PROSECUTING THE INTERNET FRAUD CASE WITHOUT GOING BROKE

Patrick E. Corbett

ABSTRACT

This Article contends that viable Internet fraud cases are not prosecuted as consistently as other Internet-related crimes. One reason involves the financial cost of bringing these types of cases to court. In general, Internet fraud cases involve multiple victims who have incurred only a small financial loss. Typically, the victims are from all over the United States and beyond. Hence, prosecuting the fraud case to the fullest extent involves use of witnesses from outside of the jurisdiction of the prosecuting authority. The cost of housing these witnesses and transporting them to the court where the crime is being prosecuted often exceeds the budget available for such an expense. Consequently, many prosecutors decline prosecution rather than incur the expense associated with a full prosecution. This Article explores various approaches to reduce the cost of prosecuting these crimes in order to ensure that Internet fraud cases are prosecuted rather than declined.

* Professor, Criminal Law and Procedure, Thomas M. Cooley Law School, Lansing, Michigan. This paper was commissioned by funds from the National Center for Justice and the Rule of Law at the University of Mississippi School of Law (National Center), which is supported by a grant from the Office of Justice Programs at the United States Department of Justice. The contents of this paper were presented at an April 2006 conference entitled “Prosecutorial Responses to Internet Victimization” held at the University of Mississippi School of Law in Oxford, Mississippi, and hosted by the National Center and the National Association of Attorneys General. Thanks to Tom Clancy, Director of the National Center, for the opportunity to write on the subject, and to Cooley Law School student, Lisa Esser, and Cooley Law School librarian, Tim Innes, for their research assistance.
I. INTRODUCTION

A. A Hypothetical Internet Fraud Case

Over the course of two months, investigators for the Attorney General’s Office for the State of Chaos received fifteen complaints from consumers against a company by the name of Bargains Galore. Further investigation revealed that Bargains Galore used a post office box located in Cooley City, Chaos.

The consumer complaints alleged that Bargains Galore offered computer game packages for sale through Internet auction site eGads. After the auction concluded, the winning bidders were notified via email that they had won the computer game that had been bid upon. Winning bidders sent payment—typically between $150.00 and $250.00—through the U.S. mail or through an online payment service. According to the complainants, either no computer game was received or they received a dated game that was of no value to the complainant. The complainants advised they attempted to contact Bargains Galore on several occasions. On a few occasions, complainants were actually able to talk with a person; on these occasions, the complainant was assured that the computer game would arrive soon.

Of the original fifteen complainants, only one resided in the State of Chaos. The Chaos complainant lost $250.00 in his transaction with Bargains Galore. Further investigation by the Attorney General’s Office revealed the existence of another thirty victims, none of whom resided in the State of Chaos. The total amount of loss for all forty-five victims amounted to approximately $20,000.00.

Fraud prosecutions in the State of Chaos are dependent upon proving a specific amount of loss. While a prosecutor is authorized to aggregate amounts of loss based upon multiple victims, the amount of loss must exceed $1000.00 to be punishable as a felony. In order to prove an amount of loss in excess of $1000.00, the prosecutor needs to gain the cooperation of at least seven to ten additional victims, the closest other victim residing in a state 500 miles away. The anticipated cost for travel, food and accommodations for these witness-
es through trial: Over $10,000.00. The Prosecutor's response: Charge it as a one count misdemeanor involving the State of Chaos victim or decline the case.

B. The Correct Response? Are There Alternatives?

The limited budgets of most prosecutor offices prevent these cases from being fully prosecuted. How can the typical office justify spending $10,000.00 on witness expenses for a case that barely reaches a $20,000.00 amount of loss and that only involves a loss of $250.00 for a State of Chaos victim?

At the same time, there appears to be no lessening of Internet fraud cases. The Federal Trade Commission (FTC) recently reported that "Internet-related complaints accounted for 46% of all reported fraud complaints, with monetary losses of over $335 million and a median loss of $345." Consumer complaints filed with the FTC reveal that fraud complaints have risen each of the last three years. Are the fraudsters out there empowered to commit more crime due to an inadequate prosecutorial response? What can be done to maximize the likelihood that these Internet fraud cases will be prosecuted?

This article explores avenues for increasing the likelihood that Internet fraud cases will be prosecuted in a manner that maximizes the deterrent effect on existing and would-be fraudsters. Part II reviews methods for building the case at the outset, including exploring law enforcement databases and working with the private sector. Part III considers some alternatives for reducing the cost of a prosecution by, inter alia, simplifying the preliminary exam process. Part IV briefly explores the impact of Blakely v. Washington and United

---


2 Id. at 4.

States v. Booker on the charging and prosecution decisions in Internet fraud cases. Part V discusses the value of prosecuting the Internet fraud case as a misdemeanor as well as considering other viable charges. Part VI discusses working with federal authorities to get the Internet fraudsters prosecuted. Part VII explores some non-prosecution methods to help potential and actual Internet fraud victims. Finally, Part VIII reviews some lessons from the field—ideas generated from successfully prosecuted Internet fraud cases. The overarching goal is to empower the reader with methods for ensuring that costly Internet fraud cases are pursued in some fashion that results in a safer Internet experience for all.

II. BUILDING THE CASE

A. A Crime Tied to Victims

Most fraud cases perpetrated through the use of the Internet or over a computer are dependent upon proof of a specific amount of loss—the higher the amount of loss, the greater the penalty. For example, Michigan law criminalizes intentionally accessing a computer system to execute a scheme to defraud. The statutory penalty for this crime varies from a ninety-three-day misdemeanor to a ten-year felony depending upon the amount of loss involved. In order to convict a person of a felony, the prosecutor needs to prove a minimum of $1000.00 loss. In calculating the statutory amount of loss, the

---

5 Mich. Comp. Laws § 752.794 (2000). Throughout this article, Michigan law is provided as an example. It is not the intention of the author to present Michigan law as a model for the country—Michigan law is far from perfect in simplifying the prosecution of computer crimes. The reader is urged to consider the applicability of similar state laws within his or her state. In the absence of similar state laws, the reader is urged to present new legislation to the appropriate state authorities.
6 Id. § 752.797 (2000). Under the statute, a loss less than $200.00 is punishable as a ninety-three-day misdemeanor; a loss between $200.00 and less than $1000.00 is punishable as a one-year misdemeanor; a loss between $1000.00 and less than $20,000.00 is punishable as a five-year felony; and a loss in the amount of $20,000.00 or more is punishable as a ten-year felony. Id.
prosecutor is authorized to aggregate the loss to "a victim or group of victims" during any "12-month period" of time.\footnote{Id. § 752.792(2). The Michigan Legislature amended this statute in 2000 to allow for aggregation of loss incurred by a "group of victims." Id. Prior to the amendment, the statute only allowed aggregation of loss incurred by a single victim—a statutory structure not conducive to Internet fraud cases involving multiple one-time victims who have only lost a small amount. Id.}

In the hypothetical discussed in Section I.A., the prosecutor needs to find ten victims in order to prove an aggregate loss of over $1000.00. How can law enforcement find victims that are willing to travel to court to testify in order to prove the minimum amount of loss? Have victims been identified that the prosecutor can "afford" to use—that do not have too far to travel and hence are not too costly to the office? How does law enforcement determine the extent of the fraud?

