Intro to Law
Cyber Law
Unit Textbook
UNIT OUTLINE

Cyber Crime Against Persons and Property
A. Cyber Consumer Fraud
   1. Online Auction Fraud
   2. Online Retail Fraud
B. Cyber Theft
   1. Identity Theft
   2. The Low Cost of Black Market Data
   3. Phishing
   4. Vishing
   5. Employment Fraud
C. Cyberstalking

Cyber Crime in the Business World
A. Credit Card Crime on the Web
B. Hackers
C. Hacking and Cyberterrorism
D. Pirating Intellectual Property Online

The Spread of Spam
A. State Regulation of Spam
B. The Federal CAN-SPAM Act
C. The U.S. Safe Web Act

Cyber Crime Against the Community—Gambling in Cyberspace
A. Legal Confusion Over Online Gambling
B. Congress Takes Action
C. Prosecuting Cyber Crimes
D. The Computer Fraud and Abuse Act
INTRODUCTION

One day, fashion retailer Forever 21 announced that someone had stolen account details of nearly 100,000 credit and debit cards via the Internet. Another day, the Best Western Hotel Group admitted that the payment details of 8 million guests had also been stolen via the Internet. On any given day, if you connect an unprotected computer to the Internet, within four minutes, that computer will be hacked and taken over by a remote network, just like tens of millions of other computers around the globe. The Internet provides enormous benefits by linking people and businesses around the world, but as these examples suggest, the Internet can also be a dangerous place. Certainly, one of the reasons that crime has flourished on the Internet is the difficulty in regulating something that has a global presence but no physical place.

A number of the previously discussed white-collar crimes, such as fraud, embezzlement, and the theft of intellectual property, are now committed with the aid of computers and are thus considered computer crimes. In this unit, we will be using a broader term, CYBER CRIME, to describe any criminal activity occurring via a computer in the virtual community of the Internet. Most cyber crimes are not new crimes; rather, they are existing crimes in which the Internet is the instrument of wrongdoing.

It is very difficult, if not impossible, to tell how much cyber crime actually takes place. Often, people never know that they have been the victims of this type of criminal activity. Furthermore, businesses sometimes fail to report such crimes for fear of losing customer confidence. Nonetheless, by June 2007 the Internet Crime Complaint Center, operated as a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center, had received its one-millionth complaint after only seven years of operation. Furthermore, the United States appears to have gained the unwanted distinction of being the world's leader in cyber crime, with more than one-third of all global computer attacks originating in this country.

CYBER CRIME AGAINST PERSONS AND PROPERTY

Perpetrators of cyber crimes are often aided by certain aspects of the Internet, such as its ability to cloak the user's identity and its effectiveness as a conduit for transferring—or stealing—large amounts of information very quickly. The challenge for the courts is to apply traditional laws, which were designed to protect persons from physical harm or to safeguard their physical property, to crimes committed in cyberspace. Here, we look at several types of activity that constitute updated crimes against persons and property—cyber consumer fraud, cyber theft, and cyberstalking.

CYBER CONSUMER FRAUD

The expanding world of e-commerce has created many benefits for consumers. It has also led to some challenging problems, including fraud conducted via the Internet. As previously discussed, fraud is any misrepresentation knowingly made with the intention of deceiving another and on which a reasonable person would and does rely to their detriment. CYBER FRAUD, then, is fraud committed over the Internet.
Frauds that were once conducted solely by mail or phone can now be found online, and new technology has led to increasingly creative ways to commit fraud. Some perpetrators of fraud even look for victims on social networks and dating sites. They persuade their victims to wire funds to their supposed love interests to pay for travel for meetings (which never occur)—a type of fraud that is rarely reported to the FBI.

Sometimes, Internet fraud is just an electronic version of frauds that used to be perpetrated by sending letters. Perhaps the longest running Internet fraud is the "Nigerian letter fraud scam." In this swindle, individuals are sent e-mails promising them a percentage if they will send funds to help fictitious officials from the African country transfer millions of nonexistent dollars to Western banks. The scam was recently updated to reflect current events, with con artists sending out e-mails asking for financial help in retrieving the fortune of a loved one or associate who had perished as a result of the conflicts in Iraq and Afghanistan.

