UNIT – II

Internet Fraud

- **Investment Fraud**
- **Auction Fraud**
- **Identity Theft**

Investment Fraud

Investment Offers

Investment offers are nothing new. Even some legitimate stockbrokers make their living by cold calling, the process of simply calling people (perhaps from the phone book) and trying to get them to invest in a specific stock.

Investment offers floods inbox on a daily basis, some of these email notifications entice you to become directly involved with a particular investment plan.

Common Schemes

One of the more common schemes involves sending out an email that suggests that you can make an outrageous sum of money with a very minimal investment. Perhaps the most famous of these schemes has been the Nigerian fraud. In this scenario, an email is sent to a number of random email addresses. Each one contains a message purporting to be from a relative of some deceased Nigerian doctor or government official. The deceased person will be someone you would associate with significant social standing, thus increasing the likelihood that you would view the offer more favorably. The offer goes like this: A person has a sum of money he wishes to transfer out of his country, and for security reasons, he cannot use normal channels. He wishes to use your bank account to "park" the funds temporarily. If you will allow him access to your account, you will receive a hefty fee. If you do agree to this arrangement, you will receive, via normal mail, a variety of very official-looking documents, enough to convince most casual observers that the arrangement is legitimate. You will then be asked to advance some money to cover items such as taxes and wire fees. Should you actually send any money, you will have lost the money you advanced and you will never hear from these individuals again.

Investment Advise

Unbiased stock advise might turn into biased stock advise. Rather than getting the advice of an unbiased expert, you may be getting a paid advertisement. This pitfall is one of the most common traps of online investment advice, more common than the blatant frauds.

Sometimes these online stock bulletins can be part of a wider scheme, often called a **pump and dump**. A classic pump and dump is rather simple. The con artist takes a stock that is virtually worthless and purchases large amounts of it. The con artist then artificially inflates the value in several ways. One common method is to begin circulating rumors on various Internet bulletin boards and chat rooms that the stock is about to go up significantly. Often it is suggested by the

trickster that the company has some new innovative product due to come out in the next few weeks. Another method is to simply push the stock on as many people as possible. The more people vying to buy a stock, the higher its price will rise. If both methods are combined, it is possible to take a worthless stock and temporarily double or triple its value.

The U.S. Securities and Exchange Commission lists several tips for avoiding such scams:[3]

- Consider the source. Especially if you are not well versed in the market, make sure you accept advice only from well-known and reputable stock analysts.
- Independently verify claims. Do not simply accept someone else's word about anything.
- Research. Read up on the company, the claims about the company, its stock history, and so forth.
- Beware of high-pressure tactics. Legitimate stock traders do not pressure customers into buying. They help customers pick stocks that customers want. If you are being pressured, that is an indication of potential problems.
- Be skeptical. A healthy dose of skepticism can save you a lot of money. Or, as the saying goes, "If it sounds too good to be true, it probably is"

Make sure you thoroughly research any investment opportunity

Auction Frauds

The U.S. Federal Trade Commission4 (FTC) lists the following four categories of online auction fraud:

- Failure to send the merchandise
- Sending something of lesser value than advertised
- Failure to deliver in a timely manner
- Failure to disclose all relevant information about a product or terms of the sale

The first category, failure to deliver the merchandise, is the most clear-cut case of fraud and is fairly simple. Once you have paid for an item, no item arrives. The seller simply keeps your money.

The second category of fraud, delivering an item of lesser value than the one advertised, can become a gray area. In some cases, it is outright fraud. The seller advertises something about the product that simply is not true. For example, the seller might advertise a signed copy of the first printing of a famous author's book but then instead ship you a fourth printing with either no autograph or one that is unverified. However, in other cases of this type of problem, it can simply be that the seller is over- zealous, or frankly mistaken. The seller might claim his baseball was signed by a famous athlete but not be aware himself that the autograph is a fraud.

The second category is closely related to the fourth item on the FTC list: failure to disclose all relevant facts about the item. For example, a book might be an authentic first printing and autographed but be in such poor physical condition as to render it worthless. This fact may or may

not be mentioned in advance by the seller. Failure to be forthcoming with all the relevant facts about a particular item might be the result of outright fraud or simply of the seller's ignorance. The FTC also lists failure to deliver the product on time as a form of fraud. It is unclear whether or not that is fraud in many cases or merely woefully inadequate customer service.

