A false representation of a matter of fact—whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed—that deceives and is intended to deceive another so that the individual will act upon it to her or his legal injury.

Fraud is commonly understood as dishonesty calculated for advantage. A person who is dishonest may be called a fraud. In the U.S. legal system, fraud is a specific offense with certain features.

Fraud is most common in the buying or selling of property, including real estate, Personal Property, and intangible property, such as stocks, bonds, and copyrights. State and federal statutes criminalize fraud, but not all cases rise to the level of criminality. Prosecutors have discretion in determining which cases to pursue. Victims may also seek redress in civil court.

Fraud must be proved by showing that the defendant's actions involved five separate elements: (1) a false statement of a material fact,(2) knowledge on the part of the defendant that the statement is untrue, (3) intent on the part of the defendant to deceive the alleged victim, (4) justifiable reliance by the alleged victim on the statement, and (5) injury to the alleged victim as a result.

These elements contain nuances that are not all easily proved. First, not all false statements are fraudulent. To be fraudulent, a false statement must relate to a material fact. It should also substantially affect a person's decision to enter into a contract or pursue a certain course of action. A false statement of fact that does not bear on the disputed transaction will not be considered fraudulent.

Second, the defendant must know that the statement is untrue. A statement of fact that is simply mistaken is not fraudulent. To be fraudulent, a false statement must be made with intent to deceive the victim. This is perhaps the easiest element to prove, once falsity and materiality are proved, because most material false statements are designed to mislead.

Third, the false statement must be made with the intent to deprive the victim of some legal right.

Fourth, the victim's reliance on the false statement must be reasonable. Reliance on a patently absurd false statement generally will not give rise to fraud; however, people who are especially gullible, superstitious, or ignorant or who are illiterate may recover damages for fraud if the defendant knew and took advantage of their condition.

Finally, the false statement must cause the victim some injury that leaves her or him in a worse position than she or he was in before the fraud.

A statement of belief is not a statement of fact and thus is not fraudulent. Puffing, or the expression of a glowing opinion by a seller, is likewise not fraudulent. For example, a car dealer may represent that a particular vehicle is "the finest in the lot." Although the statement may not be true, it is not a statement of fact, and a reasonable buyer would not be justified in relying on it.

The relationship between parties can make a difference in determining whether a statement is fraudulent. A misleading statement is more likely to be fraudulent when one party has superior knowledge in a transaction, and knows that the other is relying on that knowledge, than when the two parties possess equal knowledge. For example, if the seller of a car with a bad engine tells the buyer the car is in excellent running condition, a court is more likely to find fraud if the seller is an auto mechanic as opposed to a sales trainee. Misleading statements are most likely to be fraudulent where one party exploits a position of trust and confidence, or a fiduciary relationship. Fiduciary relationships include those between attorneys and clients, physicians and patients, stockbrokers and clients, and the officers and partners of a corporation and its stockholders.

A statement need not be affirmative to be fraudulent. When a person has a duty to speak, silence may be treated as a false statement. This can arise if a party who has knowledge of a fact fails to disclose it to another party who is justified in assuming its nonexistence. For example, if a real estate agent fails to disclose that a home is built on a toxic waste dump, the omission may be regarded as a fraudulent statement. Even if the agent does not know of the dump, the omission may be considered fraudulent. This is constructive fraud, and it is usually inferred when a party is a fiduciary and has a duty to know of, and disclose, particular facts.

Fraud is an independent criminal offense, but it also appears in different contexts as the means used to gain a legal advantage or accomplish a specific crime. For example, it is fraud for a person to make a false statement on a license application in order to engage in the regulated activity. A person who did so would not be convicted of fraud. Rather, fraud would simply describe the method used to break the law or regulation requiring the license.

Fraud resembles theft in that both involve some form of illegal taking, but the two should not be confused. Fraud requires an additional element of False Pretenses created to induce a victim to turn over property, services, or money. Theft, by contrast, requires only the unauthorized taking of another's property with the intent to permanently deprive the other of the property. Because fraud involves more planning than does theft, it is punished more severely.

Federal and state criminal statutes provide for the punishment of persons convicted of fraudulent activity. Interstate fraud and fraud on the federal government are singled out for federal prosecution. The most common federal fraud charges are for mail and wire fraud. Mail and wire fraud statutes criminalize the use of the mails or interstate wires to create or further a scheme to defraud (18 U.S.C.A. §§ 1341, 1342).