No one knows the full extent of cyber fraud, but indications are that it is a very common form of cyber crime. In 2009, the Internet Crime Complaint Center received more than 200,000 complaints of online crime involving losses of hundreds of millions of dollars. Fraud web sites increased from fewer than one hundred at the beginning of 2006 to more than ten thousand by 2009. The two most widely reported forms of cyber crime are auction fraud and retail fraud.

**ONLINE AUCTION FRAUD**

In its most basic form, online auction fraud is a simple process. A person puts up an expensive item for auction, on either a legitimate or a fake auction site, and then refuses to send the product after receiving payment. Or, as a variation, the wrongdoer may provide the purchaser with an item that is worth less than the one offered in the auction. The larger online auction sites such as eBay try to protect consumers against such schemes by providing warnings about deceptive sellers or offering various forms of insurance. The nature of the Internet, however, makes it nearly impossible to completely block fraudulent auction activity. Because users can assume multiple identities, it is very difficult to pinpoint a fraudulent seller—they will simply change their screen name with each auction.

**ONLINE RETAIL FRAUD**

Somewhat similar to online auction fraud is online retail fraud, in which consumers pay directly (without bidding) for items that are never delivered. Because most online consumers will purchase items only from reputable, well known sites such as Amazon.com, criminals have had to take advantage of some of the complexities of cyberspace to lure in unsuspecting customers. Again, though determining the actual extent of online sales fraud is difficult, anecdotal evidence suggests that it is a substantial problem.

**CYBER THEFT**

In cyberspace, thieves are not subject to the physical limitations of the real world. A thief can steal data stored in a networked computer with network access from anywhere on the globe. Only the speed of the connection and the thief's computer equipment limit the quantity of data that can be stolen.
IDENTITY THEFT

Not surprisingly, there has been an increase in IDENTIFY THEFT, which occurs when the wrongdoer steals a form of identification—such as a name, date of birth, or Social Security number—and uses the information to access the victim's financial resources. This crime existed to a certain extent before widespread use of the Internet. For instance, thieves would steal calling card numbers by watching people using public telephones, or they would rifle through garbage to find bank account or credit card numbers. The identity thief would then use the calling card or credit card number or withdraw funds from the victims account until the theft was discovered.

The Internet has provided even easier access to private data. Frequent Web surfers surrender a wealth of information about themselves without knowing it. Many Web sites use cookies to collect data on those who visit their sites. The data can include the areas of the site the user visits and the links on which the user clicks. Furthermore, Web browsers often store information such as the consumer's name and e-mail address. Finally, every time a purchase is made online, the item is linked to the purchaser's name, allowing web retailers to amass a database of who is buying what.

Identity theft criminals have devised even more ingenious methods. Recently, many corporate executives received fake subpoenas from a nonexistent federal district court in San Diego, commanding them to appear before a grand jury. The e-mail contained a link that could be clicked to view the entire subpoena. When the executive clicked on the link, however, malicious software was downloaded. It recorded all keystrokes on the computer and sent the data to the cyber crooks.

THE LOW COST OF BLACK MARKET DATA

As many consumers are discovering, any information that can be collected can be stolen. About 3 percent of all American households—3.6 million in total—report that at least one member has been the victim of a recent identity theft. In reality, the cyber criminals who steal people's identities normally do not use them. Instead, they sell the information on the Internet. Several hundred web sites sell black market private data, most of them hosted on Russian servers and out of reach of U.S. authorities.

Competition among those who traffic in the tools of identity theft has become so fierce that the price of the private information has plummeted. Among identity thieves, stolen credit card numbers are sold for as little as $1 each, while a complete identity, including date of birth, bank account, and government issued identification numbers, can be purchased for less than $15.
PHISHING

A distinct form of identity theft known as PHISHING has added a different wrinkle to the practice. In a phishing attack, the perpetrators "fish" for financial data and passwords from consumers by posing as a legitimate business such as a bank or credit card company. The phisher sends an e-mail asking the recipient to update or confirm vital information, often with the threat that an account or some other service will be discontinued if the information is not provided. Once the unsuspecting individual enters the information, the phisher can use it to masquerade as that person or to drain their bank or credit account. For example, customers of Wachovia Bank (bought by Wells Fargo) received official looking e-mails telling them to type in personal information on a web form to complete a mandatory installation of a new Internet security certificate. Of course, the web site was bogus. People who filled out the forms had their computers infected with a Trojan horse that funneled their data to a computer server; the cyber criminals then sold the data. In another scheme, e-mails purportedly from the Internal Revenue Service were sent to a number of small business owners, among others. These e-mails requested bank account information for direct deposit of federal tax refunds, which of course never came.