B. Important Partnerships

1. The Federal Trade Commission

The Federal Trade Commission (FTC) has developed a consumer complaint database entitled Consumer Sentinel. "Consumer Sentinel collects information about consumer fraud and identity theft from the FTC and over 150 other organizations and makes it available to law enforcement partners across the nation and throughout the world for use in their investigations."\footnote{See \textit{Federal Trade Commission}, supra note 2, at 2.} Contributors to this database include various governmental and corporate entities including, but not limited to, the Federal Bureau of Investigation and the Internet Crime Complaint Center.\footnote{Id. "The Internet Crime Complaint Center (IC3) is a partnership between the [FBI] and the National White Collar Crime Center (NW3C)." Internet Crime Complaint Center, Welcome to IC3, http://www.ic3.gov (last visited Feb. 3, 2007). Information about NWC3 is available at http://www.nw3c.org; information about the IC3 is available at http://www.ic3.gov. IC3's mission, in relevant part, reads as follows: "For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes." Id.} Law enforcement can access this database—and specifically receive fraud information pertinent to one's jurisdiction—simply by becoming a member of Con-
sumer Sentinel. Through use of this resource, law enforcement may be able to gain information about more victims defrauded by their suspect. In the process, they may also be able to identify victims within their state (or nearby) that won’t be too costly to use as witnesses in the Internet fraud case.

2. Private Entities Such as eBay

Prosecutors of credit card fraud often suggest that credit card companies care little about stopping the fraud by assisting in the prosecution—the bottom line concern seems to be how the credit card entity will recoup from the financial loss. While this belief is likely grounded in actual experience, not all private entities are unwilling to work with law enforcement. One entity worth noting—especially because of the large amount of Internet auction fraud in the last several years—is eBay.

A review of eBay’s privacy policy demonstrates that this company is responsive to the needs of law enforcement. Under “Our Disclosure of Your Information,” the eBay privacy policy explicitly states, in relevant part:

We may also share your personal information with . . . law enforcement or other governmental officials, in response to a verified request relating to a criminal investigation or alleged illegal activity; (In such events we will disclose name, city, state, telephone number, email address, User ID history, fraud complaints, and bidding and listing history.).

It is apparent from a reading of this section that a “verified request” does not mean a subpoena or court order because this section ends with the following statement:

Without limiting the above, in an effort to respect your priva-

---

11 Id. at 3 ("Internet Auctions was the leading complaint category [for January-December 2005] with 12% of the overall [fraud] complaints.").
According to eBay personnel, this “verified request” can be satisfied with a facsimile request with office letterhead.\textsuperscript{14}

Further exploration of the eBay website reveals a section entitled “Security and Resolution Center” where eBay provides “Police Blotter” updates of cases in which fraudsters have been caught and prosecuted.\textsuperscript{15} This webpage further provides law enforcement with links to search for publicly available data on eBay such as “seller ID” and “active listings,” information on classes for law enforcement on how eBay works, and contact numbers to communicate with eBay’s “Fraud Investigation Team.”\textsuperscript{16} Even a cursory review of this information substantiates that eBay is dedicated to working with law enforcement and wants the fraudsters to be pursued.

Finally, criminal investigations into Internet fraud will be enhanced by working closely with eBay’s Fraud Investigation Team (FIT). According to eBay personnel, their business keeps its records for two years.\textsuperscript{17} FIT has access to many investiga-

\textsuperscript{13} Id.

\textsuperscript{14} Telephone Interview with Jack Christin, Jr., eBay Trust & Safety Counsel (Jan. 6, 2006).


\textsuperscript{16} Id.; eBay Law Enforcement Center, http://pages.ebay.com/securitycenter/law_enforcement.html (last visited Feb. 3, 2007). Another interesting link on the law enforcement page introduces l.e.a.d.s.online, “the nation’s largest online investigative system in use by law enforcement for the investigation of crimes involving property.” eBay Law Enforcement Center, supra. eBay states that it “makes listings from internet drop-off stores that list items on eBay available to law enforcement in the l.e.a.d.s.online searchable database.” Id.; see also LeadsOnline Web-based Investigation System, http://www.leadsonline.com (last visited Feb. 3, 2007).

\textsuperscript{17} Telephone Interview with Jack Christin, Jr., eBay Trust & Safety Counsel
tive tools and contact information and can provide helpful tips on how to get the most out of a request for these records—such as ensuring that the request covers archived documents retained by eBay, data concerning other incidents involving the same suspect, other screen names used by the suspect, and information regarding others victimized by the suspect.\textsuperscript{18} Significantly, eBay does not charge for searching for and providing the information officially requested by law enforcement\textsuperscript{19}—not something that many private entities are willing to do.

III. COSTS ASSOCIATED WITH PRELIMINARY EXAMINATIONS

A. Know Your Court

In the hypothetical described in Section I.A., in order to charge the Internet fraud as a felony, the prosecutor needs to gain the cooperation of at least ten victims (most of whom reside out of state). The anticipated cost for travel, food and accommodations for the preliminary examination through trial is over $10,000.00. The charging decision is often based on what the office can afford. Are there ways to keep these costs down at a preliminary examination?\textsuperscript{20}

In general, prosecutors working for a state Attorney General Office practice law in county circuit courts all over the state. While the prosecutor might be well-versed in the law, is he aware of the typical court procedure in a given county? Does he know what a particular judge expects or will allow in his courtroom? It is essential to have contacts to call on—a phone call can resolve a lot of uncertainty on how to best proceed.

One potential cost-saving example—where it will be vital

\textsuperscript{18} Id.

\textsuperscript{19} Id.

\textsuperscript{20} Of course, costs associated with witness travel will still be present if the case goes to trial. The “accused” has the right “to be confronted with the witnesses against him.” U.S. Const. amend. VI. Nevertheless, if the costs associated with a preliminary examination are reduced, the prosecutor might be able to afford to bring in the necessary witnesses for trial. In addition, once past the preliminary exam the defendant might plead guilty—thus, avoiding the costs altogether.
to know in advance how the court might react—involves commencing a preliminary exam within the statutory time frame but then asking the court for an adjournment to incur the costs associated with witness travel only when it is clear that the preliminary examination will go forward. While most states require a preliminary examination to commence within a certain time period, many do not require that the exam be completed within that period. Many state statutes authorize the delay or adjournment of a preliminary examination for "good cause." Does state case law exist that holds "good cause" is present when the prosecutor is trying to avoid significant unnecessary costs? Even if there is case law on point, how will the particular judge react to this request? It might be time to pick up the phone and call your contact.

B. Establishing Probable Cause with Hearsay Testimony

Of course, the costs associated with witness testimony are non-existent when a witness does not have to appear to testify. At a preliminary examination in federal court, the "finding of probable cause may be based upon hearsay evidence in whole or in part." This is likely due to the fact that a federal grand jury indictment may also properly be based upon hearsay evidence. Some states also permit the prosecutor to use hearsay evidence at a preliminary examination.

---

21 This example is predicated upon the assumption that hearsay testimony is not admissible at the preliminary examination to establish the victim fraud.


23 See, e.g., People v. Lewis, 408 N.W.2d 94 (1987) (where preliminary examination is started within fourteen days, there is no requirement to complete the exam within fourteen days).


25 Another alternative is a mandatory status conference—scheduled well before any preliminary examination date. Such an event might be useful in helping to determine whether or not the defendant is likely to waive his right to a preliminary exam.

