

Internet Fraud, Access Fraud, Threatening Communications, and Cyberstalking

By John Arsenault and Suresh Sampath

Internet Fraud

The internet has opened the door to global commerce, bringing a world of goods and services to anyone with a credit card number. The increased reliance on the credit card system has led to the growth of crimes that take advantage of the medium. Before the ‘pump and dump’ stock and foreign money scams of the modern internet, criminals used fax machines to push stocks they were attempting to manipulate, or to send accidental faxes from high-ranking foreign government officials. The crimes of the new millennium will continue to involve theft of property, only through more anonymous means. In the United States alone, losses related to internet fraud increased from 68 million dollars in 2004 to over 198 million dollars in 2006.¹ To combat the growth in internet fraud, prosecutors rely on the federal wire fraud statute.

The governing statute for wire, television, or radio fraud can be found in Title 18 of the U.S. Code.² The elements of the statute require intent to commit fraud, for the purpose of executing a scheme that includes a material deception, while using radio, television or wire signals, that results in loss of money or property, while in interstate commerce.³ The wire fraud statute has been called a stop-gap solution to prosecuting novel forms of fraud, and has been used until

¹ 2006 Annual Internet Crime Report, Internet Crime Complaint Center, http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf (last visited 02/10/08);

² 18 U.S.C. § 1343 (2004).

³ *Id.*

Congress legislated more specific fraud laws.⁴ The wire fraud statute is even referred to by some as the prosecutor's "secret weapon."⁵

Internet fraud includes the most familiar type of internet crimes such as business opportunity fraud, auction fraud, charity fraud, and investment fraud. Auction fraud and variations thereof are the most commonly reported types of internet fraud in the United States.⁶ However, the numbers of higher-value internet fraud schemes have been increasing as recipients are increasingly inundated with high-value business opportunity scheme emails or other stories of foreign royalty needing to transfer large sums of money. While less common than auction fraud, business opportunity fraud victims often lose more substantial sums than auction fraud victims because senders request the victim to transfer at least several hundred dollars to receive the promised gain. Investment fraud involves using the internet to artificially manipulate the value of a stock or other commodity by either causing the short-term value to raise or fall while profiting from the change. Investment fraud can occur in the form of spam emails sent to hundreds of thousands of recipients on a given day, or posting misrepresentations on an internet message board related to a stock's performance.

The federal wire fraud statute has its limitations however. As technological changes lead to changes in how fraud is committed, the laws governing fraud also need to adapt to give prosecutors the tools they need to combat these crimes. Parties that surreptitiously gain access to a victim's credit card information aren't necessarily causing loss to money or property. While

⁴ Marissa Pezo, *Mail and Wire Fraud*, 44 AM. CRIM L. REV. 745, 746 (2007).

⁵ *Id.*

⁶ 2006 Annual Internet Crime Report, *supra* note 1; auction fraud accounts for 44.9% of total reported internet fraud, while non-delivery of goods is 19.0%. *Id.*

certain activities such as possessing or intercepting an unauthorized credit card number do not necessarily violate the wire fraud statute, the newer federal access device statute make certain activities illegal that might not otherwise violate the wire fraud statute.⁷

Access Device Fraud

An access device is a medium to conduct financial transactions, business, or access an account. The access device statute prohibits a number of activities that deal with accessing, intercepting, transmitting, selling, or possessing any information that allows unauthorized access to a financial account.⁸ Credit and debit cards are commonly used access devices because they permit consumers access to financial transactions or account information. Confidence in the credit card system is essential to its growth as a medium providing secure financial transactions in global commerce. Laws protecting access devices are thus increasingly important to protecting global commerce.⁹

Prohibited activities include knowingly, and with intent to defraud, production use, or trafficking counterfeit access devices.¹⁰ Also prohibited is use of a device during any one-year period, and aggregating a monetary value exceeding \$1000 while using the device.¹¹ Even possession of more than fifteen access devices can violate the statute.¹²

⁷ 18 U.S.C. 1029 (2004).

⁸ 18 U.S.C. § 1029(a) (2004).

⁹ JERRY IANNACCI, ACCESS DEVICE FRAUD AND RELATED FINANCIAL CRIMES 7 (1999).

¹⁰ 18 U.S.C. § 1029(a)(1) (2004).

¹¹ 18 U.S.C. § 1029(a)(2) (2004).

¹² 18 U.S.C. § 1029(a)(3) (2004).

The term access device is defined broadly in the statute, and includes any number of devices that allow access to obtain money, goods, services, or anything of value, or that can be used to initiate a transfer of funds.¹³ Common access devices include credit card numbers, PIN numbers, telecommunications devices, computers, and more. The statute also includes the catch-all broad term “any means of account access.” The catch-all term can be used to prosecute access device fraud involving biometric technology, or bar code identification machines.

