ROCIC Special Research Report

Holiday Crime

+ Scams and Fraud Schemes

Regional Organized Crime Information Center

Table of Contents

ROCIC Can Assist Officers with Holiday Safety

ROCIC Training and Officer Safety Resources

ROCIC Training Department

The ROCIC Training Department offers numerous training opportunities for police officers, including operational planning, response to active shooters, civil unrest planning and response, risk avoidance, crime scene management, and others. Training courses can be found at www.rocic.com/training.

ROCIC Publications

Additional training publications can be found on the ROCIC Publications webpage, including topics on fraud, credit card crime, virtual currencies, forged identification, gift card scams, burglaries and thefts, crimes against the elderly, among others. These publications can be accessed by logging into your RISSNET account at https://rocic.riss.net/publications.

ROCIC Officer Safety Website

RISS also offers officer safety resources on their Officer Safety Website, including concealment methods, law enforcement threats, gangs, narcotics, domestic terrorism, sovereign citizens, and armed and dangerous subjects. This information can be accessed by logging into your RISSNET account at https://officersafety.riss.net.

Other ROCIC Resources

ROCIC Criminal Intelligence Unit

The Intel Specialists with ROCIC's Criminal Intelligence Unit (CIU) can access dozens of research tools, specialized databases, public record information, criminal justice information, and data. They are able to search, retrieve, compile, and provide a consolidated reporting of findings to officers. This assistance helps officers in need of quick, accurate, and complete information. Information gained by ROCIC can help develop leads, link criminal activity, gain background information on suspects, and quickly obtain driver's license photos.

RISSIntel

The RISS Criminal Intelligence Databases (RISSIntel) provides for a real-time, online federated search of RISS and partner intelligence databases, including state systems. Millions of intelligence records are available via RISSIntel. These records include individuals, organizations, groups, and associates suspected of involvement in criminal activity, as well as locations, vehicles, weapons, and telephone numbers.

ROCIC Law Enforcement Coordinators

The ROCIC Law Enforcement Coordinators have specialized email lists to get your information out as fast as possible to jurisdictions that might be affected by similar cases.

ROCIC Analytical Unit

The Analytical Unit converts complex information into easy-to-understand charts and presentations. The Audio and Video Forensic Department can enhance photos and video surveillance footage. The Computer Forensics Department assists in collecting evidence from electronic devices.

ROCIC Technical Services

The ROCIC Technical Services Unit loans specialized equipment to member agencies at no charge, including surveillance cameras and recording devices.

More information on RISS and ROCIC resources can be found at www.riss.net.

Holiday Crime and Scams

Don't Be a Victim

The traditional holiday season of Thanksgiving, Christmas, and Hanukkah means spending time with family, automobile or airline travel, the exhanging of gifts, religious services and traditions, and counting our blessings. It is also an active time for all types of crooks and thieves, because they know that the sidewalks and stores are crowded with people carrying cash, expensive gifts, and financial transaction cards.

Retail sales top $600 billion and theft increases up to 30 percent during the year-end holiday period, according to sources. Shoplifters, counterfeiters, pickpockets, residential burglars, and purse snatchers are busy at work during this season, but the holiday period can also bring out the worst in people — drunk driving, robberies, vehicle theft, domestic violence, rapes and sexual assaults — so citizens also need to take precautions and stay safe.

The leading crime of the season, however, is identity theft, a crime related to our new interconnected digital world of smartphones, and tablets, and computers. Much of our commerce is now conducted online, and electronic thieves take advantage of that trade through skimming, phishing, pretexting, and other devious schemes. Crooks also prey on the goodness of people during this time, offering deals too good to be true, and charity scams that tug at our heart-strings. Be informed, stay alert, and use common sense, so that your holiday season will stay merry. Here are a few tips to safely enjoy the holiday season and thwart those nasty crooks out there.

Online or Electronic Shopping

- Check the charity: Before donating to a charity, make sure it is registered with the Secretary of State and ask how much of the money goes to the charitable fund-raiser and how much goes to the charitable purpose.
- Skip the rack: Only purchase gift cards from reputable sources. Better yet, get them directly from the store they're from—and preferably directly from the store cashier — and ask them to scan the card to ensure it has the correct balance.
- Surf safely: Do not use public Wi-Fi to check sensitive financial information, or to make purchases using your credit card.