26 Fed. R. Crim. P. 5.1 advisory committee's note.


28 See, e.g., Utah Const. art. 1, § 12 ("Nothing in this constitution shall pre-
However, even if a state generally requires non-hearsay evidence, statutes or rules may exist that authorize, in part, the use of hearsay testimony.\textsuperscript{29} For example, Michigan Rule of Evidence 1101(b)(8) provides that at a preliminary examination “hearsay is admissible to prove, with regard to property, the ownership, authority to use, value, possession and entry.”\textsuperscript{30} What witnesses in the hypothetical at Section I.A. might be included within this rule? Arguably, all of the victims should be included as the “authority to use” or “ownership” of their “property” (money or credit card information) is at issue. Additionally, representatives from eGads should be included as the “authority to use” the business “property” (the website) is at issue. Used properly,\textsuperscript{31} such a rule can greatly simplify and reduce the cost of a preliminary examination—it might eliminate the need for all witnesses except the investigating officer. Once again, it would be a good idea to find out ahead of time if the particular court one will appear before is receptive to such a practice.

\textsuperscript{29} See, \textit{e.g.}, \textsc{Kan. Crim. Proc. Code Ann.} § 22-2902(3) (West 2006) (“When the victim of the felony is a child less than 13 years of age, the finding of probable cause as provided in this subsection may be based upon hearsay evidence in whole or in part presented at the preliminary examination by means of statements made by a child less than 13 years of age on a videotape recording or by other means.”); \textsc{N.M. Metro Ct. R. Crim. P.} 7-608 (West 2006) (hearsay evidence of controlled substance test and autopsy results admissible at preliminary hearings).

\textsuperscript{30} \textsc{Mich. R. Evid.} 1101(b)(8). This provision was added effective May 14, 2001. \textit{Id.} at note (Note to 2001 Amendment). The Note to the 2001 Amendment provides: “In property crime cases, it allows the use of hearsay to prove certain elements of property crimes at the preliminary examination.” \textit{Id.}

\textsuperscript{31} To increase the likelihood that a court will allow for such an approach, the case investigator should be directed to get some kind of written certification from the witnesses. “Certified records of regularly conducted activity” are self-authenticating under \textsc{Federal Rule of Evidence} 902(11) and similar state rules. See, \textit{e.g.}, \textsc{Mich. R. Evid.} 902(11). In the alternative, a written and signed statement from the investigating officer revealing the victim’s comments regarding the “property” at issue will be of value in persuading the court.
C. Testimony through Telephonic, Voice or Video Conferencing

Even if a rule comparable to Michigan Rule of Evidence 1101(b)(8) does not exist in one's state, low cost alternatives for obtaining witness testimony may be available. Under Michigan law, on a "motion of either party" and "upon a showing of good cause," the testimony of "any witness" may be "conducted by means of telephonic, voice, or video conferencing."32 Does the courthouse have the technical capacity to conduct this kind of examination? If so, would the court consider the extraordinarily high expense of travel and accommodations as "good cause" for allowing the testimony by telephone or other means? As courtrooms across the country become better equipped to handle advances in technology,33 the judges in those courtrooms may be more willing to use high tech means for bringing in the testimony of victim witnesses at preliminary hearings.

D. Who Will Pay for the Travel?

It seems to be a common concern: United States citizens want less taxes and more money in their pockets. But how far can the "cuts" go before law enforcement can only "afford" to investigate and prosecute the most violent crimes? In light of this dilemma, might Internet fraud victims be amenable to the request that they "pay their way" to the courthouse? If the choice is between a declination and a prosecution, some victims may be willing to absorb the cost.34 Moreover, if the victim understands that the only way to get restitution is by being a witness—and the potential amount for restitution exceeds the cost of travel—the incentive for the witness to finance his or

---

34 Businesses that need to provide a witness to testify might also be willing to waive the costs of travel. While the private entity might not be willing to offer this publicly (on the website or otherwise), the entity might be willing to help out on a case by case basis. Of course, this suggestion is equally applicable to trial witnesses as it is to preliminary examination witnesses.
her own travel may rise significantly.\textsuperscript{35}

Additionally, a state may have a witness expense fund that could be used to finance witness travel.\textsuperscript{36} For example, the State of Maryland collects court costs in a variety of situations\textsuperscript{37} and then authorizes the use of those funds “to relocate victims and witnesses to protect them or to facilitate their participation in court proceedings.”\textsuperscript{38} Even if witness travel is not specifically included, there may be a statute that authorizes the court to order a defendant to pay costs associated with the investigation and prosecution of the defendant.\textsuperscript{39}

\textbf{E. Is a Preliminary Examination Really Needed?}

The Michigan Legislature is presently considering legislation that would eliminate the general right to a preliminary examination for felony crimes.\textsuperscript{40} Upon the motion of either party and for “good cause,” a court could order a preliminary examination if the maximum sentence for the underlying felony charge was imprisonment for ten years or more.\textsuperscript{41} According to Michigan Attorney General Mike Cox, “[s]udies show that 75% of preliminary exams are waived by defendants, but only after

\textsuperscript{35} This idea was discussed in detail by Todd Lawson, Assistant Attorney General, Office of the Attorney General of Arizona, in a panel discussion on “The Decision to Prosecute,” during an April 2006 conference entitled “Prosecutorial Responses to Internet Victimization” held at the University of Mississippi School of Law in Oxford, Mississippi, and hosted by the National Center for Justice and the Rule of Law and the National Association of Attorneys General.

\textsuperscript{36} This idea was provided by Carolyn Henneman, Assistant Attorney General, Office of the Attorney General of Maryland, during the presentation of this paper at an April 2006 conference entitled “Prosecutorial Responses to Internet Victimization” held at the University of Mississippi School of Law in Oxford, Mississippi, and hosted by the National Center for Justice and the Rule of Law and the National Association of Attorneys General.

\textsuperscript{37} See MD. CODE ANN., CRIM. PROC. § 7-301 (West 2006).

\textsuperscript{38} See MD. CODE ANN., CRIM. PROC. § 11-904 (West 2006).

\textsuperscript{39} See, e.g., MICH. COMP. LAWS § 769.1f (2000).


\textsuperscript{41} Id.
police officers, victims, and other witnesses have spent hours in court.\textsuperscript{42} Moreover, Cox notes, the legislature can eliminate preliminary exams because they are a "statutory right, not a constitutional right."\textsuperscript{43} Not surprisingly, the legislation is vigorously opposed by civil liberties groups.\textsuperscript{44} While passage of the legislation is far from clear, it certainly presents an alternative that would simplify and reduce the cost of Internet fraud prosecutions.\textsuperscript{45}

IV. SENTENCING GUIDELINES AND THE BOOKER PROBLEM

A. Booker Background

The Federal Sentencing Guidelines (hereinafter "Guidelines") were implemented in 1987 as a response to Congress' perception that defendants around the nation were receiving widely disparate sentences depending on the judge, location, offense, and other factors.\textsuperscript{46} The Guidelines provided a mandatory formalistic approach which limited the judge's role or discretion while expanding the traditional role of the prosecutor in determining the sentence imposed. Many states also have their own form of sentencing guidelines—some of the guidelines are mandatory and some are discretionary.\textsuperscript{47}


\textsuperscript{43} Id.