The access device fraud statute has been applied to forms of fraud that wouldn’t normally qualify using the federal wire fraud statute. In 2005, a Georgia man pled guilty to access device fraud and conspiracy to commit access device fraud for creating bar codes and replacing retail bar codes with the fraudulent bar codes at substantially lower prices than offered by the retailer.¹⁴ The conspirators would then return the purchased items in exchange for in-store credit, which was later sold online or used for personal enrichment.¹⁵ Also, a New Jersey man pled guilty in 2006 to access device fraud for using a credit skimmer to acquire consumer credit card numbers from a local gas station that employed him.¹⁶ Although these are just two examples, prosecutions similar to these have only increased across the United States in the last ten years.

The access device fraud statute has provided to law enforcement additional tools to combat the novel and ever-changing forms of fraud emerging in the twenty-first century. As the internet

¹³ 18 U.S.C. § 1029(a) (2004).

¹⁴ Duluth Man Pleads Guilty to Access Device Fraud Against Home Depot and Lowe’s, District of Northern Georgia U.S. Attorney’s Office Press Release, <http://www.usdoj.gov/usao/gan/press/2005/03-24-2005.html> (last visited Feb. 10, 2007).

¹⁵ *Id.*

¹⁶ Gas Station Attendant at a New Jersey Turnpike Rest Stop Admits Fraudulently Obtaining Patrons' Credit Card Account Numbers, District of N.J. U.S. Attorney’s Office Press Release, http://www.usdoj.gov/usao/nj/press/files/acev0525_r.htm (last visited Feb. 10, 2007).

grows and changes, fraud will also change to adapt to consumer awareness. Enforcing laws against access device fraud will continue to strengthen consumer confidence in the credit card system as a medium, and will help protect the integrity of the world's global financial transaction system.

Threatening Communications

Congress has addressed the issue of threatening communications in Interstate commerce by passing 18 U.S.C. 875.¹⁷ The various subsections of the statute cover a number of different but related crimes. Subsection (a) deals with communications to extort related to the release of a kidnapped person.¹⁸ Subsection (b) deals with threats to extort.¹⁹ Subsection (c) covers generally threatening communications which threaten bodily harm.²⁰ Subsection (d) covers extortion in relation to the communication of threats to injury to property or reputation.²¹ Three issues which have been raised in the courts are issue of interstate commerce and the issue of intent and the issue of what is a threat.

¹⁷ 18 U.S.C. 875.

¹⁸ 18 U.S.C. 875(a)

¹⁹ 18 U.S.C. 875(b)

²⁰ 18 U.S.C. 875(c)

²¹ 18 U.S.C. 875(d)

Interstate Commerce

A communication need not be made for the purposes of commerce or business to qualify as a communication in interstate commerce.²² The Holder Court held that the use of ‘the nation’s vast network of telephone lines’ constituted such interstate commerce.²³

A communication which travels out of state and back to an intrastate recipient is a communication in interstate commerce for the purposes of federal jurisdiction.²⁴ In *Kammersell*, the defendant sent a text messaged bomb threat from Utah to his girlfriend’s work computer in Ogden Utah by way of an AOL communications center in Virginia.²⁵ The Circuit held that this was a communication in interstate commerce saying that the plain language of the statute supported this view.²⁶

Intent

The prosecution, in a 18 U.S.C. 875(c) case need only prove that the defendant intended to make the communication and knew the meaning of the words.²⁷ In *Morales*, the defendant told a girl in Washington that he was going to shoot students at his Texas high school.²⁸ On appeal, the 5th Circuit considered whether the prosecution was required to prove specific intent to threaten, and

²² *U.S. v. Holder*, 302 F.Supp 296, 298 (D.C. Mont. 1969).

²³ *Id.*

²⁴ *See, U.S. v. Kammersell*, 196 F.3d 1137 (10th Cir. 1999)

²⁵ *Id.* at 1137.

²⁶ *Id.* at 1139.

²⁷ *U.S. v. Morales*, 272 F.3d 284, 287 (5th Cir. 2001)

²⁸ *Id.* at 285-86

if not, what intent exactly they had to prove.²⁹ The 5th Circuit after finding the statute contemplated general and not specific intent said, “ Prosecution under § 875(c) requires proof that the threat was made knowingly and intentionally.”³⁰ The 5th Circuit further said, “A threat is knowingly made if the maker of it comprehends the meaning of the words uttered by him.”³¹ Thus, the prosecution need only show that the defendant is aware of the meaning of the words he allegedly communicates, and that he did in fact intentionally communicate them. The prosecution is not required to prove that the defendant subjectively intends a threat.