- Sign off: Require a signature on all package deliveries. You can also write specific instructions for the delivery company on where to leave your package, and don't forget you can always have your package delivered to you at work.
- Use credit: Use a credit card instead of your debit card when making holiday purchases.
- Only buy gift cards from the official retailer and not a third-party source.
- Don't stress: Pay special attention to your health and well-being during the hectic holiday season. Research shows that people experiencing an illness, loneliness or financial difficulties are less able to spot and avoid scams.
- Beware of deals: Watch out for deals offered by companies with unfamiliar websites. Look for reviews on Yelp, the Better Business Bureau or even search the retailer's name and "scam" to see if it checks out before giving your payment information.
- Be aware of social media scams. Beware of ads for phony contests and "stay at home" job postings even if they are from friends.
- Only download mobile apps from official app stores. Check the user reviews and read the app permission policies.
- Never respond online to spam emails or click on an included link.
- Beware of Skype message scares. Never click on a suspicious link, even if it's from someone you know.
- Smishing — remember that legitimate businesses, such as banks, will not ask you to verify personal information via texts.
- When you want to donate, visit the charity's website and do a little research before donating.
- When receiving e-cards, check to see that the sender is someone you know and that it comes from a well-known e-card site.
- Phony classifieds — don't wire money for deals and make sure you don't pay for an item before receiving it.

When shopping at stores

- When parking your vehicle to go shopping, remember where you parked it! Always park in a well-lit and well-traveled area. Do not park in a remote dark area.
- When you return to your vehicle, scan the interior of your car to be sure no one is hiding inside. Check to see if you are being followed.
- Have your keys in hand when approaching your vehicle. You will be ready to unlock the door and will not be delayed by fumbling and looking for your keys.
- When storing items purchased at the stores, place them out of sight. The best place is in a locked trunk.
- Do not leave your purse, wallet, or cellular telephone in plain view.
- Be extra careful with purses and wallets. Carry a purse under your arm. Keep a wallet in an inside jacket pocket, not a back trouser pocket — even when you are grocery shopping!
- Don't resist if someone tries to take any of your belongings. Don't chase someone who robs you, they may have a weapon. Instead call 911.
- Lock your vehicle and put up your windows even while you are driving.
- If you go to an automatic teller machine for cash, check for people around and make sure it is well lit and in a safe location.
- Carry only the credit cards you need and avoid carrying large amounts of cash.
- Beware of the "good deal" scams. Things are not always what they appear to be.

For the Home/Apartment:

- Be extra cautious about locking doors and windows when you leave your house or apartment, even for a few minutes.
- Don't openly display your tree and gifts in the front window so they are easily visible from the street. It's too tempting for a potential criminal to smash the window and grab the wrapped packages…or plan a later break-in based on their earlier observation.

- Don't advertise. Burglars look for occupancy cues like outdoor lights burning 24 hours a day, piled-up newspapers, mail, or advertising flyers hanging on the door knob.
- Use an inexpensive light timer when you are away and ask a neighbor to pick up your newspapers and mail. If you are going away for the holidays, you can stop your mail online.
- If you go out for the evening, turn on lights and a radio or television so the house or apartment appears to be occupied.
- Burglars know to look for the hidden door key near the front entrance. Don't hide spare keys under rocks, in flowerpots, or above door ledges. Instead give the spare key to a trusted neighbor.
- Burglars prefer to enter through unlocked doors or windows. A holiday problem can occur when exterior Christmas-light extension cords are run inside through a window and prevent it from being secured.
- Don't post your family name on your mailbox or on your house. A burglar can call directory assistance to get your telephone number and call your home while in front of your house to confirm that you are away.
- Don't leave descriptive telephone answering machine messages like, "You've reached the Wilsons…we're away skiing for the holidays…please leave a message." Bad guys love to hear that they have plenty of time to break in and completely ransack your home.
- The day after opening presents, don't pile up empty gift boxes from your new computer, DVD player, or stereo receiver on the street for the garbage man. Burglars appreciate knowing that you have expensive gifts inside for them to steal. Break the boxes down or cut them up to better conceal the items.

Con Artists and FlimFlams

Bank Examiner

The perpetrators of this type of offense specifically target senior citizens. It is designed to take several thousand dollars (normally various amounts up to $9,000) in one or multiple transactions.

The victims are selected in many ways including criss-cross telephone books, random telephone surveys, previous obituary notices or observation at banks and shopping centers. Different suspects use many variations to convince the victim they are dealing with legitimate law enforcement or bank personnel. The victim receives a telephone call by a subject posing as a law enforcement officer, bank security, or other official. They are told that there is a "problem" at their bank. The caller may claim that other accounts are involved, and others have agreed to assist. The victim is often informed that a person at their bank is dishonest and is stealing from accounts. The caller elicits the assistance of the victim and requests they withdraw money from their bank and not talk to anyone about the withdrawal. Throughout the offense the suspect reassures the victim that their account will be replenished and they will not lose any money. He may tell the victim not to take a check, and to tell the bank teller/manager that the money is being used for a relative or other cash transaction. The caller tells the victim they will be met by an officer after the withdrawal is made, either at a pre-determined location or their home. The victim is instructed to give the currency they withdrew to the officer who will take the currency for evidence.