- Shill bidding: when fraudulent sellers (or their "shills") bid on the seller's items to drive up the price.

- Bid shielding: when fraudulent buyers submit very high bids to discourage other bidders from competing for the same item. The fake buyers then retract their bids so that people they know can get the item at a lower price.

- Bid siphoning :. In this scheme, the perpetrator places a legitimate item up for bid on an auction site. But then, in the ad for that item, she provides links to sites that are not part of the auction site. The unwary buyer who follows those links might find himself on an alternative site that is a "setup" to perpetrate some sort of fraud.

Identity Theft

Identity theft and *identity fraud* are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."

The advent of the Internet has made the process of stealing a person's identity even easier than it used to be. Many states now have court records and motor vehicle records online. In some states, a person's social security number is used for the driver's license number. So if a criminal gets a person's social security number, he can look up that person's driving record, perhaps get a duplicate of the person's license, find out about any court records concerning that person, and on some websites, even run the person's credit history.

Phishing

One of the more common ways to accomplish identity theft is via a technique called *phishing*, which is the process of trying to induce the target to provide you with personal information. For example, the attacker might send out an email purporting to be from a bank and telling recipients that there is a problem with their bank account. The email then directs them to click on a link to the bank website where they can log in and verify their account. However, the link really goes to a fake website set up by the attacker. When the target goes to that website and enters his information, he will have just given his username and password to the attacker.

Cyber Stalking

Cyber stalking, the term is used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

Real Cyber Stalking Cases

The following cases, also from the Department of Justice website, illustrate cases of cyber stalking. Examining the facts in these cases might help you to get an idea of what legally constitutes cyber stalking.

- In the first successful prosecution under California's new cyber stalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault. He faces up to six years in prison.
- A local prosecutor's office in Massachusetts charged a man who, using anonymous re-mailers, allegedly engaged in a systematic pattern of harassment of a co-worker, which culminated in an attempt to extort sexual favors from the victim under threat of disclosing past sexual activities to the victim's new husband.

How to Evaluate Cyber Stalking

The question becomes, how do you determine whether to take a threat seriously? The key is to look for four factors:

- **Credibility:** For a threat to be credible, there must be some reasonable expectation that it could be carried out. For example, suppose a woman in Nebraska is on an Internet discussion board and receives a general threat from another user living in Bangkok in the course of a heated debate. In this scenario, the sender very likely has no idea where the recipient lives. Indeed, because many people use screen names on the Internet, the sender may not even know the recipient's real name, gender, age, or appearance. That means this threat has a very low level of credibility. If, however, the woman in Nebraska receives a threat from the user in Bangkok ac- companied with personal information such as her address, her place of work, or a photo of her, that is a very credible threat.

- **Frequency:** Unfortunately, people often make ill-advised comments on the Internet. Often, however, a single hostile comment is just a person reacting too emotionally and too quickly online. For this reason, this type of comment is less of a concern than a pattern of threats over a period of time. Frequently, stalkers escalate their comments and threats over time, gradually building up to a point where they act violently. While there certainly may be cases in which a single threat warrants investigation, as a general rule, isolated threats are of less concern than a pattern of harassment and threats.

- **Specificity**: Specificity refers to how specific the perpetrator is regarding the nature of the threat, the target of the threat, and the means of executing the threat. Of course, it is very important for law enforcement officers to realize that real threats can sometimes be vague. Put another way, real threats aren't always specific. But specific threats are usually real. As an example, someone receiving an email saying, "You will pay for that" is less of a concern than an email containing a specific threat of a very specific type of violence, such as, "I will wait for you after work and shoot you in the head with my 9mm" along with a photo of the recipient leaving work. (The photo also makes it very credible.) This threat is specific and should be of much greater concern to law enforcement.

- **Intensity:** This refers to the general tone of the communications, the nature of the language, and the intensity of the threat. Graphic and particularly violent threats should always be taken very seriously by law enforcement. Often, when someone is simply venting or reacting emotionally, he may make statements that could be considered threatening. In these cases, however, most people make low-intensity statements, such as threatening to beat someone up. Threats such as these are of less concern than, say, a threat to dismember someone. This is because normal, nonviolent people can lose their temper and want to punch someone in the nose. But normal, nonviolent people don't usually lose their temper and want to cut someone into pieces with a chainsaw. Anytime a threat is raised to a level that is beyond what a reasonable person might say, even in a hostile situation, that threat becomes of greater concern.