VISHING

When phishing involves some form of voice communication, the scam is known as VISHING. In one variation, the consumer receives an e-mail saying there is a problem with an account and that she or he should call a certain telephone number to resolve the problem. Sometimes, the e-mail even says that a telephone call is being requested so that the recipient will know that this is not a phishing attempt. Of course, the goal is to get the consumer to divulge passwords and account information during the call. In one scheme, e-mails seemingly from the Federal Bureau of Investigation asked recipients to call a special telephone number and provide account information. Vishing scams use Voice over Internet Protocol (VoIP) service, which enables telephone calls to be made over the Internet. Such calls are inexpensive and enable scammers to easily hide their identity.

EMPLOYMENT FRAUD

Cyber criminals also look for victims at online job-posting sites. Claiming to be an employment officer in a well-known company, the criminal sends bogus e-mail messages to job seekers. The message asks the unsuspecting job seeker to reveal enough information to allow for identity theft. The job site Monster.com had to ask all of its users to change their passwords because cyber thieves had broken into its databases to steal user identities, passwords, and other data. The theft of 4.5 million users' personal information from Monster.com was one of Britain's largest cyber theft cases. As the recession dragged on into 2010 and the unemployment rate continued to rise, opportunities for employment fraud were also on the increase.
CYBERSTALKING

California passed the first antistalking law in 1990, in response to the murders by stalkers of six women—including Rebecca Shaeffer, a television star. The law made it a crime to harass or follow a person while making a "credible threat" that puts the person in reasonable fear for their safety or the safety of that person's immediate family. Almost every state and the federal government followed with their own antistalking legislation.

By the mid-1990s, it had become clear that these laws, most of which required a "physical act," such as following the victim, were insufficient. They could not protect persons against CYBERSTALKING, in which the perpetrator uses the Internet, e-mail, or some other form of electronic communication to carry out the harassment. In 1998, California, once again leading the way, amended its stalking statute to include threats made through an electronic communication device. Today, forty-five states and the federal government have their own legislation that makes cyberstalking a crime.

Although no trustworthy statistics exist, most experts assume that cyberstalking is more commonplace than physical stalking. While it takes a great deal of effort to physically stalk someone, it is relatively easy to harass a victim with electronic messages. Furthermore, the possibility of personal confrontation may discourage a physical stalker from closely pursuing the victim. This disincentive is irrelevant in cyberspace. Finally, physical stalking requires that the stalker and the victim be in the same geographic location. A cyberstalker can carry on the harassment from anywhere on the planet, as long as they have access to a computer.

CYBER CRIME IN THE BUSINESS WORLD

Just as cyberspace can be a dangerous place for consumers, it presents a number of hazards for businesses that wish to offer their services on the Internet. The same circumstances that enable companies to reach a wide number of consumers also leave them vulnerable to cyber crime. The Federal Bureau of Investigation (FBI) estimates that all types of computer crime do about $400 billion in damage to U.S. businesses each year.

