Fraud

The crime of fraud is the act of obtaining something of value by means of deception. This is clearly an instance of a traditional crime being carried out in new and novel ways through the use of computer technology and the Internet. Internet crime schemes steal millions of dollars each year from victims and continue to plague the Internet through various methods.

Fraud can violate civil law(i.e., a fraud victim may sue the fraud perpetrator to avoid the fraud or recover monetary compensation), a criminal law(i.e., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities), or it may cause no loss of money, property or legal right but still be an element of another civil or criminal wrong. The purpose of fraud may be monetary gain or other benefits, for example by obtaining a passport or driver's license.

Internet fraud is a type of fraud or deception which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace. It is, however, differentiated from theft since, in this case, the victim voluntarily and knowingly provides the information, money or property to the perpetrator. It is also distinguished by the way it involves temporally and spatially separated offenders.

There are many types of fraud schemes and we can only touch on some of them here.

1) Romance fraud.

Romance frauds often begin on websites where the perpetrator pretends to be an attractive suitor looking for a romantic relationship. He/she persuades the victim to send her/him money and/or gifts. This can continue for months or even years, depending on the skill of the perpetrator and the gullibility of the victim. Once the victim realizes he/she has been fooled, there is little he/she can do because the perpetrator often assumes a false identity. In addition, the victim may not want to admit that he/she has been the victim of a romance fraud and may quietly let the matter rest with no further action.

A more specific example follows:

Romance scammers create fake profiles on dating sites and apps, or contact their targets through popular social media sites like Instagram, Facebook, or Google Hangouts.

The scammers strike up a relationship with their targets to build their trust, sometimes talking or chatting several times a day. Then, they make up a story and ask for money. They'll often say they're living or traveling outside of the United States or they will say they are:

•working on an oil rig
•in the military
•a doctor with an international organization

Romance scammers ask their targets for money to:

•pay for a plane ticket or other travel expenses
•pay for surgery or other medical expenses
•pay customs fees to retrieve something
•pay off gambling debts
•pay for a visa or other official travel documents

Scammers ask victims to pay:

•by wiring money
•with gift cards from vendors like Amazon, Google Play, iTunes, or some other online site.

2. Sales and Investment Fraud

Sales or marketing fraud is the act of purposely misleading or deceiving the public in order to generate more interest in or acceptance of a product. Some examples of marketing fraud are false advertising, exaggerating claims, or misrepresenting product characteristics in advertising.

Marketing fraud can take many forms. Those who would perpetrate such scams generally engage in the following acts:

- Advertising or offering a good for sale and selling it and collecting the money for it without ever delivering it (without ever intending to).
- Advertising a good or service and then, once paid, delivering a good or providing a service that is of lesser quality.
- Pressuring a buyer into purchasing something that they do not want or need.
- Misrepresenting credentials or expertise to sell a good or service that is unneeded or not effective.

The internet is fertile ground for marketing fraud because of the anonymity and the ability to spam messages into inboxes and across message boards and blogs. Indeed, with the pace of change in information technology and, especially with social media, marketing fraud has become global in scale. Marketing fraud perpetrators may not even live on the same continent as their victims.

Because of its reach and cost-effectiveness, mass marketing fraud is most often committed via a web-based platform, such as email, online advertisements, messaging apps and social media.

Investment Fraud

Investment fraud involves the illegal sale or purported sale of financial instruments. The typical investment fraud schemes are characterized by offers of low- or no-risk investments, guaranteed returns, overly-consistent returns, complex strategies, or unregistered securities.

Investment fraud may involve stocks, bonds, notes, commodities, currency or even real estate. The scams can take many forms; the most common frauds tend to fall into the following general schemes:

•Pyramid Schemes**:** A pyramid scheme is when fraudsters claim that they can turn a small investment into large profits within a short period of time.

•Ponzi Schemes**:** This is when a fraudster or "hub" collects money from new investors and uses it to pay purported returns to earlier-stage investors, rather than investing or managing the money as promised.

