74] By definition, mediation is "a method of nonbinding dispute resolution involving a neutral third party who tries to help the disputing parties reach a mutually agreeable solution."[75] The role of the mediator, therefore, is to assist the parties in reaching an agreement that is acceptable to all involved. If mediation is unsuccessful, the parties may then pursue an alternative, enforceable course of action, such as filing a suit in court.

While ODR on its face may seem to be the answer consumers are looking for, three major drawbacks undermine the viability of ODR as a practical remedy for consumers. First, ODR requires the cooperation and participation of the seller. If the seller has vanished, or is impossible to track, such as in the Playstation example, ODR is not an option. Similarly, if the seller has failed to send the merchandise because he has no merchandise, he will be unlikely to cooperate, if he can even be reached. Second, many consumers who

---

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] *See* BLACK'S LAW DICTIONARY 996 (7th ed. 1999) [hereinafter BLACK'S].

[74] *What is Mediation?*, *at* http://www.SquareTrade.com (last visited Mar. 24, 2002).

[75] BLACK'S, *supra* note 73, at 996.

have been defrauded have suffered only a small pecuniary loss.[76] Therefore, the fees necessary to participate in ODR serve as a deterrent and may preclude many from ODR altogether.[77] Likewise, consumers will be wary of paying a fee for dispute resolution when these sites offer no guarantee that the dispute will be successfully settled or enforced.[78] Third, ODR currently stands unregulated by the government.[79] As will be discussed below, government regulation of the Internet continues to be the subject of heated debate, and ODR is no exception.

Neither the traditional filing suit in court, nor the more recent ODR provides a sure-fire remedy to Internet consumers. Jurisdiction may be lacking, attorney's fees and filing fees may exceed the initial loss, and ODR may be daunting and confusing. Some argue that for precisely these reasons, only the creation of a new remedy or cause of action will successfully alleviate Internet fraud.[80]

IV. Internet Regulation: Benefit or Burden?

There is a debate currently raging amongst legal scholars, government agencies, and technology experts. The debate centers on whether regulation of the Internet is necessary, and if so, whether the Internet should be self-regulated or government-regulated. The debate goes even further to ask what restrictions should self- or government-regulation place on the Internet. There is no shortage of opinions, and they cover the entire spectrum of regulation.

A. The Internet Should Not Be Regulated. Period.

Critics at one extreme believe the Internet should not be subject to any limitations or restrictions whatsoever. The *ALA v. Pataki* court characterized the Internet as "one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation, that taken to its most extreme,

---

[76] Ponte, *supra* note 58, at 69.

[77] *Id.*

[78] *Id.*

[79] *Id.* at 65-66.

[80] Sanney, *supra* note 4, at 231.

could paralyze the development of the Internet altogether."[81] One man who supports the *Pataki* court is John Perry Barlow, a political activist who likens his revolt against government regulation of the Internet to the Boston Tea Party.[82] Barlow characterizes his movement and his written work, a Declaration of the Independence of Cyberspace as "dump[ing] some tea in the virtual harbor."[83] The Declaration states in part:

> I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor [sic] do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor [sic] do you know our world. Cyberspace does not lie within your borders. Do not think you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.[84]

Those who take this position find government regulation of the Internet to be not only undesirable, but also dangerous to technological development.[85] They believe that imposing constraints on Internet use will curtail personal freedoms and stifle technological creativity.[86] Proponents of this position fail to recognize, however, that non-regulation is dangerous to consumers, and allows fraudulent practices to breed and multiply. The bottom line is that the damage fraudulent Internet practices have caused, and continue to cause, calls for some type of change. The reality is that this change is most likely to come in the form of regulation.

---

[81] Am. Libraries Ass'n (ALA) v. Pataki, 969 F.Supp. 160, 181 (S.D.N.Y. 1997).

[82] John Perry Barlow, *Cyberspace Declaration of Independence*, *available at* http://hobbes.ncsa.uiuc.edu/sean.declaration.html (last visited Feb. 23, 2002).

[83] *Id.*

[84] *Id.*

[85] *ALA*, 969 F.Supp. at 181.

[86] Barlow, *supra* note 82.

B. Existing Remedies are Sufficient for Righting Internet Wrongs

Other critics agree that the Internet should not be regulated, but for different reasons.[87] Most, if not all, of the offenses committed online are not new crimes.[88] Rather perpetrators of these offenses utilize a new means, the Internet, to commit old crimes.