\textsuperscript{45} According to audience participants during the presentation of this paper at the April 2006 conference entitled "Prosecutorial Responses to Internet Victimization" held at the University of Mississippi School of Law in Oxford, Mississippi, several states, including Colorado, Maryland and Florida, have adopted laws with similar provisions.

\textsuperscript{46} United States Sentencing Commission, http://www.ussc.gov (last visited Feb. 3, 2007). For more information, visit the United States Sentencing Commission's website. Id.

\textsuperscript{47} See National Center for State Courts, Knowledge and Information Services: Sentencing FAQs, http://www.ncsconline.org/WC/FAQs/SentenFAQ.htm (last visited Feb. 3, 2007); see also U.S. Dept. of Justice, State Court Organization 1998,
Over the last six years, however, through various decisions of the United States Supreme Court, including United States v. Booker, and Blakely v. Washington, the Court has deemed mandatory sentencing guidelines unconstitutional under the Sixth Amendment, thus rendering them advisory rather than mandatory. In Booker, the Court held that "[a]ny fact (other than a prior conviction) which is necessary to support a sentence exceeding the maximum authorized by the facts established by a plea of guilty or a jury verdict must be admitted by the defendant or proved to a jury beyond a reasonable doubt." In other words, the Sixth Amendment requires juries, not judges, to find facts relevant to sentencing.

While subject to interpretation in the courts, Booker and Blakely appear to have an impact only in those states with mandatory sentencing guidelines—they do not affect sentencing in those jurisdictions where sentencing guidelines are wholly discretionary. As one commentator stated, "The very breadth of their discretion seems to somehow insulate them from jury


51 Booker, 543 U.S. at 244.

52 Regarding sentences handed down prior to Booker and Blakely, the United States Supreme Court recently held that appellate courts can rely on a harmless error analysis in reviewing those sentences. Washington v. Recueno, 126 S. Ct. 2546 (2006).

53 See, for example, People v. McCuller, 715 N.W.2d 798 (Mich. 2006), and People v. Drohan, 715 N.W.2d 778 (Mich. 2006), where the Michigan Supreme Court held that Michigan’s sentencing guidelines do not violate Blakely because the guidelines score the minimum range of an indeterminate sentence.
States with discretionary or indeterminate sentencing guidelines seem to remain free from constitutional trouble even though judges in those states may engage in “invisible” fact finding in arriving at the appropriate sentence.

B. Booker Relevancy to Internet Fraud Cases

How ought a state with mandatory sentencing guidelines approach the charging decision in an Internet fraud case? If a prosecutor hopes to hold a defendant accountable at sentencing for a specific amount of fraud loss, the full amount of loss needs to be proved before a jury. Just as with other elements of a crime on which a conviction is based, calculating the amount of loss which has an effect on a defendant’s conviction must be proven to a jury beyond a reasonable doubt.

United States v. Davis, a mandatory guidelines case, is instructive. In Davis, the sentencing judge independently made factual findings of the amount of loss, which enhanced the defendant’s sentence for bank fraud beyond the facts established by the jury verdict. The court found that, just as Booker’s sentence was based on independent fact-finding and thus violated the Sixth Amendment, this sentence, too, violated the Sixth Amendment. Therefore, the court remanded the case for resentencing.

So what does this mean for the Internet fraud prosecution? In a jurisdiction with “mandatory” sentencing guidelines, it appears that the prosecutor should include some kind of reference—in the charging document—to the victims he wants to hold the defendant accountable for at sentencing. Of course,

---

55 397 F.3d 340 (6th Cir. 2005).
56 Id. at 350-51.
57 Due to Booker, many federal courts now view the United States Sentencing Guidelines as merely advisory. This approach allows trial judges to continue with judicial fact-finding at sentencing—without violating the Sixth Amendment. See, e.g., United States v. Owens, 441 F.3d 486, 490 (7th Cir. 2006) (“Booker clearly permits a district court to grant a sentencing enhancement based on facts not
that means that the prosecutor needs to know early on in the prosecution which victims he can "afford" to include in the charging document. Once again, the high costs might present an insurmountable barrier. Are there ways to reduce the costs?

C. Value of Plea Agreements

In United States v. Murdock, the defendant contended that his sentence for causing another to possess false documents with intent to defraud must be vacated because the judge decided the amount of loss without submitting the issue to the jury for a determination of loss beyond a reasonable doubt. The Sixth Circuit Court of Appeals held, however, that there was no Sixth Amendment violation because the sentencing court's determination of the amount of loss was supported by the defendant's admission in the plea agreement and at the plea hearing regarding the amount of loss. As held in Booker, the court noted that sentencing facts "established by a plea of guilty or a jury verdict" do not violate the Sixth Amendment.

What does Murdock (and cases similarly decided) mean for Internet fraud prosecutions? Plea agreements provide a means to reduce the costs of prosecuting an Internet fraud case. As Booker does not appear to prohibit reliance on a defendant's own admissions, a prosecutor might work to generate a plea agreement involving an agreement to a specific amount of fraud loss. Defendant might agree in a plea to a certain amount of fraud loss in exchange for the prosecutor not pursu-

---

charged in the indictment, not proven to a jury beyond a reasonable doubt or not admitted by the defendant." (citing United States v. Booker, 543 U.S. 220, 226-27 (2005); United States v. Gonsalves, 435 F.3d 64, 72 (1st Cir. 2006); United States v. Crosby, 397 F.3d 103, 112 (2d Cir. 2005).

58 398 F.3d 491 (6th Cir. 2005).

59 Id. at 501 (quoting Booker, 543 U.S. at 244); see also United States v. Bradley, 400 F.3d 459, 462 (6th Cir. 2005) (the Sixth Amendment and Booker do not apply to "agreed-upon facts"), cert. denied, 126 S. Ct. 145 (2005).

60 See Barry Boss & Nicole L. Angarella, Negotiating Federal Plea Agreements Post-Booker: Same as It Ever Was? 21 CRIM. JUST. 22, 25 (2006) ("Although it is important to understand this new sentencing landscape and consider it in negotiating a plea deal with the government, the reality is that the new system has not brought any radical change to plea or sentencing practices.").
ing a greater amount of loss and victims. The defendant might have an incentive to agree to this kind of an offer if he thinks he can avoid prosecution for a greater amount of loss.

D. Booker’s Impact on Restitution

In United States v. Sosebee, defendant challenged the validity of the restitution order in light of Booker. She argued that her sentence violated her Sixth Amendment rights because the restitution order was based on a factual determination by the district court that was neither found beyond a reasonable doubt by a jury nor admitted by the defendant. Noting that even though restitution may be considered punishment, the Sosebee court nevertheless held that restitution orders are not affected by the Supreme Court’s recent ruling in Booker.