•Pump-and-Dump**:** A scheme in which a fraudster deliberately buys shares of a very low-priced stock of a small, thinly traded company and then spreads false information to drum up interest in the stock and increase its stock price. Believing they're getting a good deal on a promising stock, investors create buying demand at increasingly higher prices. The fraudster then dumps his shares at the high price and vanishes, leaving many people caught with worthless shares of stock.

•Advance Fee Fraud**:** This type of fraud plays on an investor's hope that he or she will be able to reverse a previous investment mistake involving the purchase of a low-priced stock. The scam generally begins with an offer to pay you an enticingly high price for worthless stock. To take the deal, you must send a fee in advance to pay for the service. But if you do so, you never see that money again.

•Offshore Scams**:** These come from another country and target U.S. investors. Offshore scams can take a variety of forms, including those listed above. Many involve "Regulation S," a rule that exempts U.S. companies from registering securities with the Securities and Exchange Commission (SEC) that are sold exclusively outside the U.S. to foreign or "offshore" investors. Fraudsters can manipulate these types of offerings by reselling Reg S stock to U.S. investors in violation of the rule

These schemes often seek to victimize affinity groups—such as groups with a common religion or ethnicity—to utilize the common interests to build trust to effectively operate the investment fraud against them. The perpetrators range from professional investment advisers to persons trusted and interacted with daily, such as a neighbor or sports coach. The fraudster's ability to foster trust makes these schemes so successful.

The Internet is a useful way to reach a mass audience without spending a lot of time or money. A website, online message, or "spam" e-mails can reach large numbers with minimum effort. It's easy for fraudsters to make their messages look real and credible and sometimes hard for investors to tell the difference between fact and fiction.

Here are some of the ways investors can be tricked online:

Online Investment Newsletters

Fraudulent promoters may claim to offer independent, unbiased recommendations in newsletters when they stand to profit from convincing others to buy or sell certain stocks. They may spread false information to promote worthless stocks.

Online Bulletin Boards

Online bulletin boards are a way for investors to share information. While some messages may be true, many turn out to be bogus – or even scams. Fraudsters may use online discussions to pump up a company or pretend to reveal "inside" information about upcoming announcements, new products, or lucrative contracts.

People claiming to be unbiased observers may actually be insiders, large shareholders, or paid promoters. One person can easily create the illusion of widespread interest in a small, thinly traded stock by posting numerous messages under various aliases.

Pump and Dump Schemes

These schemes often occur on the Internet where it is common to see messages urging readers to buy a stock quickly. Often, the promoters will claim to have "inside" information about a development that will be positive for the stock. After these fraudsters dump their shares and stop hyping the stock, the price typically falls, and investors lose their money.

Spam

“Spam" – junk e-mail – often is used to promote bogus investment schemes or to spread false information about a company. With a bulk e-mail program, spammers can send personalized messages to millions of people at once for much less than the cost of cold calling or traditional mail. Many scams, including advance fee frauds, use spam to reach potential victims.

Fraudulent Ordering of Goods

The Internet has made it easy to shop for merchandise without leaving one's home. All a consumer has to do it visit a retailer's website, place an order for one or more items, give his/her credit or debit card number, a delivery address, and the transaction is completed. This has (not unexpectedly) made it possible for scammers to make fraudulent orders. Such a criminal transaction typically involves the following steps.

1) The fraudster uses a retailer's website to place an order for merchandise- this is similar to a legitimate transaction, except that the scammer is likely to order a greater quantity of items or better quality items than he/she might ordinarily order since he/she has no intention to pay for the goods.
2) The fraudster uses a stolen credit/debit card to pay for the merchandise- he/she may have stolen the card him/herself or may have purchased it from a hacker who actually stole it.
3) The fraudster uses a temporary address to which the goods are to be delivered- this could be a residence where the scammer knows the occupants aren't home during the day or a warehouse where he/she could "sign" as the company representative.
4) The fraudster, after receiving the merchandise, leaves with it and is not seen again- the owner of the stolen credit/debit card will get the bill and will have to work his/her way out of this financial proble.

