Fraud (PUN013)

Fraud refers to any deceptive activity engaged in by an individual with the aim of gaining something through means that violate the law. One keyword in fraud is deception, wherein the perpetrator leads their victim to believe in an untruth in order to obtain a benefit or value, the most common place where fraud occurs is in the real estate industry, specifically in selling and buying, as well as in falsifying documents such as taxes and medical insurance claims. Fraud is not uncommon and is often carried out by individuals, organizations, and even companies.

E-commerce Fraud: In the past, credit card frauds were the only thing people were wary about. However, with technological advancements and all the personal information people willingly input online, hackers are becoming more "resourceful" and "creative" in their means to deceive people. Here are some of the types of e-commerce fraud we can all become victims of Identity theft No matter the era, identity theft will always remain a major concern for everyone, especially for online merchants, credit companies, and banks. What hackers do is take over the identity of the account owner and make purchases, for example, using stolen credit card information. For as long as they are in possession of the individual's personal details such as name, address, phone number, and credit card details, they can actually successfully purchase what they want online at the expense of the credit card owner. Friendly fraud Merchants are often the victims of this type of fraud. What fraudsters do is make purchases using their debit or credit card and then ask for a chargeback, saying that their credit card details were stolen. The merchant ends up giving a refund while the fraudster keeps the goods. Clean fraud Not even calling it clean fraud makes it clean or right. Clean fraud involves stealing credit cards and using the cards to make purchases while making sure that the perpetrators are able to escape theft detection that is being practiced by payment processors. Using the personal details of the card owner, the thief can successfully make purchases using the stolen card. Merchant fraud Merchant fraud is very common, especially online. It is also the reason why many people are doubtful about purchases that don't do cash-on-delivery transactions. In merchant fraud, the order is received and confirmed by an e-commerce store but then no product or service is delivered, and no chargebacks are allowed. Merchant fraud is also otherwise called internet fraud. Check fraud Even issuing a check while knowing that there is not enough balance in this account is considered fraudulent. A check fraud also happens when a person steals another person's check and forges their signature to make purchases or payments. Pyramid schemes Pyramiding involves a company that encourages people to make investments with the promise that they will get their returns if they are able to recruit downlines and when their downlines recruit their own downlines, too. Charities fraud People should be wary about groups claiming to be supporting or running charitable organizations and asking for donations. Before doing so, people must make sure to check if the group indeed is legitimate – that the charity does actually exist before falling into the trap of charities fraud.

Fraud Warning Signs: Fraud can happen to anyone who isn't careful or selective in the offers they accept. Everyone should be aware of the warning signs to avoid falling prey to such fraudulent activities. Dubious phone calls People should watch out for telephone calls that claim to be from the federal government asking for their Social Security numbers and other personal details. There are also certain fraudsters that call and offer something in exchange for money. Random emails Random emails that ask the recipient to input their login details in the link as this may be a form of phishing. Once they click the link and they enter their details, the fraudsters can now use the login information to steal their accounts. Unknown text messages or emails Receiving a text message from an unknown number or email from an unknown sender stating that the recipient's won the grand prize of a raffle and that they can receive the prize money if they deposit a certain amount of money to the sender. Questionable job listings There are job listings online wherein the person is asked to handle payments for the "boss." The person will receive the money in their account, and they are to forward it to several recipients. It should be avoided at all costs as it may involve something illegal like money laundering. Unverified wire transfer requests People asking their victims to wire money is definitely another sign of fraud. Wiring money cannot be undone, and the perpetrator can access the money almost instantly, making reversals impossible. Fraud is very common, and it can happen to everyone, regardless of status in life. Fraudsters don't target only rich people but anyone who is willing to take their bait. So, everyone should be vigilant. Financial fraud happens when someone deprives you of your money, capital, or otherwise harms your financial health through deceptive, misleading, or other illegal practices. This can be done through a variety of methods such as identity theft or investment fraud. For all types of financial fraud, it is important to report the crimes to the appropriate agencies and law enforcement as soon as possible. Fraudulent charges should also be disputed or cancelled as soon as they are discovered. Furthermore, victims should gather all documentation related to the crime (e.g. bank statements, credit reports, tax forms from current and previous years) and continue to file important information throughout the reporting process. Unfortunately, most victim compensation programs do not cover money lost to fraud or fraudulent schemes. Check your specific state laws regarding victim compensation to make sure. Civil justice may be the only legal option to recover lost money.