According to the Sosebee court, restitution orders are authorized by statute and in that sense are “distinct and separate from the United States Sentencing Guidelines.” The court noted that “[a]lthough the guidelines mandate imposition of restitution where allowable under the statutes, the restitution statutes function independently from the guidelines and do not rely on the guidelines for their validity.” Furthermore,

---

61 Of course, the prosecutor is only capable of binding his or her own office. Prosecutors in other states could still pursue a case in their state assuming they have proper jurisdiction. The likelihood of this occurring, however, is quite small—especially if the defendant resides in the state in which the defendant pleaded guilty.
62 Nevertheless, it will be difficult for a prosecutor to have the capability to work this kind of agreement if the defense bar thinks the prosecutor’s office will not work the case because they can’t afford it.
63 419 F.3d 451 (6th Cir. 2005).
64 Several other circuits have also held that Booker does not apply to restitution orders under the Victim and Witness Protection Act or the Mandatory Victim Restitution Act. See, e.g., United States v. Belk, 435 F.3d 817 (7th Cir. 2006); United States v. Craiglow, 432 F.3d 816 (8th Cir. 2005); United States v. Garza, 429 F.3d 165, 170 (5th Cir. 2005); United States v. Visinaiz, 428 F.3d 1300 (10th Cir. 2005); United States v. Bussell, 414 F.3d 1048 (9th Cir. 2005); United States v. May, 413 F.3d 841 (8th Cir. 2005); United States v. George, 403 F.3d 470 (7th Cir. 2005). See also Sosebee, 419 F.3d at 461 (citing cases).
66 419 F.3d. at 462.
67 Id.
"the Victim and Witness Restitution Act and the Mandatory Victim Restitution Act specifically state that the amount of restitution should be equal to the ‘amount of each victim’s losses as determined by the court.’\textsuperscript{68} Thus, Booker’s holding that the Sentencing Guidelines are now merely advisory does not appear to affect orders of restitution.\textsuperscript{69}

The Sosebee lesson appears to be that a prosecutor can ask the sentencing court for a restitution amount higher than the fraud amount proved beyond a reasonable doubt before the jury.\textsuperscript{70} In addition to helping reduce the cost of prosecution, this might provide the prosecutor with some negotiating leverage.

V. ALTERNATIVE PROSECUTION ROUTES

A. Misdemeanor Charges

When making the determination of how to spend precious budget dollars, some jurisdictions appear to place higher priority on felony convictions. But what’s so bad about a misdemeanor conviction? In all likelihood, acceptance of a misdemeanor conviction as a valuable remedy for Internet fraud—by law enforcement and, to a lesser extent, the public—is the biggest barrier. When the choice becomes declination or a prosecution, however, a misdemeanor is a valuable alternative. Moreover, there are some fairly strong reasons to consider misdemeanor convictions as the best choice.

In the hypothetical described in Section I.A., the suspect company had a presence in the State of Chaos and at least one victim within the State of Chaos—a victim who had lost $250.00. Under a typical fraud statute, this crime could be prosecuted as a one-year misdemeanor.\textsuperscript{71} Such a conviction, at a minimum, serves to satisfy the local interests in a prosecu-

\textsuperscript{68} Id (emphasis in original) (quoting 18 U.S.C. § 3664(f)(1)(A) (2000)).
\textsuperscript{69} Id.
\textsuperscript{70} While Sosebee involved federal restitution laws, a similar analysis arguably applies to state restitution laws.
\textsuperscript{71} See, e.g., MICH. COMP. LAWS § 752.787(1)(b)(i) (2000) (loss between $200.00 and less than $1000.00 is punishable as a one-year misdemeanor).
tion. Moreover, the cost of the prosecution is manageable—whether hearsay is permitted at a preliminary examination or not. Finally, the likelihood of collecting restitution—and actually providing the victim with money to recoup his losses—is much higher with such a conviction. One victim, a local defendant, and a small amount of loss—these facts do not present an insurmountable barrier to collection of the loss. In the long run, few fraud victims are happier than those that actually get their money back.

B. Identity Theft

For various reasons, a prosecutor might consider charging an Internet fraud case as an identity theft case. Numerous states have passed laws addressing the problems of identity theft.72 Oftentimes, a financial fraud case can easily be re-characterized as an identity theft case. For example, considering the hypothetical in Section I.A., further investigation may reveal that the post office box located in Cooley City, Chaos, was set up with the unauthorized personal identifying information of another person living in the State of Chaos. Some excellent reasons exist for considering this case as an identity theft matter.

Unlike Internet fraud statutes, identity theft statutes are generally not based upon proof of an amount of loss.73 The paramount concern in identity theft cases is not the money lost—it is the unauthorized usage of another’s personal identifying information.74 Therefore, an amount of loss is neither

---


73 See, e.g., MICH. COMP. LAWS §§ 445.65-69 (West 2006).

74 The Michigan law provides one example of a definition of “[p]ersonal identifying information”:

[A] name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person’s financial
needed nor relevant. Quite obviously, this means fewer witnesses are needed (and, hence, a reduction in cost of prosecution in comparison to the Internet fraud case).

Moreover, in many states, using an identity theft statute provides a prosecution for a felony rather than a misdemeanor.\textsuperscript{75} Oftentimes, the statutory maximum penalty for identity theft exceeds that for Internet fraud—especially when comparing the available penalty for the Internet fraud prosecution that involves only the low cost local victims (likely a misdemeanor).\textsuperscript{76} The high available penalty for identity theft would certainly seem to satisfy the law enforcement entities concerned with ensuring that their precious dollars are allocated in a high impact fashion.

C. Enhancing the Penalty and Plea Negotiations With Computer Crime Statutes

In the hypothetical discussed in Section I.A., the defendant did not merely commit identity theft. By using a computer system to offer up bogus products and provide a payment method involving a post office box obtained in another’s name, he also committed a computer crime.

State legislatures often consider usage of a computer to

accounts, including, but not limited to, a person’s name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother’s maiden name, demand deposit account number, savings account number, financial transaction device account number or the person’s account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

\textit{Id.} § 445.63(k).

\textsuperscript{75} See, e.g., \textit{id.} § 445.69(1).

\textsuperscript{76} \textit{Id.} ("[A] person who violates section 5 or 7 is guilty of a felony punishable by imprisonment for not more than 5 years or a fine of not more than $25,000.00, or both."); cf. \textit{id.} § 752.797 (loss less than $200.00 is punishable as a ninety-three-day misdemeanor; loss between $200.00 and less than $1000.00 is punishable as a one-year misdemeanor; loss between $1000.00 and less than $20,000.00 is punishable as a five-year felony; and loss in the amount of $20,000.00 or more is punishable as a ten-year felony).
commit a crime—even a traditional crime—a more serious criminal act.\textsuperscript{77} The mere fact that a computer or computer system was used to facilitate the crime makes the act more severe. For example, Michigan law provides: “A person shall not use a computer program, computer, computer system, or computer network to commit, attempt to commit, conspire to commit, or solicit another person to commit a crime.”\textsuperscript{78} This charge is in addition to any other crime committed during the time in question including the underlying offense the computer was used to commit.\textsuperscript{79}

Even more significant, however, is the potential for an enhanced penalty. Oftentimes the penalty is tied to the crime that the computer was used to commit.\textsuperscript{80} By way of illustration, assume that the crime of identity theft is a five-year felony. Under Michigan law, using a computer to commit this five-year felony would be punishable as a separate seven-year felony.\textsuperscript{81} In addition, the law might provide for a consecutive sentence\textsuperscript{82}—which certainly enhances the potential for effective plea negotiations. Quite obviously, effective and low-cost prosecution alternatives exist—but the prosecutor needs to think beyond merely considering the case as a monetary scheme to defraud.