Embezzlement

Embezzlement refers to a form of white-collar crime in which a person or entity misappropriates the assets entrusted to him or her. In this type of fraud, the embezzler attains the assets lawfully and has the right to possess them, but the assets are then used for unintended purposes. Embezzlement is a breach of the fiduciary responsibilities placed upon a person. Embezzling funds can be as minor as a store clerk pocketing a few dollars from a cash register. However, on a grander scale, embezzlement also occurs when the executives of large companies falsely expense millions of dollars, transferring the funds into personal accounts.

Individuals who are entrusted with access to an organization’s funds are expected to safeguard those assets for their intended use. It is illegal to intentionally access that money and convert it to personal use. Such activities can include diverting funds to accounts that appear to be authorized to receive payments or transfers.

However, the account is a front that allows the individual, or a third-party they are collaborating with, to take the funding. For instance, an embezzler might create bills and receipts for business activities that never took place or services that were never rendered to disguise the transfer of funds as a legitimate transaction.

An embezzler might collaborate with a partner who is listed as a consultant or contractor who issues invoices and receives payment, yet never actually performs the duties they are charging for.

Some types of embezzlement might be combined with other forms of fraud, such as Ponzi schemes. In such cases, the embezzler scams investors to entrust them with their assets to invest on their behalf but instead uses the money for personal gain and enrichment. Maintaining the fraud often includes seeking out new investors to bring in more money to appease prior investors.

An embezzler might also transfer other assets aside from money. An embezzler might claim the real estate, company vehicles, smartphones, and other hardware such as laptops that belong to an organization for personal use.

Embezzlement might take place in the government sector as well if employees seize local, state, or national funding for themselves. Such instances may occur when funding is disbursed to fulfill contracts or to support projects, and a member of the staff skims some of the money that was earmarked.

Some embezzlers “skim off the top” so that they continually acquire a small amount over a particular time interval. This method reduces the likelihood of being caught. On the other hand, some embezzlers steal a very large amount of the goods or funds on a single instance and then disappear. Sometimes company managers under-report income to their supervisors and keep the difference.

Auction Fraud

Auction fraud is defined by the Internet Crime Complaint Center as “fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non- delivery of products purchased through an Internet auction site.”

Fraud can encompass any false or misleading statements, material misrepresentations, or false promises of future actions. A person can be charged with auction fraud even if he/she is not successfully able to carry out a fraud scam. If prosecutors can prove *beyond a reasonable doubt* that a person made an attempt to commit fraud through misleading behavior or false statements, he/she could be looking at a criminal indictment.

Internet auction fraud takes many different forms. Common examples of fraudulent or misleading behavior include:

Overpayment fraud: A seller is the target of this auction fraud scam, which typically involves a high-dollar item being sold. The scam involves sending the seller a counterfeit check or money order for a larger amount than the item’s sale price. The seller is asked to deduct the sale price and return the difference to the buyer, which the seller may do before finding out the check or money order is fraudulent.

Non-delivery or failure to ship merchandise – This is the simplest type of eBay fraud. A seller lists an item on eBay or other auction site and receives payment for the item, but then never sends it to the buyer.

Wire transfer schemes– Wire transfer scams occur when buyers are asked to wire money but never receive items. A seller who is overpaid using a fraudulent check may also be asked to wire the “overpayment”

Second chance schemes– Second chance schemes involve contacting losing bidders of legitimate auctions offering to sell products to them at their highest bid price. The money is collected but the items are never sent.

Misrepresentation– Misrepresentation involves dishonesty about the quality, type, or condition of a product being sold in an online auction. A painting may be misrepresented as being by a famous artist when it is not, or a counterfeit product may be misrepresented as being real.

Triangulation– Triangulation is a complicated auction scam in which a seller lists a high-value item on eBay for a lower price than it can be purchased for elsewhere. The item is then purchased from Amazon (at a higher cost) with a stolen credit card number and is sent to the eBay buyer. Amazon's fraud division forces the eBay bidder to surrender the item to Amazon for nonpayment and is unable to contact the original seller.