Tax fraud against the federal government consists of the willful attempt to evade or defeat the payment of taxes due and owing (I.R.C. §7201). Depending on the defendant's intent, tax fraud results in either civil penalties or criminal punishment. Civil penalties can reach an amount equal to 75 percent of the underpayment. Criminal punishment includes fines and imprisonment. The degree of intent necessary to maintain criminal charges for tax fraud is determined on a case-by-case basis by the Internal Revenue Service and federal prosecutors.

There are other federal fraud laws. For example, the fraudulent registration of Aliens is punishable as a misdemeanor under federal law (8 U.S.C.A. § 1306). The "victim" in such a fraud is the U.S. government. Fraud violations of banking laws are also subject to federal prosecution (18 U.S.C.A. §§ 104 et seq.).

The Federal Sentencing Guidelines recommend consideration of the intended victims of fraud in the sentencing of fraud defendants. The guidelines urge an upward departure from standard sentences if the intended victims are especially vulnerable. For example, if a defendant markets an ineffective cancer cure, that scheme, if found to be fraudulent, would warrant more punishment than a scheme that targets persons generally, and coincidentally happens to injure a vulnerable person. Federal courts may require persons convicted of fraud to give notice and an explanation of the conviction to the victims of the fraud (18 U.S.C.A. § 3555).

All states maintain a general criminal statute designed to punish fraud. In Arizona, the statute is called the fraudulent scheme and artifice statute. It reads, in pertinent part, that "[a]ny person who, pursuant to a scheme or artifice to defraud, knowingly obtains any benefit by means of false or fraudulent pretenses, representations, promises or material omissions" is guilty of a felony (Ariz. Rev. Stat. Ann. § 13-2310(A)).

States further criminalize fraud in a variety of settings, including trade and commerce, Securities, taxes, real estate, gambling, insurance, government benefits, and credit. In Hawaii, for example, fraud on a state tax return is a felony warranting a fine of up to $100,000 or three years of imprisonment, or both, and a fraudulent corporate tax return is punished with a fine of $500,000 (Haw. Rev. Stat. § 231-36). Other fraud felonies include fraud in the manufacture or distribution of a controlled substance (§ 329-42) and fraud in government elections (§ 19-4). Fraud in the application for and receipt of public assistance benefits is punished according to the illegal gain: fraud in obtaining over $20,000 in food coupons is a class B felony; fraud in obtaining over $300 in food coupons is a class C felony; and all other public assistance fraud is a misdemeanor (§ 346-34). Alteration of a measurement device is fraud and is punished as a misdemeanor (§ 486-136).

In civil court, the remedy for fraud can vary. In most states, a plaintiff may recover "the benefit of the bargain." This is a measure of the difference between the represented value and the actual value of the transaction. In some states, a plaintiff may recover as actual damages only the value of the property lost in the fraudulent transaction. All states allow a plaintiff to seek Punitive Damages in addition to actual damages. This right is exercised most commonly in cases where the fraud is extremely dangerous or costly. Where the fraud is contractual, a plaintiff may choose to cancel, or rescind, the contract. A court order of Rescission returns all property and restores the parties to their precontract status.

Fraud is also penalized by administrative agencies and professional organizations that seek to regulate certain activities. Under state statutes, a professional may lose a license to work if the license was obtained with a false statement.

One particularly well publicized area of fraud is Corporate Fraud. Corporate fraud cases are largely governed by the Securities Exchange Act of 1934 (15 USCA §§ 78a et seq.), along with other rules and regulations propagated by the Securities and Exchange Commission. These laws were a response to the market turmoil during the 1930s and well-publicized corporate fraud cases.

The Securities Exchange Act and the SEC regulate anything having to do with the trading or selling of securities and stocks. They govern fraudulent behavior ranging from stock manipulation to insider trading. They also provide for civil and criminal penalties for corporate fraud.

Despite the act and the SEC, in the early part of the twenty-first century, corporate fraud began to seem endemic. Such well-known companies as energy trader Enron, Telecommunications company WorldCom, cable provider Adelphia, and other lesser-known firms went into Bankruptcyas a result of corporate fraud. In light of these events, Congress decided to tighten up corporate fraud requirements with the passages of theSarbanes-Oxley Act of 2002 (U.S. PL 107-204).