In a recent Maryland Supreme Court case, a Maryland woman purchased $6,100 worth of dolls over the Internet to add to her Barbie doll collection.[89] The seller, a resident of Georgia, misrepresented the dolls, to the purchaser's disappointment.[90] The state attorney general attempted to prosecute the Georgian seller for fraud in Maryland.[91] Critics found the cross-jurisdictional action to be unnecessary, arguing that sufficient legal remedies for interstate fraud are already in place.[92] Furthermore,

> [c]ourts and consumer protection agencies in the states of the sellers provide other recourses. Internet commerce only changes the medium of communication. It doesn't change the essential nature of interstate . . . transactions. Maryland courts should not be burdened with disgruntled Internet consumers seeking a legal advantage. If there's a pattern of fraud, let the local authorities take action. Otherwise let the buyer use existing remedies.[93]

This position advances a valid point: existing law may be the best remedy for a number of Internet transactions. In fact, the majority of FTC actions have "attacked fraudulent practices that are not unique to the online world; they are schemes or problems that have been

---

[87] *The Dark Side of the Internet*, *at* http://www.du.edu/~soa/ (last visited Mar. 24, 2002).

[88] *Id.*

[89] State v. Cain, 360 Md. 205, 210 (MD 2000).

[90] *Id.*

[91] *Id.* at 209.

[92] *Maryland Prosecutors Wrongly Seek Change in Legal Rules to Benefit Unwary Buyers*, BALT. SUN, June 10, 2000, at 10A.

[93] *Id.*

around for years . . . ."[94] Because incidences of Internet fraud continue to rise, and the Commission can only undertake a limited number of actions, existing law does not appear to be adequate or effective.

The problem, however, may not be the law, but rather law enforcement. Law enforcement capabilities simply are not up to speed with new technology, in terms of both training and equipment.[95] In 1990, the growth of the Internet prompted police departments to employ detectives with technology training to keep track of computer-related crimes.[96] These detectives are crucial to law enforcement. Technology-trained detectives seize and examine computers they believe have been utilized in the commission of a crime, and "pick bits and bytes of information from [the] computers" that may be used as evidence in prosecuting Internet criminals.[97] According to a Washington Senior Deputy District Attorney who prosecutes high-tech crimes, "[w]ithout their assistance, we are looking into a dark room and not seeing anything . . . . They help us turn on the light."[98] Interpreting the technological intricacies of the Internet requires assistance by trained detectives.

Law enforcement authorities are attempting to catch up with cybercrime. In Oregon, for example, the number of certified examiners has increased from six to thirty over a three-year period.[99] In addition, the FBI is currently developing a new division targeting prevention of cybercrime and high-tech crime.[100] While these efforts are commendable, and law enforcement must start somewhere, Internet and computer capabilities continue to grow at an unprecedented rate. In fact, a California Deputy District Attorney warns that "our society is about to feel the impact of the first generation of children who have grown up using computers. The increasing sophistication of hackers suggests that computer crime will soar as members of this new

---

[94] Thompson, *supra* note 29, at 11.

[95] Ryan Frank, *Keyboard Cops on the Hard Drive*, PORTLAND OREGONIAN, December 6, 2001, *available at* 2001 WL 3626150.

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

generation commit more serious offenses."[101] This prospect is not comforting, especially in light of the fact that in December 2001, more than 13,000 of the FBI's computers were too old to run basic software.[102] Bob Dies, assistant director of the Information Resources Division of the FBI confirmed that, of these 13,000 computers, many have low-speed Internet access, do not function with a mouse, and cannot store charts or photographs.[103]

It is possible that existing law would have a greater success rate of eliminating computer crimes if current enforcement mechanisms for Internet deception and fraud were more advanced. Instead of creating new laws, pouring additional resources into law enforcement programs could be the key to eliminating rampant fraud from the online world.

C. Self-Regulation is the Best Recipe for Success

Many people, including the FTC, tout the values of self-regulation, "if effective and grounded in real commitment, especially in rapidly developing industries such as the Internet."[104] While the FTC has broad law enforcement authority that empowers it to pursue criminals on the Internet, the Commission has also played an integral role in promoting self-regulation of commercial practices over the Internet.[105] A chief task of the Commission, for example, has been to help "foster a climate in which Internet self-regulation is both possible and meaningful."[106] To retain customers, merchandisers must control fraud on their sites to the best of their abilities. Consumer confidence

---

[101] Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 470 (1997).