Fee stacking– Fee stacking involves tacking on fees after a sale has been made. Usually, fees for shipping are added on.

Selling black market goods– Black market goods are items for sale illegally. Items may include copies of computer software or counterfeited designer clothing or jewelry. Items typically are misrepresented as being legitimate but come with no warranty or protections for buyers.

Selling counterfeit goods- Counterfeit goods are items made bearing a trademark without the trademark owner's permission. Fake handbags and jewelry are examples of some of the counterfeit goods routinely sold on eBay and other online auction websites.

Multiple bidding– Multiple bidding involves a buyer placing multiple bids on an item, including a high-priced bid to scare off other potential buyers. At the last minute, the high priced bid is withdrawn and the buyer is able to purchase the item for a lower amount.

Shill bidding– Shill bidding involves a seller using an alias or someone associated with the auction scam to bid on his item, driving up the price.

International auction fraud– International auction fraud frequently involves individuals from countries outside of the United States flooding auction sites with in-demand products and collecting funds for the products using wire transfer. Items are never sent.

Escrow services scams– Escrow services are supposed to protect buyers. Money is placed with a trusted third party until the merchandise is sent and approved. Escrow services scams, however, involve the creation of a false escrow site resembling a legitimate site. Money or goods are sent to the escrow site but the seller is never paid for the goods or the buyer never receives the item.

Internet fencing– Internet fencing involves using eBay or other online auction sites to sell stolen property to unknowing consumers.

Shell auctions – Shell auctions are auctions in which no merchandise actually exists and the auction is listed solely for the purpose of obtaining money or personal information from a buyer.

Both buyers and sellers can be accused of Internet auction fraud. In many cases, an accusation of fraud is made based on a simple mistake, like a seller not being aware the items he was providing are counterfeit goods.

Unauthorized Funds Transfer

Electronic fund transfers are defined as transactions that use computers, phones or magnetic strips to authorize a financial institution to credit or debit a customer's account. This includes the use of ATMs, debit cards, direct deposits, point of sale transactions, transfers initiated by phones and pre-authorized withdrawals from checking or savings accounts. Consumers typically use a card or pin number to initiate transfers from one account to another.

An unauthorized transaction is any transaction that an individual didn't make and he/she didn't permit anyone else to make. Unauthorized transactions could be made by someone whom the person doesn't know, who finds or steals his/her card or his/her account information. Or they could be made by someone the individual does know but who didn't have permission to use the card. In either case, the person would have to dispute the transactions with the card issuer. The company will then investigate the dispute. If a family member or friend used the card, the persons may have to sign a sworn statement that they took the card without permission. (However, if the individual revealed his/her PIN, the card issuer will consider it a case of his/her giving permission to them to use the card.)

An Example

One recent afternoon, I logged onto to my bank account online to see if a check had cleared. When the screen popped up, I was puzzled. There were a string of debits from the joint checking account my husband and I share. The red-flag charges had begun the previous night.

$38.93 at a McDonalds in Rockville, Md.; $17.12 at a nearby Taco Bell 20 minutes later; various 7-Eleven charges, gas station purchases and so forth. The total amount drained in less than 24 hours: roughly $300.

Neither of us was anywhere near Rockville. My husband had been in New York City; I was in Virginia. The crook apparently somehow got my husband's debit card. (I have a different card with a different number.)

I was told that nothing could be done about the cash that had already been siphoned until my husband called and reported the card lost. But I had no idea whether his card had been lost, stolen or if someone had just skimmed the number from his card at an ATM he used. (His chip card is supposed to guard against that from happening, but lots of ATMs had yet to convert.)

I was certain that my husband was not making these purchases. Eventually, I reached him by phone. He didn't know he had lost the card, but quickly discovered that it wasn't in his wallet. (We surmised that he dropped it in our local bank branch's parking lot after using it and before driving to New York.)

He then called the bank’s toll-free number and filed an official report. The bank made the adjustments to our account three days later by re-depositing the funds that had been withdrawn for each charge. My husband received a new debit card the following business day. As far as I know, that’s the end of our story.