Financial Crimes: For a detailed overview of common financial crimes and action steps for reporting please see our Taking Action guide to financial crimes. Identity theft, someone steals your personal financial information (e.g. credit card number, social security number, bank account number) to make fraudulent charges or withdrawals from your accounts. Sometimes people will use the information to open credit or bank accounts and leave the victim liable for all the charges. Identity theft often results in damaged credit rating, bounced checks/denied payments, and being pursued by collections agencies.
Examples:

- Unfamiliar charges or purchases on your credit card or bank account statements.
- Perpetrators posing as a bank, government office, or official institution in order to steal your personal financial information

Investment Fraud: Selling investments or securities with false, misleading, or fraudulent information. This may befalse/grandiose promises, hiding/omitting key facts, and insider trading tips among other things.
Examples:

- Ponzi schemes: Investment fraud scheme where returns are paid to investors using new capital from newly recruited investors as opposed to interest and profits from legitimate investments.
- Pump & Dump schemes: Stock traders or stock brokers purchase a stock at a low value then entice other clients to buy the same stock in order to inflate its price. Those who bought the stock at its low value then sell their shares and pocket the profit.
- Selling a business or real estate opportunity investment with bad, inaccurate, or false information. Also includes omitting or hiding information that is important to an investment decision.

Mortgage and Lending Fraud: Someone else (often a friend or family member) opens a mortgage or loan using your information or using false information or lenders selling you mortgage or loans with inaccurate information, deceptive practices, and other high-pressure sales tactics.

Mass Marketing Fraud: Often committed using mass mailings, telephone calls, or spam emails. Mass marketing fraud typically involves fake checks, charities, sweepstakes, lotteries, and exclusive club or honour society invitations. These offers and letters are used to steal your personal financial information or solicit contributions and fees to fraudulent organizations. Fake charity donation solicitations, Exclusive Club or Honour Society invites. Usually, invitations are sent through mail or emailed and promise membership in a particular organization for a small fee or setting up a recurring charge with no discernible service provided. Also used to steal personal financial information, award or prize notifications. Also seen on the internet as "10,000th Visitor" type notifications. Usually, ask for personal financial information or fee to be paid in order for a prize to be delivered or award to be made official. If you do not remember applying or entering a competition for the award or prize it is probably fraudulent. Phone calls claiming to be from the government, your bank, or other "official" agency, for all types of financial crime, you should contact at least the following agencies, local police or law enforcement to report the crime and obtain a police report, your bank(s) to report the crime and explore any possibleresources the bank has available, local District Attorney.

Identity Theft: No matter the era, identity theft will always remain a major concern for everyone, especially for online merchants, credit companies, and banks. What hackers do is take over the identity of the account owner and make purchases, for example, using stolen credit card information, for as long as they are in possession of the individual's personal details such as name, address, phone number, and credit card details, they can actually successfully purchase what they want online at the expense of the credit card owner.

Friendly Fraud: Merchants are often the victims of this type of fraud. What fraudsters do is make purchases using their debit or credit card and then ask for a chargeback, saying that their credit card details were stolen. The merchant ends upgiving a refund while the fraudster keeps the goods.
Clean fraud: Not even calling it clean fraud makes it clean or right. Clean fraud involves stealing credit cards and using the cards to make purchases while making sure that the perpetrators are able to escape theft detection that is being practiced by payment processors. Using the personal details of the card owner, the thief can successfully make purchases using the stolen card.

Merchant fraud: Merchant fraud is very common, especially online. It is also the reason why many people are doubtful about purchases that don't do cash-on-delivery transactions. In merchant fraud, the order is received and confirmed by an e-commerce store but then no product or service is delivered, and no chargebacks are allowed. Merchant fraud is alsootherwise called internet fraud.