Protecting Yourself Against Cyber Crime

Now that you know about the various frauds that are prevalent on the Internet and have looked at the relevant laws, you might be wondering what you can do to protect yourself. There are several specific steps you can take to minimize the chances of being the victim of Internet crime. There are also some clear guidelines on how you should handle the situation, should you become a victim.

Protecting Against Investment Fraud

To protect yourself against investment fraud, follow these guidelines:

1. Only invest with well-known, reputable brokers.
2. If it sounds too good to be true, then avoid it.
3. Ask yourself why this person is informing you of this great investment deal. Why would a complete stranger decide to share some incredible investment opportunity with you?

4. Remember that even legitimate investment involves risk, so never invest money that you cannot afford to lose.

Protecting Against Identity Theft

When the issue is identity theft, your steps are clear:

1. Do not provide your personal information to anyone if it is not absolutely necessary. This rule means that when communicating on the Internet with anyone you do not personally know, do not reveal anything about yourself—not your age, occupation, real name, anything.
2. Destroy documents that have personal information on them. If you simply throw away bank statements and credit card bills, then someone rummaging through your trash can get a great deal of personal data. You can obtain a paper shredder from an office supply store or many retail department stores for less than $20. Shred these documents before disposing of them. This rule may not seem like it is related to computer security, but information gathered through nontechnical means can be used in conjunction with the Internet to perpetrate identity theft.
3. Check your credit frequently. Many websites, including www.consumerinfo.com, allow you to check your credit and even get your beacon score for a nominal fee. I check my credit twice per year. If you see any items you did not authorize, that is a clear indication that you might be a victim of identity theft.
4. If your state has online driving records, then check yours once per year. If you see driving in- fractions that you did not commit, this evidence is a clear sign that your identity is being used by someone else. In an upcoming chapter on cyber detective work, we will explore in detail how to obtain such records online, often for less than $5.

To summarize, the first step in preventing identity theft is restricting the amount of personal information you make available. The next step is simply monitoring your credit and driving records so that you will be aware if someone attempts to use your identity.

Another part of protecting your identity is protecting your privacy in general. That task means preventing others from gaining information about you that you don't explicitly provide them. That preventive method includes keeping websites from gathering information about you without your knowledge.

Secure Browser: Many websites store information about you and your visit to their site in small files called cookies. These cookie files are stored on your machine. The problem with cookies is that any website can read any cookie on your machine—even ones that the website you are

currently visiting did not create. So, if you visit one website and it stores items like your name, the site you visited, and the time you were there, then another website could potentially read that cookie and know where you have been on the Internet. One of the best ways to stop cookies is to change your Internet settings to help reduce exposures to your privacy.

Protect against Auction Fraud

Dealing with auction fraud involves a different set of precautions; here are four good ideas.

1. Only use reputable auction sites. The most well-known site is eBay, but any widely known, reputable site will be a safer gamble. Such auction sites tend to take precautions to prevent fraud and abuse.
2. If it sounds too good to be true, don't bid.
3. Some sites actually allow you to read feedback other buyers have provided on a given seller. Read the feedback, and only work with reputable sellers.
4. When possible use a separate credit card, one with a low limit, for online auctions. That way, should your credit card be compromised, your liability is limited. Using your debit card is sim- ply inviting trouble.

Protect against Online Harassment

Online auctions can be a very good way to get valuable merchandise at low prices. However, one must exercise some degree of caution when using these services.

Protecting yourself from online harassment also has its own guidelines:

1. If you use chat rooms, discussion boards, and so forth, do not use your real name. Set up a sep- arate email account with an anonymous service, such as Yahoo!, Gmail, or Hotmail. Then use that account and a fake name online. This makes it very hard for an online stalker to trace back to you personally.
2. If you are the victim of online harassment, keep all the emails in both digital and printed format. Use some of the investigative techniques we will explore later in this book to try to identify the perpetrator. If you are successful, then you can take the emails and the information on the perpetrator to law enforcement officials.
3. Do not, in any case, ignore cyber stalking. According to the Working to Halt Online Abuse website, 19% of cyber stalking cases escalate to stalking in the real world.

It is not the intent of this chapter or of this book to make you frightened about using the Internet. I routinely use the Internet for entertainment, commerce, and informational purposes. One simply needs to exercise some caution when using the Internet.