CREDIT CARD CRIME ON THE WEB

In the previous section, credit card theft was mentioned in connection with identity theft. An important point to note, however, is that stolen credit cards are much more likely to hurt merchants and credit card issuers (such as banks) than the consumer from whom the card or card number has been appropriated. In most situations, the legitimate holders of credit cards are not held responsible for the costs of purchases made with a stolen number. That means the financial burden must be borne either by the merchant or by the credit card company. Most credit card issuers require merchants to cover the costs—especially if the address to which the goods are sent does not match the billing address of the credit card. Companies take further risks by storing their customers' credit card numbers. In doing so, companies provide quicker service; the consumer can make a purchase by providing a code or clicking on a particular icon without entering the lengthy card number. These electronic warehouses are, however, quite tempting to cyber thieves. Several years ago, an unknown person was able to gain access to computerized records at CardSystems Solutions, a company in Tucson, Arizona, that processes credit card transactions for small Internet businesses. The breach exposed 40 million credit card numbers.
HACKERS

The person who broke into Card Systems' database to steal the credit card numbers was a hacker. A hacker is someone who uses one computer to break into another. The danger posed by hackers has increased significantly because of botnets, or networks of computers that have been appropriated by hackers without the knowledge of their owners. A hacker will secretly install a program on thousands, if not millions, of personal computer "robots," or "bots," that allows them to forward transmissions to an even larger number of systems.

Botnets are one of the latest forms of malware, a term that refers to any program that is harmful to a computer or, by extension, a computer user. A worm, for example, is a software program that is capable of reproducing itself as it spreads from one computer to the next. In 2009, a computer worm called "Conficker" spread to more than a million computers around the world in a three-week period. It was transmitted to some computers through the use of Facebook and Twitter. This worm also infected servers and any device plugged into an infected computer via a USB port, such as iPods and pen drives. Security advisers at F-Secure determined that any person or group controlling Conficker could engage in a variety of criminal activities on an unprecedented scale. Microsoft developed a clean-up removal tool for infected computers and servers. The only problem is that Conficker blocks Internet traffic attempting to access the tool.

A virus, another form of malware, is also able to reproduce itself, but must be attached to an infected host file to travel from one computer network to another. Hackers are now capable of corrupting banner ads that use Adobe's Flash Player. When an Internet user clicks on the banner ad, a virus is installed. Worms and viruses can be programmed to perform a number of functions, such as prompting host computers to continually crash and reboot, or otherwise infect the system.

Though the hackers and other techies who create worms and viruses are often romanticized as youthful rebels, they cause significant damage. A destructive virus can overload a company's computer system, making e-mail and many other functions impossible until it is cleaned out of the system. This cleansing process can cost between $100,000 and $5 million per day, depending on the size of the computer system affected. Experts estimate that about ten thousand viruses and worms are spreading through the Internet at any given time, with five hundred new ones being created every month. The Computer Crime and Security Survey polled more than six hundred U.S. companies and large government institutions and found that 52 percent had suffered security breaches through computer-based means.

HACKING AND CYBERTERRORISM

Hackers who break into computers without authorization often commit cyber theft. Sometimes, though, their principal aim is to prove how smart they are by gaining access to others’ password-protected computers and causing problems. Cyberterrorists are hackers who, rather than trying to gain attention, strive to remain undetected so that they can exploit computers for a serious impact. Just as real terrorists destroyed the World Trade Center towers and a portion of the Pentagon in September 2001, cyberterrorists might explode "logic bombs" to shut down central computers. Such activities can pose a danger to national security. In 2009, Chinese and Russian cyber spies reportedly hacked into our nation's electrical power grid and left behind software that could be used to disrupt the system during a war or crisis. U.S. intelligence officials were concerned that the hackers might try to hijack electrical facilities or a nuclear power plant via the Internet.
Cyberterrorists as well as hackers may target businesses. The goals of a hacking operation might include a wholesale theft of data, such as a merchant's customer files, or the monitoring of a computer to discover a business firm's plans and transactions. A cyberterrorist might also want to insert false codes or data. For example, the processing control system of a food manufacturer could be changed to alter the levels of ingredients so that consumers of the food would become ill. A cyberterrorist attack on a major financial institution such as the New York Stock Exchange or a large bank could leave securities or money markets in flux and seriously affect the daily lives of millions of citizens. Similarly, any prolonged disruption of computer, cable, satellite, or telecommunications systems due to the actions of expert hackers would have serious repercussions on business operations—and national security—on a global level. Computer viruses are another tool that can be used by cyberterrorists to cripple communications networks.