Among other features, Sarbanes-Oxley required expanded and more frequent disclosure by public companies of their finances to prevent fraud. It created a Public Company Accounting Oversight Board to register and regulate accounting firms and accounting practices. It also enhanced the SEC's power to monitor and investigate compliance with securities laws, adding stiff penalties for fraudulent behavior by corporations, their officers, and their accountants.

data diddling The unauthorized changing of data on a computer system: for example changing entries in an ACCESS CONTROL LIST. It is also known asTAMPERING.

Data Diddling

Data diddling is the changing of data before or during entry into the computer system. Examples include forging or counterfeiting documents used for data entry and exchanging valid disks and tapes with modified replacements.

Computer Crime Prevention

Computer crime is becoming ever prevalent in our society. More and more, companies and individuals rely on the services and resources provided through networks and computers. Companies may be dependent on the data to conduct business, while individuals may store information that is important to their personal or work-related activities. Due to this, it becomes vital that steps are taken to protect computer systems and the data that's stored on them.

It is important to remember that no system can ever be completely secure. The only network, Web site, or computer system that's 100% secure is one that can't be accessed by anyone or anything, which makes it completely unusable. Natural disasters, malicious, users who make mistakes, or motivated criminals can compromise security and/or cause damage. The goal for securing your system should be to balance security with accessibility.

Common Types of Computer Related Crime

There are a number of common attacks and methods of committing a computer related crime. Some of these are less sophisticated than others, and can be committed by someone with limited knowledge of computers. Others require programming skills and/or an advanced knowledge of how computers and various software can work together to commit a crime.

COMPUTER VIRUSES

Computer viruses are programs that can attach themselves to other programs or files. The virus infected files can then become carriers of the virus, or become damaged in some way. The virus may effect computer services, displaying messages or playing sounds, or may crash the operating system so that the computer won't run as expected (if at all).

You can prevent computer viruses by installing an anti-virus program on your computer, which scans files for known viruses. There are a number of these programs on the market, and they can be purchased from software stores or acquired on the Internet. Once installed, you will need to regularly update anti-virus files, which are used to detect and remove viruses from your system.

DATA DIDDLING

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transmitting data.

This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable. For example, a person entering accounting may change data to show their account, or that or a friend or family member, is paid in full. By changing or failing to enter the information, they are able to steal from the company.

To deal with this type of crime, a company must implement policies and internal controls. This may include performing regular audits, using software with built-in features to combat such problems, and supervising employees.

HACKERS AND CRACKERS

In computer jargon, "hacker" has a variety of meanings, including being synonymous with programmers and advanced computer users. In these cases, it refers to someone who hacks away at a keyboard for long periods of time, performing any number of computer-related tasks. In recent years, hacking has come to mean the same as another term "cracker," which is a person who cracks the security of a system or computer application. Hacking (and cracking) now refers to the act of gaining unauthorized access to a computer, network, Web site, or areas of a system.

A person may hack their way into a system for a variety of reasons; curiosity, the challenge of breaking through security measures, or to perform malicious actions and destroy or steal data. All to often, it involves performing mischief and damaging a Web site or corporate network in some manner.

Commonly, hackers will impersonate a valid user to gain access to a system. If the system requires a username and password before allowing entry, a hacker may take an authentic user's identity. On a network or an office with Internet access, a hacker can impersonate someone else by simply sitting at the unattended workstation of another user who hasn't logged off. It also commonly occurs when someone has an easy to guess username and password, or allows this information to be known by others.

Another common method hackers use to gain access is to guess or crack a username and password that's used to access a computer, network, or Internet account. To prevent being hacked in this manner, you should use passwords that are difficult to guess. You should also make your passwords a mixture of letters, numbers, and special characters (e.g. !, @, #, $, %, ^, &, *). You should change your password at regular intervals, and set a minimal length to passwords (such as being a minimum of six or eight characters).

Data diddling attack by hackers

Data diddling attacks involve capturing , altering and corrupting data traveling on a network or residing on the hosts . It also involves resending data packets over the networking or rerouting the data packets to invalid destinations . Hackers launch this attack by taking advantage of inherent vulnerabilities in the network protocols or the operating systems . A common data diddling attack is one in which a hacker gains access into a website and modifies its contents . A data diddling attack can be generated by methods like spoofing , sniffing , session hijacking rerouting and port scanning

Data Diddling

Have you heard of data diddling? It is a method adopted by computer criminals.Data diddling is the changing of data before or during entry into the computer system or altering the raw data just before it is processed by a computer and then changing it back after the processing is completed. Using this technique the criminal can manipulate the output and it is not so easy to identify. But using cyber forensic tools we can trace out when the data was changed and changed it back to the original form.