In multiple transactions which may continue for several days or weeks, the victim may receive further calls informing them of the progress of the "investigation" and convince the victim to make further withdrawals to reinforce the case against the dishonest employee. Normally the same pattern is followed by the suspect when taking the victim's money.

Broken Bottle Scam

A con man walks around carrying a bag filled with broken or breakable glass and deliberately bumps into a person and drops his cargo. The mark is accused of breaking the bottle and feels guilty or intimidated into paying for a replacement. There are

several variations on this trick. Sometimes the grifter uses eyeglasses, sometimes he claims that the mark broke a bottle of prescription medicine. Assuming $20 to $40 per successful scam, that's a pretty decent day's wage.

Caller ID or Spoofing

Technology now exists that enables callers to manipulate the phone number and even the name that shows up on the unsuspecting recipient's Caller ID display, allowing them to masquerade as officials of legitimate companies, churches, banks, credit card companies and courthouses. Spoofing doesn't require any substantial investment, and there are a number of firms that specialize in selling the service. One such firm, with its motto "Be who you want to be," SpoofCard.com, sells calling cards for as little as $10 for 60 minutes of talk time. This is how it works: SpoofCard has a dedicated toll-free number where a user enters a PIN, the desired fake caller identity and the number they'd like to call. SpoofCard users also have the ability to select a male or female voice. The caller speaks normally, but the person on the other end hears the altered male or female voice selected by the caller. Companies selling Spoofing services claim its markets include legitimate users such as private investigators, law enforcement officials and lawyers. For example, if a law enforcement officer is attempting to find a suspect and has reason to believe that person is at a particular residence, the investigator probably wouldn't want to place a call with telltale police department information showing up on the caller ID. Another example could be a situation where the caller makes a call from their personal cell phone and doesn't want the recipient to have the cell phone number, the caller could use spoofing technology to display their office number instead. But there is a dark side to spoofing that's emerging at a high rate of speed. Scam artists are using this service, persuading consumers to reveal their Social Security numbers or other sensitive personal information. For example - You receive an incoming call and your Caller ID display indicates the call is coming from your local courthouse. The caller tells you that you have failed to show up for jury duty and requests you pay a fine or provide your SSN or other personal data so the court may reschedule you for jury duty. If you are contacted by a person claiming to be from a jury office, with your caller ID showing a courthouse number, requesting that you pay a fine or provide personal information because you missed jury duty, do not give that person any information. Bottom line...do not automatically assume

the information displayed in your caller id accurately identifies the caller.

C.O.D. Scam

The suspect will scout a neighborhood to find a suitable unoccupied home. He will check a city directory publication to determine the name of the homeowner. He will put the name on a phony shipping label and attach that to a box containing rocks or similar type debris. He will then return dressed in an "express delivery" type of uniform. He will pretend to knock or ring the doorbell at the unoccupied house. Getting no answer, he will then go to a next-door or nearby neighbor and ask them to accept the package and pay the C.O.D. fee.

Diversion Burglary

A man, woman and one or two children appear at the victim's door and plead to use the victim's phone. They claim to have an emergency -- car problems, a sick child -- and must call for help. Or they may simply ask for a drink of water. Once inside, one offender distracts the victim while another searches the house for valuables to steal.

Door-To-Door Solicitor

As a door-to-door solicitor, the bunco artist asks for a donation to benefit a nonexistent organization or purpose, or sells a product for a reduced price if the person signs the contract immediately and pays cash at the time of sale. Verify a door-to-door solicitor's identification and permit. If in doubt, call local law enforcement immediately. Tell the solicitor the contract will not be signed until an attorney has reviewed it.

Fortune Telling Fraud

A crime designed to financially exploit a victim under of the guise of providing assistance. It involves gaining the victim's complete trust and, then through carefully managed manipulation, convincing the victim to give valuables to the suspect(s). Victims of these cases are of any age and background and share a common trait of seeking help in solving a problem in their life. Problems generally fall into three major categories: Love, Money and Health. The offense starts off innocently with a 'read-

ing' for a nominal fee. The suspect may use a method and props such as:

Religious icons, Tarot Cards, Crystal Ball, Palm Reading, Tea Leaves Reading, Coffee Grind Reading, Sand Reading, ESP Psychic Reading, and Dice etc. During the reading, the reader elicits information from the victim, using both verbal and non-verbal clues, and then repeats it back in such a way as to reinforce the fact that the reader does, in fact, have certain powers. In subsequent sessions, the victim is most often convinced that their 'problem' is the result of a curse that has been placed on them or their family. The reader convinces the victim that through spiritual or physic powers she/he alone is able to remove this curse. To prove that a curse exists, many different ploys are used. The reader performs a ritual, (using common magic tricks) which is designed to convince the victim that the evil of the curse has manifested itself in the item. For instance, a devils head that appears when an egg is broken, needles that come out of a tomato, water that turns red, a live chicken dies, a small snake or worm appears to come out of an item or the victim's body. The reader convinces the victim that she/he 'has the gift' and can remove the curse. The curse removal sometimes entails the destruction of the cause of the curse, which invariably is money or jewelry. In some cases the suspect takes the valuables, with a promise to return them, to have them blessed or prayed over. In other cases, the reader convinces the victims that the valuables must be destroyed or buried with an accompanying ritual to remove the curse. The curse removal can be carried out in one short operation or more generally is carried out over a period of months and sometimes years, taking all of the victim's liquid assets. When these assets are used up, some offenses continue by having the victim obtain more money though the use of their credit. A long-term offense results in the total psychological manipulation of the victim, which isolates them from any independent support from family or friends and keeps them vulnerable to any suggestions given by the reader.

Handkerchief Switch

The key elements in these offenses is that a stranger, with a large amount of currency, joined by a second stranger convince the victim to hold the currency for safekeeping or distribution to a charity after putting the money from all three in a handkerchief or paper bag. After the strangers leave, examination of the package reveals the currency is cut up paper. These offenses may be known as the South African Letter,

Jamaican Switch, and Country Boy Switch. The South African Letter, which became very popular in the 1990's, is the most frequently used at the current time. The offenses normally employ two suspects. The first is known on the street as the "Catch" and the second is known as the "Cap."

The offense can be played by one suspect, but that is infrequent. The offenses generally go through the following progression. The victim is approached on the street by the Catch who will pose as a South African with a large amount of currency obtained in an insurance settlement; a Jamaican or other foreign seaman with a large amount of currency obtained from wages; or a country boy with a large amount of currency from the sale of produce, land, etc. The Catch may play the part of a fool and asks the victim for assistance in locating an address, which is non-existent. In the case of the South African, the Catch may be looking for a church or charitable institution to donate the money to, as he cannot take the currency home because of political turmoil. He may show letters from an attorney or insurance company indicating the amount of money and a letter from his home country explaining that he cannot bring the currency back. In the case of the Jamaican or County Boy, the Catch may explain that he paid several hundred dollars to a woman to "have a good time" and is looking for the hotel (non-existent) where she told him to meet her. If the Catch determines that the intended victim is suitable, he will pull in (signal) the Cap to join in. The Catch will then explain the scenario a second time to the Cap. During all conversations the Catch will display a large roll of what appears to be several thousand dollars. The Cap will tell the Catch that the location does not exist and caution him about showing the money in public, as people will rob him. At this point a discussion about banks may ensue which will help determine if the victim has money in the bank. At this point the suspects make a determination whether to play the victim for the cash he has on him or attempt to get money that is in the victim's bank. If they decide to play for the bank money, the Catch may claim ignorance about banking procedures and will not believe that currency can be taken out of the bank. The Cap enlists the aid of the victim to convince the Catch how banks work. In some cases the Catch will tell the victim and the Cap that he will match anything they get out of the bank to prove that money can be taken out as an incentive to have the victim withdraw currency. The Cap may or may not pretend to make a withdrawal to show the Catch. The victim is the induced to do likewise.

Jury Duty Scam

A senior receives a phone call from the county courthouse saying that because she missed jury duty that week, a warrant for her arrest was being issued. The caller says the local judge had given him a list of jury "no-shows" about to be arrested that included the senior's name, phone number and address (which the scammer probably found in an ordinary phone book). When the senior protests, the caller asks for a Social Security number for confirmation. It's yet another identity theft scam that tries to scare people into divulging personal information such as birth dates, Social Security numbers, and credit card account numbers. After originating in upstate New York in 2001, it has spread to other states. These calls may actually appear on your caller ID to be coming from the county courthouse a technique called "spoofing" which allows scammers to choose any telephone number they want and have it displayed on a recipient's caller ID. Authentic jury duty notifications, as well as "no-show" summons, are almost always delivered by mail. Local, state, and federal judicial officials would never ask for personal information over the phone.

Latin Lotto

Victims in these cases are normally Hispanic and the suspects are male and female Hispanics. The suspects normally speak only Spanish while playing this offense. The first suspect, who claims to be looking for an attorney, approaches the victim on the street. The suspect goes on to say that he has a winning lottery ticket but is afraid to cash it as he is in the country illegally. The second suspect joins the scenario and the story is told again. The first suspect either offers to pay the two a substantial amount of money or sell them the winning ticket at a great discount for assistance in cashing the ticket. Once the victim agrees to help, the suspect claims to want proof that they know how to handle money or needs currency to purchase or redeem the ticket and induces the victim to withdraw several thousand dollars. Once the money is withdrawn it is taken from the victim either in a switch or, more frequently, by sending the victim into a drug store and driving off. In this scenario, one of the suspects feigns sickness throughout the offense and pretends to very ill when the victim returns from the bank. The victim is sent into the drug store for medicine and the suspects drive off.