**PIRATING INTELLECTUAL PROPERTY ONLINE**

Intellectual property consists of goods and services that result from intellectual, creative processes. The government provides various forms of protection for intellectual property such as copyrights and patents. These protections ensure that a person who writes a book or a song or creates a software program is financially rewarded if that product is sold in the marketplace. Intellectual property such as books, films, music, and software is vulnerable to piracy—the unauthorized copying and use of the property. In the past, copying intellectual products was time consuming, and the quality of the pirated copies was clearly inferior. In today's online world, however, things have changed. Simply clicking a mouse can now reproduce millions of unauthorized copies, and pirated duplicates of copyrighted works obtained via the Internet are the same as the original, or close to it. The Business Software Alliance estimates that 35 percent of all business software is pirated, costing software makers more than $5 billion per year. The International Federation of the Phonographic Industry believes that 37 percent of purchased CDs have been pirated. In the United States, digital pirates can be prosecuted under the No Electronic Theft Act and the Digital Millennium Copyright Act. In 2005, the entertainment industry celebrated the United States Supreme Court's decision in Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd. The ruling provided film and music companies with the ability to file piracy lawsuits against Internet file sharing web sites that market software used primarily to illegally download intellectual property. By 2009, the recording industry announced that it would no longer file lawsuits against most individuals who pirate music online. The music industry continues to look for a business model that will allow it to make profits in spite of widespread pirating.
THE SPREAD OF SPAM

Businesses and individuals alike are targets of SPAM, or unsolicited junk e-mails that flood virtual mailboxes with advertisements, solicitations, and other messages. Considered relatively harmless in the early days of the Internet's popularity, by 2009 spam accounted for more than 73 percent of all e-mails. Far from being harmless, the unwanted files can wreak havoc on business operations.

STATE REGULATION OF SPAM

In an attempt to combat spam, thirty-six states have enacted laws that prohibit or regulate its use. Many state laws that regulate spam require the senders of e-mail ads to instruct the recipients on how they can opt out of further e-mail ads from the same sources. For instance, in some states an unsolicited e-mail ad must include a toll-free phone number or return e-mail address through which the recipient can contact the sender to request that no more ads be e-mailed. Responding to complaints from overwhelmed constituents, a number of jurisdictions have started to pass antispamming laws.

THE FEDERAL CAN-SPAM ACT

In 2003, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, which took effect on January 1, 2004. The legislation applies to any "commercial electronic mail messages" that are sent to promote a commercial product or service. Significantly, the statute preempts state antispam laws except for those provisions in state laws that prohibit false and deceptive e-mailing practices. Generally, the act permits the use of unsolicited commercial e-mail but prohibits certain types of spamming activities, including the use of a false return address and the use of false, misleading, or deceptive information when sending e-mail. The statute also prohibits the use of "dictionary attacks"—sending messages to randomly generated e-mail addresses and the "harvesting" of e-mail addresses from web sites with specialized software. In 2007, federal officials arrested Robert Alan Soloway, considered one of the world's most prolific spammers. Because Soloway had been using botnets to send out hundreds of millions of unwanted e-mails, he was charged under antiidentity theft laws for the appropriation of other people's domain names, among other crimes. In 2008, Soloway, known as the "Spam King," pleaded guilty to mail fraud and failure to pay taxes. Arresting prolific spammers, however, has done little to curb spam, which continues to flow at a rate of 70 billion messages per day.

THE U.S. SAFE WEB ACT

After the CAN-SPAM Act of 2003 prohibited false and deceptive e-mails originating in the United States, spamming from servers located in other nations increased. These crossborder spammers generally were able to escape detection and legal sanctions because the Federal Trade Commission (FTC) lacked the authority to investigate foreign spamming. Congress sought to rectify the situation by enacting the U.S. Safe Web Act of 2006 (also known as the Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act). The act allows the FTC to cooperate and share information with foreign agencies in investigating and prosecuting those involved in Internet fraud and deception, including spamming, spyware, and various Internet frauds. It also provides Internet service providers (ISPs) with a "safe harbor" (immunity from liability) for supplying information to the FTC concerning possible unfair or deceptive conduct in foreign jurisdictions.
One of the greatest challenges in cyberspace is how to enforce laws governing activities that are prohibited under certain circumstances but are not always illegal. Such laws generally reflect the will of the community, which recognizes behavior as acceptable under some circumstances and unacceptable under others. While it is legal in many areas to sell a pornographic video to a fifty-year-old, it is never legal to sell the same item to a fifteen-year-old. Similarly, placing a bet on a football game with a bookmaker in Las Vegas, Nevada, is legal, but doing the same thing with a bookmaker in Detroit, Michigan, is not. Of course, in cyberspace it is often impossible to know whether the customer buying porn is aged fifty or fifteen, or if the person placing the bet is from Las Vegas or Detroit.