\textsuperscript{77} See, e.g., \textit{id.} § 752.796(1).
\textsuperscript{78} \textit{Id.} § 752.796(2).
\textsuperscript{79} \textit{Id.} §§ 752.796(2)-3.
\textsuperscript{80} \textit{Id.} § 752.797.
\textsuperscript{81} \textit{Id.} (“If the underlying crime is a felony with a maximum term of 4 years or more but less than 10 years, the person is guilty of a felony punishable by imprisonment for not more than 7 years or a fine of not more than $5,000.00, or both.”).
\textsuperscript{82} \textit{Id.} § 752.797(4) (“The court may order that a term of imprisonment imposed under subsection (3) be served consecutively to any term of imprisonment imposed for conviction of the underlying offense.”). The Michigan legislature permits a consecutive sentence within the discretion of the sentencing court. Even greater potential would exist if this law required mandatory consecutive sentences.
VI. WORKING WITH FEDERAL AUTHORITIES

A. Connection with Federal Authorities

Ideally, the Internet fraud case that is investigated by local or state authorities should be prosecuted in the state courts. Frequently, however, law enforcement concludes that prosecuting the Internet fraud case in state court is cost-prohibitive. Given the "deeper pockets" of the federal government, there are some strong reasons to consider working with the federal authorities to get the case prosecuted in federal court.\(^83\)

Initially, it helps to realize that the United States Attorneys Offices do not want to steal state cases.\(^84\) This seemingly widespread belief likely stems from the fact that once a case becomes a federal case, it must comply with the federal criminal justice system. This includes a defendant's right to be prosecuted through a grand jury indictment.\(^85\) Federal grand jury proceedings are governed by a general rule of secrecy—a knowing violation of this may be punished as a contempt of court.\(^86\) This might help explain the lack of a free flow of information between the state and federal authorities once the case becomes a federal case. The lack of communication that follows may induce state and local officers to believe that the federal government does not want to work with the states—a belief that is generally untrue.

The hypothetical discussed in Section I.A. involved some forty-five witnesses throughout the country with a total loss amount of approximately $20,000.00. Given the fact that the Chaos defendant victimized people from all over the country—thus impacting on interstate commerce—it appears on its

\(^83\) Of course, United States v. Booker, 543 U.S. 220 (2005), and its implications on the federal charging decision as well as the federal sentencing, needs to be considered. See supra notes 47-70 and accompanying text.

\(^84\) This statement is based upon the personal experience of the author while working in the United States Attorney's Office for the Eastern District of Michigan from 1989-1999.

\(^85\) U.S. CONST. amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury . . . ").

\(^86\) FED. R. CRIM. P. 6(e)(2), (7).
face to be worthy of federal consideration. How does a state prosecutor go about getting a case prosecuted in federal court?

At the outset, it helps if the local and state investigators have contacts within the federal system. Many federal law enforcement agencies investigate fraud cases. These contacts can, at a minimum, provide the connection to get a case considered for federal prosecution.

Preferably, however, the local and state investigators won't merely have federal contacts. Internet fraud task forces—comprised of both state and federal authorities—provide the most efficient means for choosing the correct forum for prosecution. Some task forces might also work closely with private industry. Working side by side, maybe even assisting in each other's search warrants, law enforcement officers will know from the beginning whether a case should be prosecuted in state or federal court.

B. Internal Prosecution Guidelines

Of course, federal law exists that criminalizes Internet fraud. It is important to know, however, that United States

---

87 Based upon the personal experience of the author, the following federal agencies, amongst others, investigate fraud matters on varying levels: The Federal Bureau of Investigation, the United States Secret Service, the United States Postal Inspectors, the Internal Revenue Service-Criminal Investigation Division, United States Customs, United States Bureau of Alcohol, Tobacco and Firearms, United States Food and Drug Administrations, and the United States Department of Education.


89 See, e.g., 18 U.S.C. § 1028 (2000) ("Fraud and related activity in connection with identification documents and information"); id. § 1029 ("Fraud and related activity in connection with access devices"); id. § 1030 ("Fraud and related activity in connection with computers"); id. § 1541 ("Frauds and swindles"); id. § 1343
Attorney Offices often have internal “prosecution guidelines” before a case will be accepted for federal prosecution.\footnote{This information is not publicly available. One needs to contact the specific United States Attorney Office to determine if such a prosecution guideline exists in that office.} Using the hypothetical discussed in Section I.A., assume that the State of Chaos has two federal districts—the Eastern District of Chaos (located in a large urban area) and the Western District of Chaos (located in a smaller urban area). The Eastern District—given the larger number of fraud cases in that district—might require the fraud loss to exceed $40,000.00 before the case can be presented to a grand jury. The Western District—given that it is located in an area with less fraud—might merely require the fraud loss to exceed $10,000.00.\footnote{Amount of loss is not the only factor that might be considered. United States Attorney Offices also consider, inter alia, factors such as the number of victims, the prevalence of the fraud, and the complexity of the crime. One needs to contact the specific United States Attorney Office to determine the specific requirements of the prosecution guidelines for that office.} Equipped with knowledge of the prosecution guidelines, law enforcement will know from the outset if a federal prosecution can even be considered.\footnote{Of course, the full amount of loss may not be known until well into the investigation—another reason why working with a task force is a good idea. In such a scenario, a case that started out as a state prosecution might develop into a much larger fraud. If state and federal officers are jointly working the case in the context of a task force, presenting the matter to the United States Attorney Office when the larger fraud is discovered will be routine.} 

C. Special Assistant United States Attorneys

Even if an appropriate federal statute exists and the Internet fraud case meets the threshold required for the prosecution guidelines of the relevant United States Attorney Office, the United States Attorney’s Office might not have a federal prosecutor available to prosecute the case. In the alternative, even if a federal prosecutor is available, the state prosecutor—due to his ongoing involvement in the case—might be best situated to prosecute the matter.\footnote{Of course, if the only alternative is to have an existing federal prosecutor}
a state prosecutor then should seek authorization to prosecute the case in federal court as a Special Assistant United States Attorney (hereinafter SAUSA). Federal law authorizes the United States Attorney General to “appoint Special Assistants to assist the United States Attorney when the public interest so requires.” Arguably, “public interest” requires such a desig-

pursue the case, this choice is certainly better than no prosecution at all.


96 THE UNITED STATES DEPARTMENT OF JUSTICE, supra note 94. In its entirety, section 3-2.300 provides:

Section 543 of Title 28 authorizes the Attorney General to appoint Special Assistants to assist the United States Attorney when the public interest so requires, and to fix their salaries. These Assistants are designated as Special Assistants to the United States Attorney and are appointed for the purpose of assisting in the preparation and presentation of special cases. Their salaries, if any, are a matter of agreement between the Department and the individual, and are fixed at an annual, monthly, per diem, or when-actually-employed rate. Under the appropriate circumstances, a private attorney may receive a Special Assistant appointment pursuant to 28 U.S.C. Sec. 543, with or without compensation, to assist the United States Attorney with specific matters. Such appointments raise ethics and conflict of interest issues that must be addressed. To appoint private attorneys as Special Assistant United States Attorneys pursuant to 28 USC Section 543, compensated or not, approval is required by EOUSA.

Attorneys employed in other departments or agencies of the federal government may be appointed as Special Assistants to United States Attorneys, without compensation other than that paid by their own agency, to assist in the trial or presentation or cases when their services and assistance are needed. Such appointments, and appointments of Assistant United States Attorneys from one United States Attorney’s office to another, may be made by the United States Attorney requiring their services.