Lottery Scams / Foreign Lottery

In this scam, you receive a call, email or letter -- usually from a foreign country -- telling you about a way to select winning lottery numbers, and you need to call a toll-free number to find out more. There is no need to call that number. All the con criminal has is a winning way to take your money.

Lotteries

A person offers to sell a winning lottery ticket or a "law firm" says someone has left you a winning lottery ticket, but you must send money so a computer can verify your identity. The "winning" ticket may be counterfeit or not exist. Be suspicious, do NOT buy a ticket from an individual, and do not send money!

Pickpocket Diversion

"Oh I'm so sorry to stain your shirt/dress," says the con artist after squirting ketchup, mustard or some such substance on your clothing. While fumbling in his attempts to clean your clothes, he cleans you out, wallet and all.

Pigeon Drop

The key element of a Pigeon Drop offense is the finding of a large quantity of currency and convincing the potential victim they can share in the money. The offense can be committed on any victim but is normally committed on an older victim by two suspects, females and/or males. However; it can be committed by one suspect acting in concert with someone on the telephone. The initial approach is made in retail shopping areas and follows this general described pattern. The victim is approached by at least one suspect who engages the victim in conversation. The suspect alone (or joined by a second suspect) will find or tell the victim they found a package, wallet, etc. Subsequent examination will reveal the package contains what appears to be a large amount of currency. One of the suspects volunteers to check with her "boss" to get advice on what to do with the "found money." The suspect may use a cellular phone to contact the "boss" or leave with the package to see the "boss." After consulting with the "boss," the suspect will tell the victim the money came from

an illegal source such as gambling, narcotics, etc. and the package contains several thousand dollars (i.e. $100,000) and they can split the money three ways. The victim may also be told that the package contained a valuable bond or security worth several thousand dollars which adds to the total they can split. The victim is told the boss will help them share the money and cash the bond. He may require each of them to show, "good faith" by producing money of their own to demonstrate they can manage large amounts of money without spending it for 30 days or he may offer to make the income derived from the division of the "found money" look legitimate such as proceeds from an investment which he will "postdate." The victim is led through the ensuing process by the suspects who let them believe they will receive a share of the "found money" for just being present when the money was found and doing very little on their part. This may entail the ruse of bank withdrawals by one of the suspects and a trip to see the "boss" with the suspect returning and displaying a share of the money. Eventually, after several temporary set backs, the victim is convinced to withdraw several thousand dollars to be able to receive a share of the "found money." Initially the victim believes they will not lose possession of the money. Eventually the money is taken from the victim and given to the purported "boss." The victim is sent into a business to see the "boss" and retrieve their money and their share of the found money only to discover there is no boss and the suspects are gone.

Police Follow-up Scam

This scam is also known as the "Double-Play". It is perhaps one of the most vicious of all of the scams. It is always played upon someone who has been victimized by a previous con game, or in some instances a more common crime such as robbery or burglary. The key to this crime occurring is usually the fact that the original suspects learned the victim still has sizable sums of cash. The suspects in the previous crime pass on this information to others who specialize in the impersonation of police officers and commit this second crime. The new suspects, armed with the particulars of the previous crime, approach the victim at their residence and identify themselves as police officers. They describe the previous crime in detail and tell the victim that the suspects in the original crime have been caught and that they have recovered the victim's money. They tell the victim that they can't release the money right now as it is needed as evidence and they have uncovered evidence that an employee at the bank

was also involved. Shortly after the suspects arrive, the victim may receive a phone call from someone who will identify himself or herself as a police official. This person asks the victim if the "officers" have arrived. This call is designed to help to convince the victim that the people at the door really are officers and to induce the victim's voluntary cooperation. The suspects, at the victim's house, may talk to the caller to bolster the victim's belief they are dealing with legitimate law enforcement officers. They tell the victim that they need their help to catch this dishonest employee in the act of stealing. Once the victim agrees, they instruct the victim to go their bank and withdraw a sizable amount of money so the suspect can be caught red-handed. The amount is usually under $9,000 dollars to avoid mandatory reporting by the bank. They tell the victim that no money will actually be withdrawn from their account because the police department or the bank has arranged to replenish the account. After the withdrawal the suspects take the money and leave. In some cases they have given the victim a receipt.

Recovery Rooms

Been Ripped Off? We'll Get Your Money Back! These "recovery rooms" get the names of people who have been defrauded in other scams and then call, claiming to be Federal attorneys or agents who can get your lost money back-for a fee. When the Federal government sues scam artists, there is never a charge to consumers to return any money recovered.