[102] *FBI Agents Ill-Equipped to Predict Terror Acts, available at* http://www.canvasdreams.com/linguist/viewarticle.cfm?articleid=1028 (last visited Feb. 21, 2002); *Mueller Vows to Restore FBI, available at* http://www.newsmax.com/archives/articles/2001/7/30/213352.html (last visited Feb. 21, 2002); *More Feds, Not Fewer, available at* http://www.fcw.com/fcw/articles/2001/1015/mgt-milt-10-15-01.asp (last visited Feb. 21, 2002).

[103] *Id.*

[104] Thompson, *supra* note 29, at 41.

[105] John Graubert & Jill Coleman, *The Impact of Technological Change in the Canada/U.S. Context*, 25 CAN.-U.S. L.J. 275, 286 (1999).

[106] *Id.*

is key; if consumers doubt the credibility or security of a site, they will most likely take their business elsewhere, eventually putting less reputable, less secure sites out of business. This method is essentially the laissez-faire approach to correcting Internet fraud.

While self-regulation appears to be an effective remedy for Internet fraud, it has failed to prove effective in the online auction setting.[107] eBay provides an example of commendable, yet somewhat ineffective regulation. Even though eBay offers numerous safeguards on its website, criminals continue to commit fraudulent acts, turning online auctions into hotbeds for fraud. One safeguard eBay offers is free insurance against fraud that automatically "covers the first $200 of any purchase with a $25 deductible."[108] As a second safety precaution, eBay requires that both buyers and sellers register a credit card number for identification purposes.[109] As a third safeguard, eBay allows, but does not require, bidders to create an escrow account for payment.[110] Unfortunately, opting for an escrow account tacks on an additional one to three percent of the total value of the transaction.[111] As a fourth precaution, eBay provides a "customer feedback feature," which affords a buyer a means of checking the history of the seller.[112] After consumers complete a transaction, they may use this feature to post a message for other eBay users about any aspect of the transaction with the seller, from timeliness of shipment to authenticity of goods.[113]

These protections are theoretically effective, but are not always practically effective. For example, examining a seller's rating appears to be a safeguard against fraud, but "bid shilling" eliminates the accuracy of consumer feedback.[114] The practice of bid shilling involves a co-conspirator of the seller who purports to purchase merchandise, and adds positive feedback to the seller's rating.[115] A related practice is "bid shielding," in which the perpetrator of fraud

---

[107] Snyder, *supra* note 14, at 461-62.

[108] *See* http://www.ebay.com (last visited Mar. 24, 2002).

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] Snyder, *supra* note 14, at 457.

[115] *Id.*

wants to purchase an item.[116] The individual places a bid, and the bid shielder, a co-conspirator, will place a very high bid, which will discourage others from bidding.[117] At the last minute, before the auction ends, the bid shielder withdraws his high bid, allowing the individual to purchase the item at a low price.[118] While some criminals have friends or co-conspirators who engage in this type of activity, these criminals do not need assistance from anyone in order to accomplish their aims.[119] Rather, they can create false identities and multiple email addresses with which they can post their own positive feedback, or drive bidding higher.[120]

While the safeguards eBay has instituted are not fraud-proof, eBay should be commended on its efforts. eBay has become an industry leader, speaking out against fraud and devising new mechanisms to prevent fraudulent and deceptive acts from being committed on its website.[121] eBay has made an affirmative commitment to "effective self-regulation and to the proactive implementation of programs and policies to empower and protect consumers."[122] While eBay has taken the initiative to implement numerous guidelines that seem comprehensive, two concerns remain. First, the majority of the programs in place provide for consumer assistance after fraud has occurred.[123] Post-transaction policies are crucial to dispute resolution, but equal efforts must be directed toward preventing fraudulent and deceptive practices before they occur.[124] Second, the policies and programs eBay offers are not subject to any governmental regulation or enforcement.[125] At the present time, nothing "ensure[s] that these policies are carried out in a fair and

---

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.* at 460.

[122] *Id.*

[123] *Id.* at 461-62.

[124] *Id.* at 462.

[125] *Id.*

consistent manner."[126] Programs without enforcement mechanisms leave consumers with the equivalent of no remedy at all.