In instances where an entire United States Attorney’s Office recuses itself, the Attorney General may, pursuant to 28 U.S.C. Sec. 515, appoint any officer of the Department of Justice, or any attorney specially appointed under law, to conduct any kind of legal proceeding which United States Attorneys are authorized by law to conduct, whether or not such appointee is a resident of the district in which the proceeding is brought. Said appointee specially retained under authority of the Department of Justice is appointed as a Special Assistant or a Special Attorney to the Attorney General and reports directly to the Attorney
nation when a viable federal crime exists that will otherwise be declined.

Determination of whether to grant SAUSA status is generally a wholly discretionary matter decided by the United States Attorney in the specific federal district. In general, the United States Attorney’s Office has to be convinced that it helps in some prosecution goal or program area or the prosecution of a specific case. Of course, it would help in gaining SAUSA status to request no salary in excess of what one is making as a state prosecutor. Ideally, a state prosecutor working with a state/federal task force will have obtained the SAUSA designation in advance to maximize the capacity of the prosecutor to take the case to the most appropriate forum whenever the need arises.

D. Benefits of Prosecuting Internet Fraud as a Federal Case

Some significant advantages exist in gaining SAUSA status and taking an Internet fraud case to federal court. From reduced costs to simplification of the prosecution, the federal courts offer a prosecution alternative worthy of consideration.

In investigating the matter, Federal Rule of Criminal Procedure 41 provides broad authority for the issuance of search warrants. If the search warrant involves Internet service providers, federal law allows federal courts to issue nationwide search warrants for unopened e-mail. The only restriction on the nationwide scope of the e-mail warrant is that the issuing court must have jurisdiction over the offense under investigation. This obviously holds the potential to simplify the re-

General or delegee. Such appointments are executed by the Executive Office for United States Attorneys.

Id.

The textual comments are the opinion of the author based upon actual experience.

Id.

FED. R. CRIM. P. 41(b).


Id. §2703(d). Congress authorized this section as part of the PATRIOT Act
trial of relevant evidence in an Internet fraud case.

In prosecuting the case, the federal prosecutor only needs one witness at a preliminary examination. Unlike many states, hearsay evidence is admissible at a federal preliminary examination.\textsuperscript{102} Notably, one’s entire case can be presented through the case agent assigned to the matter\textsuperscript{103}—no victim needs to attend at all.

Due to the grand jury system, many prosecutors choose to indict a defendant before any preliminary examination occurs.\textsuperscript{104} Like a preliminary examination, hearsay evidence is admissible in grand jury proceedings.\textsuperscript{105} Many prosecutors choose to seek indictments from federal grand juries through the testimony of one witness—the case agent.\textsuperscript{106} Like a federal preliminary examination, no victim needs to be present—which obviously reduces some of the initial costs associated with an Internet fraud prosecution.

In the typical Internet fraud case, witnesses live all over the United States and often out of the country.\textsuperscript{107} Assuming the case must go to trial, the long reach of the federal government makes connecting with these witnesses easier. Trial subpoenas may be served by “a marshal, a deputy marshal, or any

---

and, as originally written, was set to “sunset” on December 31, 2005, unless renewed by Congress. President Bush recently signed legislation making this provision permanent. Alexei Alexis, \textit{Bush Signs Bill Renewing PATRIOT Act With New Provisions to Safeguard Data}, 78 CRIM. L. REP. (BNA) 669, Mar. 15, 2006.

\textsuperscript{102} At a preliminary examination in federal court, the “finding of probable cause may be based upon hearsay evidence in whole or in part.” \textit{Fed. R. Crim. P.} 5.1.

\textsuperscript{103} Based upon the personal experience of the author, most federal preliminary exams involve no more than a few witnesses.

\textsuperscript{104} If a federal prosecutor does this, he does not need to proceed with the preliminary examination as the determination of “probable cause” as been accomplished by the grand jury.

\textsuperscript{105} \textit{Costello v. United States}, 350 U.S. 359 (1956).

\textsuperscript{106} This statement is based upon the personal experience of the author.

\textsuperscript{107} Subpoenas directed to witnesses in a foreign country are discussed at 28 U.S.C. § 1783 (2000). In such a situation, the prosecutor ought to consider seeking assistance from the United States Department of Justice, Office of International Affairs. See United States Department of Justice, Criminal Division, Office of International Affairs, http://www.usdoj.gov/criminal/odia.html (last visited Feb. 3, 2007).
nonparty who is at least 18 years of age.\textsuperscript{108} Moreover, the federal subpoena "requiring a witness to attend a hearing or trial may be served at any place within the United States."\textsuperscript{109}

Finally, and maybe most importantly, any fees connected with a federal case are, of course, paid for by the federal government.\textsuperscript{110}

\section*{VII. NON-PROSECUTION METHODS TO HELP VICTIMS}

Victims of Internet fraud are nearly powerless to correct the damage caused by the fraudsters. The ideal remedy (police catching the defendant) is sometimes not realistic because the thieves are quite often in a different state, country, or even continent. Assuming the prosecutor cannot pursue the case criminally, can law enforcement help out in other ways?

The Internet is replete with sources on how to prevent fraud.\textsuperscript{111} Information is available to help both businesses and consumers enhance the security of online transactions.\textsuperscript{112} The biggest problem with this publicly available information is that

\textsuperscript{108} FED. R. CRIM. P. 17(d). Federal agents exist all over the county who can assist in serving subpoenas.

\textsuperscript{109} FED. R. CRIM. P. 17(e)(1); see also 18 U.S.C. §§ 3481-3510 (2000) ("Witnesses and Evidence").


\textsuperscript{111} Using the term "fraud prevention," a Google search by the author on March 6, 2006, revealed 29,300,000 links to related online sources.

\textsuperscript{112} While there are many excellent sites, one exceptional source is OnGuard Online, http://onguardonline.gov (last visited Feb, 3, 2007). On the homepage, OnGuard Online states that it "provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information." \textit{Id.} Another great resource is Scambusters.org, http://www.scambusters.org (last visited Feb. 3, 2007). Scambusters.org provides links to articles covering just about every topic in the area of Internet fraud. \textit{Id.} Of course, as has already been discussed, the Federal Trade Commission and the National White Collar Crime Center are also excellent resources. See \textit{supra} notes 9-12 and accompanying text.
there is simply too much information.113 Citizens often do not know where to begin—either to prevent the fraud or to act properly once they have been defrauded.

Law enforcement can help by disseminating good information. Prosecutors should seek authorization to speak to community groups about fraud prevention—while this may not be the traditional role of the prosecutor, it is a vital public role given the difficulties in bringing the Internet fraud cases to court. Prosecutors should consider creating a copy of an Internet fraud prevention guide or making copies available of other excellent resources.114

Law enforcement can help victims help themselves. Assume, for example, that the Chaos victim described in Section I.A. contacts the prosecutor’s office. Believing that he has been financially defrauded, he is also worried that he may be a victim of identity theft. What help can the prosecutor provide—even if the office cannot take the case for prosecution? He can begin by introducing the victim to the resources of the Federal Trade Commission.