Rock In A Box

What a bargain! - $100 for a new color TV. Sure it's suspicious but the box is sealed. Maybe it is stolen, but that's not your problem. Victim buys TV and takes it home. When he/she opens the box out comes well padded rocks.

Sweetheart Swindle Con

This is a con game normally perpetrated by transient criminals, targeting mostly elderly widowed or single males or females. The operatives will have a "chance meeting" with the intended victim on the street; in a supermarket; bank; or other public

areas frequented by the elderly. Conversations will ensue and over a period of time the con artist will engage the victim in a bogus romantic relationship. The con artist may indicate that they are in dire financial circumstances and tell the victim they are waiting on a large insurance/law suit settlement. The suspect may ask for a loan for a sewing business (either for material or machinery) or they may ask for a loan for an expensive medical procedure and promise to pay the loan back when they get the money from the settlement. This relationship may lead to professions of love and even promises of marriage. As the relationship progresses, the con artist may ultimately induce the victim into signing a Power of Attorney form.

This opens up the opportunity for the player or an associate to completely drain all the financial assets of the victim.

The player may also induce the victim to change an existing will, having them named as the major heir. In some of these cases, the players are successfully able to get the victims to sign over the ownership of their homes.

Once achieved, the con artist immediately resells the home and pockets the proceeds. Once the perpetrator has depleted all of the victim's finances, they may obtain a life insurance policy on the victim, naming himself or herself or an associate as beneficiary. The sweetheart scam will continue until either the money runs out, the victim dies, or fear that the police might become involved. Very rarely will the victim call the police. Usually it's the victim's family that eventually discovers the scam and reports

it against the victim's wishes. When confronted by police, the victim may or may not remember every incident in which he or she has been scammed out money. The victim may also be reluctant to prosecute, because he or she's in love, scared, or embarrassed. Prosecution of these types of cases is sometimes difficult, due to either the victim's reluctance to assist or because of their advanced age, their memory is so poor that they tend to make bad witnesses.

Three-Card-Monte

Most people are familiar with this one. Find the red card amidst two black ones and win whatever amount you bet. While you watch, someone does just that, and then persuades you to try your hand. You never win since the hustler is palming the cards.

The "winner" was a plant. Even if you win, pickpockets will relieve you of your cash. Or right after you place your bet, someone yells police and the operator disappears with your money.

Truck Stop Three-Card-Monte

The following Method of Operation is used in the scams. Several people (part of the group) are seen playing Three Card Monte and winning large amounts of money. In some cases, thousands of dollars are exchanged and a group of spectators gather to watch. Nearby potential victims are encouraged to join in. The suspects may entice potential victims at motels, etc. that there are Hooter's Girls outside on the parking lot or that a guy who just won the lottery is losing large amounts of money in a card game. A victim is enticed to enter the game and quickly wins several hundred to several thousand dollars. The dealer expresses concern that the new player has enough money to cover his bets and asks to see his money. When the player shows his currency and/or jewelry the other "players" grab his valuables and run or in many cases, take his valuables by force when he resists. In some cases, the suspects just ask for change and when the victim takes his money out of his pocket, the suspects take in and run. These subjects appear to be part of a large group of subjects who are based in the Greater Cincinnati area and travel throughout the country committing these offenses. Most recently they have conducted their activities at motels, truck stops, gas stations, car auctions, biker rallies, sporting events such as car races and rest areas on interstate highways. The group generally travel in several automobiles.

Toner Rooms

We're Your Office Supplies Company and We Have a Great Deal! Prices are going up soon, so place your order now. These scam artists ship low-quality goods at high prices and try to bully companies into paying for them. Typical come-ons involve sales of copier toner, copy paper, cleaning supplies, and light bulbs. If your company receives unordered goods, don't pay. But do complain.

Yellow Page Advertising Scheme

The solicitation from an alternative business directory may have the appearance of an invoice. It may bear the walking fingers logo and feature the name "Yellow Pages." It also may falsely suggest that the publisher is affiliated with your local telephone company or with another bona fide Yellow Pages publisher you recognize. Further, the solicitation may lead you to believe that your business already has been listed in the telephone directory and you are now being billed when, in fact, you are only being solicited for placing an ad.

Business and Investment Fraud

- Purchase merchandise from reputable dealers or establishments.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.
- Purchase merchandise directly from the individual/company that holds the trademark, copyright, or patent.

Nigerian Letter or "419" Fraud

Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter mailed from Nigeria offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author—a self-proclaimed government official—is trying to transfer illegally out of Nigeria. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name and account numbers, and other identifying information using a fax number provided in the letter. Some of these letters have also been received via e-mail through the Internet. The scheme relies on convincing a willing victim, who has demonstrated a "propensity for larceny" by responding to the invitation, to send money to the author of the letter in Nigeria in several installments of increasing amounts for a variety of reasons.

Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria. In actuality, the millions of dollars do not exist, and the victim eventually ends up with nothing but loss. Once the victim stops sending money, the perpetrators have been known to use the personal information and checks

that they received to impersonate the victim, draining bank accounts and credit card balances. While such an invitation impresses most law-abiding citizens as a laughable hoax, millions of dollars in losses are caused by these schemes annually. Some victims have been lured to Nigeria, where they have been imprisoned against their will along with losing large sums of money. The Nigerian government is not sympathetic to victims of these schemes, since the victim actually conspires to remove funds from Nigeria in a manner that is contrary to Nigerian law. The schemes themselves violate section 419 of the Nigerian criminal code, hence the label "419 fraud."

Tips for Avoiding Nigerian Letter or "419" Fraud:

- If you receive a letter from Nigeria asking you to send personal or banking information, do not reply in any manner. Send the letter to the U.S. Secret Service, your local FBI office, or the U.S. Postal Inspection Service. You can also register a complaint with the Federal Trade Commission's Complaint Assistant.
- If you know someone who is corresponding in one of these schemes, encourage that person to contact the FBI or the U.S. Secret Service as soon as possible.
- Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.

Advance Fee Schemes

An advance fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value—such as a loan, contract, investment, or gift—and then receives little or nothing in return.

The variety of advance fee schemes is limited only by the imagination of the con artists who offer them. They may involve the sale of products or services, the offering of investments, lottery winnings, "found money," or many other "opportunities." Clever con artists will offer to find financing arrangements for their clients who pay a "finder's fee" in advance. They require their clients to sign contracts in which they agree to

pay the fee when they are introduced to the financing source. Victims often learn that they are ineligible for financing only after they have paid the "finder" according to the contract. Such agreements may be legal unless it can be shown that the "finder" never had the intention or the ability to provide financing for the victims.

Tips for Avoiding Advanced Fee Schemes:

- If the offer of an "opportunity" appears too good to be true, it probably is. Follow common business practice. For example, legitimate business is rarely conducted in cash on a street corner.
- Know who you are dealing with. If you have not heard of a person or company that you intend to do business with, learn more about them. Depending on the amount of money that you plan on spending, you may want to visit the business location, check with the Better Business Bureau, or consult with your bank, an attorney, or the police.
- Make sure you fully understand any business agreement that you enter into. If the terms are complex, have them reviewed by a competent attorney.
- Be wary of businesses that operate out of post office boxes or mail drops and do not have a street address. Also be suspicious when dealing with persons who do not have a direct telephone line and who are never in when you call, but always return your call later.
- Be wary of business deals that require you to sign nondisclosure or non-circumvention agreements that are designed to prevent you from independently verifying the bona fides of the people with whom you intend to do business. Con artists often use non-circumvention agreements to threaten their victims with civil suit if they report their losses to law enforcement.

Fake Check Scams

- You unexpectedly receive notice that you are getting a grant from the government or a foundation and a processing fee is required.
- A company hires you to work at home as a mystery shopper or processing payments and instructs you to send money somewhere as part of the job.

- Someone sends you more than the asking price for an item you are selling and instructs you to wire the extra money somewhere else.
- A stranger sends part of the profits you were promised in a foreign business deal and asks you to pay legal fees to get the rest.
- Someone you meet online asks you to cash a check or money order as a favor. No matter the story, fake check scams always involve someone giving you a genuine-looking check or money order and asking you to wire money somewhere in return. After you deposit or cash the check or money order and send the money, you learn that it was phony. Now the crook has the money and you owe it back to your bank or credit union.

Your bank or credit union confirms that the check or money order is legitimate before letting you have the money, right?

Wrong. Federal law allows you to get the cash quickly, usually within 1-2 days. But your bank or credit union cannot tell if there is a problem with a check or money order until it goes through the system to the person or company that supposedly issued it. This can take weeks. You are responsible because you are in the best position to know if the person who gave you the check or money order is trustworthy. Victims typically lose $3,000-$4,000. Once the counterfeit is discovered, your bank or credit union will deduct the amount of the check or money order from your account.

But that's not all:

- If there is not enough in your account to cover the amount, you could face collection or be sued.
- Your account may be frozen or closed, and you could be reported to a database of checking account abusers, making it difficult to open another account.
- Some victims are even charged with check fraud. You will also have to repay the money if you cash fake checks or money orders at check cashing services or stores. If you are a fake check victim, try to resolve the problem immediately with your bank, credit union or check-casher.

How can you protect yourself?