Fraudulent schemes on retailer websites logically occur less frequently than on an auction sites due to the fact that a retailer involves only one seller. Auction sites naturally have a greater likelihood of fraudulent transactions as a result of the high number of buyers and sellers. Well-known online retailers have added fraud protections to their websites, primarily in the form of credit card protection, and the protection of private information.[127] Large retailers generally do not provide a great deal of information regarding Internet fraud on their sites, for fear of scaring away customers. Their practices can hardly be self-regulated in accordance with prevailing community and industry standards when the practices are unknown. Unknown procedures coupled with other unknown aspects of Internet technology breed uncertainty among consumers. Uniformity of procedures and resolutions fosters consumer confidence. Government regulation can provide a level of similarity and certainty that retailers cannot.

D. Effective Regulation of the Internet Requires Government Involvement

Regulation without the threat of legally-imposed penalties and punishments simply cannot be effective in deterring criminals from engaging in Internet fraud. Critics of this position believe that "these industry attitudes will discourage development of effective private regimes for protecting mice when they deal with elephants."[128] The National Consumer League ("NCL") stated that while it "applauds self-regulatory efforts" and industry-made codes of conduct that encourage good business practices, self-regulatory schemes are not a substitute for consumer protection laws because of their voluntary nature.[129] Not all businesses participate, and some participants fail to live up to the standards to which they have promised to adhere.[130]

---

[126] *Id.*

[127] *See, e.g.*, http://www.amazon.com/exec/obidos/tg/browse/-/468494/102-4916/16-8486516 (last visited Feb. 23, 2002).

[128] Perritt, *supra* note 1, at 701.

[129] Snyder, *supra* note 14, at 470.

[130] *Id.* at 470-71.

The FTC must take measures to definitively curtail the ever-increasing incidences of Internet fraud. "The Internet is a new medium for conducting business, as well as a new technology, and it is inevitable that it will require some new rules. These rules must be practical and enforceable and make sense for the American economy."[131] To achieve the eradication of Internet fraud and deceptive practices the FTC must set forth "a succinct legal framework to guide the industry in its pursuit of fraud-free transactions." The FTC should outline requirements that all online auction houses and retailers must follow in order to ensure against liability for fraud.[132]

While some critics continue to support the "hands-off" libertarian philosophy, a more compelling argument takes into account the need for some type of regulation.[133] In fact, supporters of regulation argue that "cyberspace already is becoming a highly regulable space – not because of government, but because of the architecture of the Internet as it becomes more predominantly a technology of commerce."[134] State attorneys general bear the burden of devising these much-needed laws, which must strike a delicate balance between affording consumers protection and allowing the Internet enough space to grow.[135] Attorneys general have an important job to do, and that job requires investigating and eliminating fraud, so that the economy may flourish in an environment that is light on regulation and heavy on consumer protection.[136] "As history has shown, commercial abuse often results in regulation, or attempted regulation, of the activity."[137] The Internet is no exception to this historical recurrence. Fraud threatens commercial transactions over the Internet on a daily basis, which is precisely the reason why government agencies and lawmakers are attempting, through some

---

[131] Modisett, *supra* note 57, at 646.

[132] Snyder, *supra* note 14, at 471.

[133] Modisett, *supra* note 57, at 644.

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] Mary Kay Finn et al., *Policies Underlying Congressional Approval of Criminal and Civil Immunity for Interactive Computer Service Providers Under Provisions of the Communications Decency Act of 1996 – Should E-buyers Beware?*, 31 U. TOL. L. REV. 347, 347 (2000).

form of regulation, to provide an accessible, effective remedy for consumers who are victims of unscrupulous fraudulent schemes perpetrated over the Internet.

V. Conclusion

Current remedies for Internet fraud are, for all practical purposes, non-existent. As the Internet becomes a greater part of the daily lives of all Americans, something must be done to curtail online fraud. Ideal government-regulation would secure rights for consumers that are supported by individually accessible remedies. However, an enormous hurdle stands in the way of regulation: the speed at which technology continues to advance. Lawmakers are behind. Law enforcement agencies are behind. Is it possible to not only catch up, but to surpass technology? Is it possible to predict where technology will go, and to beat criminals to the punch? In a frenzy to keep pace with the Internet, will law enforcement agencies fail to weigh the costs and benefits of various means of regulation? Rights and remedies that are imposed in a rush could be more dangerous than no regulation at all. Lawmakers must take action on behalf of consumers, but they must tread lightly.

***