ATM Fraud

Just like any computing device, ATMs have vulnerabilities.

An ATM is composed of a computer (and its peripherals) and a safe.

The computer usually runs on Windows—a version specifically created for ATMs. ATM users don't see the familiar Windows desktop interface because access is restricted. What we do see are user-facing applications that aid us in making transactions with the machine.

The majority of ATM fraud campaigns involve a level of physically manipulating parts of the machine or introducing devices to it to make the scheme work.

Skimming. This is a type of fraud where a skimming device, usually a tandem of a card reader (skimmer) and keypad overlay or pinhole camera, is introduced to the machine by placing it over the card slot and keypad, respectively. The more closely it resembles that of the machine's, the better it will work (and less likely to draw suspicion).

The purpose of the reader is to copy data from the card's magnetic stripe and PIN so the criminal can make forgeries of the card.

Criminals can up the ante of their skimming campaign by purchasing a second-hand ATM (at a bargain price) and then rigging it to record data. These do not dispense cash.

Shimming. One may refer to shimming as an upgraded form of skimming. While it still targets cards, its focus is recording or stealing sensitive data from their embedded chips. A paper-thin shimming device is inserted in the ATM's card slot, where it sits between the card and the ATM's chip reader. This way, the shimmer records data from the card chip while the machine's chip reader is reading it. Unlike earlier skimming devices, shimmers can be virtually invisible if inserted perfectly, making them difficult to detect. However, one sign that an ATM could have a shimming device installed is a tight slot when you insert your bank card.

Card Trap. ATM card theft can occur in a low-tech way by taking someone's ATM card. It can also be carried out by placing something inside an ATM machine that prevents a card from being removed after insertion. When the customer leaves, the card is retrieved. This is often a multi-part ATM scam. When the card is trapped inside the machine, a co-conspirator may suggest to the card's owner that he should re-enter his pin number. A spotter can watch and record the pin number. When the customer leaves without the card, those involved in the scam now have both the card and the PIN.

Forgery

Forgery is defined as the criminal act that includes the purposeful defrauding, misleading, deception, and misrepresentation of a product, service, or item with the intent to deceive. The scope of forgery is a vast one; forgery can include the production of falsified documents, counterfeited items - products intended to resemble other products, and the misrepresentation of fraudulent identification.

The misuse of computer networks, the internet, and various avenues within the online community in order to defraud potential victims of identity theft is classified as electronic – or online forgery. Electronic Forgery is quite common within the digital age, which can include the illegal and unlawful reproduction of endorsements in the form of electronic signatures in order to illicitly assume the identity of the victim of identity theft.

Forgery involves a false document, signature, or other imitation of an object of value used with the intent to deceive another. Those who commit forgery are often charged with the crime of fraud. Documents that can be the object of forgery include contracts, identification cards, and legal certificates. Most states require that forgery be done with the intent to commit fraud or larceny.

The most common form of forgery is signing someone else's name to a check. Objects, data and documents can also be forged. Legal contracts, historical papers, art objects, diplomas, licenses, certificates and identification cards can be forged. Currency and consumer goods can also be forged, but this crime is usually referred to as counterfeiting

Example 1

A popular scam is called account takeover. One person writes someone else a check and the latter goes online to a check-printing service and orders 200 checks with the first person’s account information. The forger might even put his/her own name and address on them. Most people don't reconcile their bank accounts. By the next statement, the forger has already written checks that have cleared the account.

Example 2

In one notorious case of identity theft, the criminal, a convicted felon, incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name. The perpetrator even called his victim to taunt him. The criminal served a brief custodial sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused.

Example 3

On a larger scale, forgery occurs in the fields of art and literature. German forger Wolfgang Beltracchi forged artworks claiming they were painted by Picasso and other European masters. Perhaps the world's most famous case of literary forgery took place with the 1983 "discovery" of the alleged "Hitler Diaries." The diaries supposedly contained passages written by Adolf Hitler between 1932 and 1945. The diaries were actually written by a forger named Konrad Kujau in the early 1980's.