The Federal Trade Commission provides great advice on four immediate steps the victim should take.115 First, the victim can prevent future damage by alerting credit reporting agencies as soon as possible and placing a fraud alert on his credit report. Second, the victim needs to close all financial accounts that he believes have been affected by the fraud. The victim needs to fill out an identity theft affidavit116 “when disputing new unauthorized accounts.”117 Third, the victim should file a police report in the community where the fraud took place.118 This report, along with the identity theft affida-

---

113 See supra note 112.
117 See supra note 116.
118 In Michigan, law enforcement officials are required to provide a copy of
vit, will help the victim in dealing with creditors.\textsuperscript{119} Lastly, the victim should file a complaint with the Federal Trade Commission.\textsuperscript{120} As already discussed,\textsuperscript{121} the Federal Trade Commission maintains a database of consumer complaints—this data might help other law enforcement authorities build a better case against the fraudster in question.\textsuperscript{122}

Law enforcement should also inform the victim about the possible availability of civil remedies. Importantly, if the proof is lacking in terms of the criminal charges ("beyond a reasonable doubt" standard), civil suits can often still prevail ("preponderance of the evidence" standard). The State Attorney General might be able to bring suit.\textsuperscript{123} The citizen victim might also be able to bring a suit.\textsuperscript{124} In the event a criminal prosecution is not available, law enforcement needs to know what civil remedies potentially exist. Providing information to Internet fraud victims can, at the least, give the victim a sense that the situation is not hopeless.

\section*{VIII. Lessons from the Field}

The contents of this paper were presented at an April 2006 conference entitled "Prosecutorial Responses to Internet Victimization" held at the University of Mississippi School of Law in Oxford, Mississippi, and hosted by the National Center for Justice and the Rule of Law and the National Association of

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{119}] In providing this kind of documentation, law enforcement can provide a tremendous credibility boost for the victim in dealing with the creditors.
\item[\textsuperscript{120}] See supra note 116.
\item[\textsuperscript{121}] See supra notes 9-12 and accompanying text.
\item[\textsuperscript{122}] See also Federal Trade Commission, Taking Charge: Fighting Back Against Identity Theft, February 2005, available at http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm. This document provides important details on how the victim can help himself. Id.
\item[\textsuperscript{123}] In Michigan, for example, violations of Michigan's Identity Theft Protection Act are also actionable under the Consumer Protection Act as "unfair, unconscionable, or deceptive methods, acts, or practices." Mich. Comp. Laws § 445.903(1)(jj) (2000). The Attorney General can also bring a class action suit. Id. § 445.910.
\item[\textsuperscript{124}] Under Michigan law, consumers can recover actual damages or $250, whichever is greater, along with attorney fees. Id. § 445.911(2).
\end{itemize}
\end{footnotesize}
Attorneys General. Present in the audience were assistant attorneys general from all over the United States. Some of the attorneys present provided answers to questionnaires on lessons they had learned in prosecuting Internet fraud cases in their respective states. Many of the comments are interspersed throughout this article.

In particular, however, the Oklahoma Attorney General’s Office provided some very helpful insights. Rather than paraphrasing the remarks from this office, the comments are provided herein in their entirety. The remarks speak for themselves and are valuable in that they are the comments of a prosecutor presently working Internet fraud cases on a routine basis. As you read through the comments, pay particular attention to the suggestions regarding following the money trail to the banks and the possibility of questioning the suspect before the arrest. The remarks follow the questions presented in the questionnaire as follows:

1) Have you had success in your Internet Fraud prosecutions? If so, please explain. Please provide specific reasons why your prosecutions have been successful.

Our office has had a 100% success rate in prosecuting Internet auction fraud cases. I believe the reason for this is threefold. First, our investigators thoroughly investigate these cases to the point that it is virtually impossible for the defense to dispute. Many times, the defendant admits guilt when questioned after being Mirandized or quickly decides to plead guilty and take a deal rather than face the uncertainty of a jury trial. How do our investigators accomplish this? After they have identified a person as a target, they send the Internet auction fraud site such as eBay a subpoena to obtain the target’s records. These records contain the full registration, IP addresses, complete listing and bid history and financial information. We use this information to obtain further records including PayPal

---

125 Special thanks to Julie A. Bays, Assistant Attorney General, Oklahoma Attorney General’s Office, Consumer Protection Unit, for her thoughtful comments as provided herein.
records, credit card and banking information. We can usu-
ally follow the financial transactions directly to the target's
bank account or PayPal account. In Oklahoma we also
have the added benefit of a cable company that keeps IP
address information for at least six months. Every time the
target logs on or registers, we have the IP address for that
person. It always leads right back to the target.
Secondly, our investigators usually look for potential tar-
gets that have victims residing in or near our state in
order to make it practical if a witness needed to testify. If
we cannot find anyone near Oklahoma, we then look for
victims that are willing to travel even with the possibility
of sharing some of the expense. This usually means that
we find victims that have lost a large amount of money in
order to make it worthwhile for them. However, we have
occasionally prosecuted cases that fell under $500.00 which
is our threshold for felonies. We make these decisions de-
pending on the number of victims and the overall total
loss.
Thirdly, most of the defendants we have prosecuted are
first time offenders. We can offer them a deferred sentence
with monthly restitution payments under our state law.
The prospect of an actual conviction if tried by a jury ver-
sus no conviction at all if the defendant abides by the rules
of probation provide an incentive to plead guilty and take
our offer.
2) Have you faced any obstacles in your Internet Fraud
prosecutions? What were those obstacles? How did you over-
come them (if you did)? If you did not overcome them, please
explain why.
Our biggest obstacle is the fact that many potential defen-
dants do not meet our monetary threshold for a felony. We
are seeing this in all types of internet fraud activity and I
believe that state legislators need to change the statutes.
For instance, phishing schemes and spam do not necessari-
ly end up with a monetary loss and we would like to prose-
cute these as felonies under our state law. As I stated
above, we have filed charges against persons that have
defrauded Internet auction buyers for less than the threshold. I am not sure if my office could have afforded to fly witnesses into the state for their loss of $20.00 or so dollars each. We have overcome some of this by interviewing the defendant. For instance, in the case of State of Oklahoma v. Maple, we filed five misdemeanor counts only after she was Mirandized and admitted guilt to our investigators.

3) Have the Booker and Blakely decisions, and the effect those decisions had on your state sentencing guidelines, affected your ability to prosecute Internet fraud cases? If so, how? How did your office respond?

The Booker and Blakely decisions do not affect our ability to prosecute Internet fraud cases. Our sentencing guidelines are advisory with regards to these crimes. Plus, we have not tried a case to the jury yet, but if we did, the jury would recommend the sentence within the guidelines.

4) Do you have any further comments or experiences you would like to share in relation to Internet Fraud prosecutions?

The only comment I would like to make is that we need our state and federal laws revised regarding the monetary loss threshold in order to make it easier for prosecutors to do their jobs.

IX. CONCLUSION

There is no quick fix for Internet fraud. It is here to stay and will likely only get worse. Fraudsters need to know, however, that the sheriff is “IN” when it comes to Internet fraud. Law enforcement is urged to consider some of the suggestions in this article to reduce the cost, and hence, increase the likelihood of prosecuting Internet fraud crimes. At a minimum, prosecutors ought to consider a one-time full blown prosecution for deterrent effect on would-be fraudsters. Without some hard work on the part of law enforcement, consumer confidence in the safety of the Internet will only get worse.126