Check Fraud: Even issuing a check while knowing that there is not enough balance in this account is considered fraudulent. A check fraud also happens when a person steals another person's check and forges their signature to make purchases orpayments.

Pyramid Schemes: Pyramiding involves a company that encourages people to make investments with the promise that they will get their returns if they are able to recruit downlines and when their downlines recruit their own downlines, too. Charities fraud: People should be wary about groups claiming to be supporting or running charitable organizations and asking for donations. Before doing so, people must make sure to check if the group indeed is legitimate – that the charitydoes actually exist before falling into the trap of charities fraud.

Fraud Warning Signs: Fraud can happen to anyone who isn't careful or selective in the offers they accept. Everyone should be aware of the warning signs to avoid falling prey to such fraudulent activities. Dubious phone calls, people should watch out for telephone calls that claim to be from the federal government asking for their Social Security numbers and other personal details. There are also certain fraudsters that call and offer something in exchange for money, Random emails, random emails that ask the recipient to input their login details in the link as this may be a form of phishing. Once they click the link and they enter their details, the fraudsters can now use the login information to steal their accounts, Unknown text messages or emails, receiving a text message from an unknown number or email from an unknown sender stating that the recipient's won the grand prize of a raffle and that they can receive the prize money if they deposit a certain amount of money to the sender, Questionable job listings, there are job listings online wherein the person is asked to handle payments for the "boss." The person will receive the money in their account, and they are to forward it to several recipients. It should be avoided at all costs as it may involve something illegal like money laundering, Unverified wire transfer requests, people asking their victims to wire money is definitely another sign of fraud. Wiring money cannot be undone, and the perpetrator can access the money almost instantly, making reversals impossible. Fraud is very common, and it can happen to everyone, regardless of status in life. Fraudsters don't target only rich people but anyone who is willing to take their bait. So, everyone should be vigilant, financial fraud happens when someone deprives you of your money, capital, or otherwise harms your financial health through deceptive, misleading, or other illegal practices. This can be done through a variety of methods such as identity theft or investment fraud, for all types of financial fraud, it is important to report the crimes to the appropriate agencies and law enforcement as soon as possible. Fraudulent charges should also be disputed or cancelled as soon as they are discovered. Furthermore, victims should gather all documentation related to the crime (e.g. bank statements, credit reports, tax forms from current and previous years) and continue to file important information throughout the reporting process. Unfortunately, most victim compensation programs do not cover money lost to fraud or fraudulent schemes. Check your specific state laws regarding victim compensation to make sure. Civil justice may be the only legal option to recover lostmoney.

Common Types of Financial Crimes: For a detailed overview of common financial crimes and action steps for reporting please see our Taking Action guide to financial crimes. Identity theft: Someone steals your personal financial information (e.g. credit card number, social security number, bank account number) to make fraudulent charges or withdrawals from your accounts. Sometimes people will use the information to open credit or bank accounts and leave the victim liable for all the charges, identity theft often results in damaged credit rating, bounced checks/denied payments, and being pursued by collections agencies, Investment Fraud: Selling investments or securities with false, misleading, or fraudulent information. This may be false/grandiose promises, hiding/omitting key facts, and insider trading tips among other things, Mortgage and Lending Fraud: Someone else (often a friend or family member) opens a mortgage or loan using your information or using false information or lenders selling you mortgage or loans with inaccurate information, deceptive practices, and other high-pressure sales tactics, Mass Marketing Fraud: Often committed using mass mailings, telephone calls, or spam emails. Mass marketing fraud typically involves fake checks, charities, sweepstakes, lotteries, and exclusive club or honour society invitations. These offers and letters are used to steal your personal financial information or solicit contributions and fees to fraudulent organizations.
How to Report Financial Fraud: For all types of financial crime, you should contact at least the following agencies:

- Local police or law enforcement to report the crime and obtain a police report
- Your bank(s) to report the crime and explore any possible resources the bank has available
- Local District Attorney

Thank You…