Threat

In order to separate protected speech from a ‘true threat’, Courts apply an objective standard, whether the recipient of the communication would reasonably perceive a defendant’s communication as threatening bodily harm.

In *U.S. v. Alkhabaz*, the defendant posted stories depicting sexual violence to a usenet group.³² One of these stories involved the torture, rape, and murder of a young woman who shared the same name as one of the defendant’s classmates at the University of Michigan.³³ Some time after this, the defendant and a friend exchanged email messages expressing an interest in sexual violence.³⁴

²⁹ *Id.* at 287

³⁰ *Id.*

³¹ *Id.*

³² *U.S. v. Alkhabaz*, 104. F.3d 1492, 1493 (6th Cir. 1997)

³³ *Id.*

³⁴ *Id.*

The defendant was arrested under 18 U.S.C. 875 for sending threatening interstate communications.³⁵ The District Court dismissed the indictment against the defendant, saying that his stories and messages did not constitute true threats and were protected speech.³⁶ The government appealed the dismissal of the indictment.³⁷

The 6th Circuit saw the potential for the statute to sweep too broadly and impermissibly sweep in protected speech and articulated a standard to separate protected speech from a ‘true threat’ that would be the subject of the 18 U.S.C. 875 statute.³⁸ The Court held that to constitute a “communication containing a threat” under Section 875(c), “a communication must be such that a reasonable person (1) would take the statement as a serious expression of an intention to inflict bodily harm (the mens rea), and (2) would perceive such expression as being communicated to effect some change or achieve some goal through intimidation (the actus reus).”³⁹

In *Morales*, the Court phrased a nearly identical standard. The 5th Circuit in *Morales* said “[a] communication is a threat if in its context it would have a reasonable tendency to create apprehension that its originator will act according to its tenor.”⁴⁰ The 5th Circuit further explained that to distinguish political hyperbole from a true threat, “a fact finder must determine that the recipient of the in-context threat reasonably feared it would be carried out.”⁴¹

³⁵ Id.

³⁶ Id.

³⁷ Id.

³⁸ Id. at 1494-95

³⁹ Id. at 1495.

⁴⁰ *Morales*, 272 F.3d at 287.

⁴¹ Id.

Thus, the courts, when deciding whether a communication is a threat, focus on the reasonable recipient rather than the subjective motivations of the sender.

There have been several other issues related to 18 U.S.C. 875 worth mentioning. First, the prosecution need not prove that the sender intended to make the communication in interstate commerce.⁴² Second, the threat must involve bodily injury to a person, although it need not be a specific person.⁴³ Finally, the general intent cases seem to apply only to 875(c). In *U.S. v. Heller*, the court held in a prosecution under §875(a), the prosecutor was required to prove subjective intent to extort.”⁴⁴

Cyberstalking

In response to the highly publicized murder of actress Rebecca Shaeffer, Congress enacted 18 U.S.C. 2261A as part of the Violence Against Women Act of 1994.⁴⁵ The statute allows prosecution of “Whoever . . . [uses] any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury to [a person, a member of the immediate family of that person, or a spouse or intimate partner of that person.]”⁴⁶

⁴² *U.S. v. Darby*, 37 F.3d 1059, 1067 (4th Cir. 1994)

⁴³ *U.S. v. DeAndino*, 958 F.2d 146, 148 (6th Cir. 1992).

⁴⁴ *U.S. v. Heller*, 579 F.2d 990, 995 (6th Cir. 1978).

⁴⁵ A previous Cybercrime Powerpoint Presentation

⁴⁶ 18 U.S.C. 2261A.

The constitutionality of the statute has been challenged on a number of occasions and been upheld. *U.S. v. Bowker* was such a case, where the defendant made overbreadth and vagueness challenges.⁴⁷ The 6th Circuit rejected both challenges.⁴⁸ The Court that a defendant would reasonably know what conduct was proscribed.⁴⁹ The court also found words like harass and intimidate to be words of common understanding.⁵⁰

In *U.S. v. Bell*, the 9th circuit suggested that a single act would not be an actionable offense under the statute, and that the term “course of conduct” in the statute meant a pattern of conduct comprised of two or more acts.⁵¹

⁴⁷ *U.S. v. Bowker*, 372 F.3d 365, 378-84 (6th Cir. 2004)

⁴⁸ *Id.*

⁴⁹ *Id.* at 380-81.

⁵⁰ *Id.* at 381.

⁵¹ *U.S. v. Bell*, 303 F.3d 1187, 1192 (9th Cir. 2002)