**LEGAL CONFUSION OVER ONLINE GAMBLING**

In general, gambling is illegal. All states have statutes that regulate gambling—defined as any scheme that involves the distribution of property by chance among persons who have paid valuable consideration for the opportunity to receive the property. In some states, certain forms of gambling, such as casino gambling or horseracing, are legal. Many states also have legalized state-operated lotteries, as well as lotteries, such as bingo, conducted for charitable purposes. A number of states also allow gambling on Native American reservations. In the past, this mixed bag of gambling laws has presented a legal quandary: Can citizens in a state that does not allow gambling place bets to a website located in a state that does? After all, states have no constitutional authority over activities that take place in other states. Complicating the problem was the fact that many Internet gambling sites are located outside the United States in countries where Internet gambling is legal, and no state government has authority over activities that take place in other countries. Property, including funds, involved in illegal gambling can be seized under federal law through a civil forfeiture action. A defendant, however, may assert a defense to reclaim the property.

**CONGRESS TAKES ACTION**

In 2006, Congress, concerned about money laundering stemming from online gambling, the problem of addiction, and underage gambling, passed legislation that greatly strengthened efforts to reduce online gaming. The Unlawful Internet Gambling Enforcement Act (UIGEA) of 2006 cut off the money flow to Internet gambling sites by barring the use of electronic payments, such as credit card transactions, at those sites. The reaction by the online gambling industry was swift and dramatic: after the passage of this bill, many of the foreign-based companies suspended the use of real money on the web sites serving the United States. Without the incentive of playing for cash, the sites have lost their appeal for most clients. In 2005, approximately 12 million Americans wagered $6 billion online, but as soon as the law was enacted, those numbers plummeted.
PROSECUTING CYBER CRIMES

The location of cyber crime (cyberspace) has raised new issues in the investigation of crimes and the prosecution of offenders. A threshold issue is, of course, jurisdiction. A person who commits an act against a business in California, where the act is a cyber crime, might never have set foot in California but might instead reside in New York, or even in Canada, where the act may not be a crime. If the crime was committed via e-mail, the question arises as to whether the e-mail would constitute sufficient "minimum contacts" for the victim's state to exercise jurisdiction over the perpetrator. Identifying the wrongdoer can also be difficult. Cyber criminals do not leave physical traces, such as fingerprints or DNA samples, as evidence of their crimes. Even electronic "footprints" can be hard to find and follow. For instance, e-mail may be sent through a remailer—an online service that guarantees that a message cannot be traced to its source. For these reasons, laws written to protect physical property are difficult to apply in cyberspace. Nonetheless, governments at both the state and federal levels have taken significant steps toward controlling cyber crime, both by applying existing criminal statutes and by enacting new laws that specifically address wrongs committed in cyberspace.

THE COMPUTER FRAUD AND ABUSE ACT

Perhaps the most significant federal statute specifically addressing cyber crime is the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (commonly known as the Computer Fraud and Abuse Act, or CFAA). This act, as amended by the National Information Infrastructure Protection Act of 1996, provides, among other things, that a person who accesses a computer online, without authority, to obtain classified, restricted, or protected data, or attempts to do so, is subject to criminal prosecution. Such data could include financial and credit records, medical records, legal files, military and national security files, and other confidential information in government or private computers. The crime has two elements: accessing a computer without authority and taking the data. This theft is a felony if it is committed for a commercial purpose or for private financial gain, or if the value of the stolen data (or computer time) exceeds $5,000. Penalties include fines and imprisonment for up to twenty years. A victim of computer theft can also bring a civil suit against the violator to obtain damages, an injunction, and other relief.