There is no legitimate reason why anyone would give you a check or money order and ask you to send money anywhere in return. If that is the deal, it is a scam. Phony sweepstakes, lotteries and grants, work-at-home schemes, foreign business deals and other scams are not new and do not always involve fake checks – sometimes the crooks simply ask you to send money. But using realistic-looking checks or money orders makes their stories more convincing.

Requests for payment to claim prizes are illegal. Real winners pay taxes directly to the government.

- Government agencies and foundations do not hand out "free" money. They usually provide grants for specific projects based on extensive applications.
- Unexpected offers to make money in a foreign business deal are never legitimate.
- Companies that hire people to work from home do not ask them to send money.
- Scammers ask for payment through money transfer services because it is fast and hard to trace. Only use these services to send money to people you have met in person and known for a long time.

Redemption / Strawman / Bond Fraud

Proponents of this scheme claim that the U.S. government or the Treasury Department control bank accounts—often referred to as "U.S. Treasury Direct Accounts"—for all U.S. citizens that can be accessed by submitting paperwork with state and federal authorities. Individuals promoting this scam frequently cite various discredited legal theories and may refer to the scheme as "Redemption," "Strawman," or "Acceptance for Value." Trainers and websites will often charge large fees for "kits" that teach individuals how to perpetrate this scheme. They will often imply that others have had great success in discharging debt and purchasing merchandise such as cars and homes. Failures to implement the scheme successfully are attributed to individuals not following instructions in a specific order or not filing paperwork at correct times.

This scheme predominately uses fraudulent financial documents that appear to be legitimate. These documents are frequently referred to as "bills of exchange," "promissory bonds," "indemnity bonds," "offset bonds," "sight drafts," or "comptrollers war-

rants." In addition, other official documents are used outside of their intended purpose, like IRS forms 1099, 1099-OID, and 8300. This scheme frequently intermingles legal and pseudo legal terminology in order to appear lawful. Notaries may be used in an attempt to make the fraud appear legitimate. Often, victims of the scheme are instructed to address their paperwork to the U.S. Secretary of the Treasury.

Tips for Avoiding Redemption/Strawman/Bond Fraud:

- Be wary of individuals or groups selling kits that they claim will inform you on to access secret bank accounts.
- Be wary of individuals or groups proclaiming that paying federal and/or state income tax is not necessary.
- Do not believe that the U.S. Treasury controls bank accounts for all citizens.
- Be skeptical of individuals advocating that speeding tickets, summons, bills, tax notifications, or similar documents can be resolved by writing "acceptance for value" on them.
- If you know of anyone advocating the use of property liens to coerce acceptance of this scheme, contact your local FBI office.

Letter of Credit Fraud

Legitimate letters of credit are never sold or offered as investments. They are issued by banks to ensure payment for goods shipped in connection with international trade. Payment on a letter of credit generally requires that the paying bank receive documentation certifying that the goods ordered have been shipped and are en route to their intended destination. Letters of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped.

Other letter of credit frauds occur when con artists offer a "letter of credit" or "bank guarantee" as an investment wherein the investor is promised huge interest rates on the order of 100 to 300 percent annually. Such investment "opportunities" simply do not exist. (See Prime Bank Notes for additional information.)

Tips for Avoiding Letter of Credit Fraud:

- If an "opportunity" appears too good to be true, it probably is.
- Do not invest in anything unless you understand the deal. Con artists rely on complex transactions and faulty logic to "explain" fraudulent investment schemes.
- Do not invest or attempt to "purchase" a "letter of credit." Such investments simply do not exist.
- Be wary of any investment that offers the promise of extremely high yields.
- Independently verify the terms of any investment that you intend to make, including the parties involved and the nature of the investment.

Prime Bank Note Fraud

International fraud artists have invented an investment scheme that supposedly offers extremely high yields in a relatively short period of time. In this scheme, they claim to have access to "bank guarantees" that they can buy at a discount and sell at a premium. By reselling the "bank guarantees" several times, they claim to be able to produce exceptional returns on investment. For example, if $10 million worth of "bank guarantees" can be sold at a two percent profit on 10 separate occasions—or "traunches"—the seller would receive a 20 percent profit. Such a scheme is often referred to as a "roll program."

To make their schemes more enticing, con artists often refer to the "guarantees" as being issued by the world's "prime banks," hence the term "prime bank guarantees." Other official sounding terms are also used, such as "prime bank notes" and "prime bank debentures." Legal documents associated with such schemes often require the victim to enter into non-disclosure and non-circumvention agreements, offer returns on investment in "a year and a day", and claim to use forms required by the International Chamber of Commerce (ICC). In fact, the ICC has issued a warning to all potential investors that no such investments exist.

The purpose of these frauds is generally to encourage the victim to send money to a foreign bank, where it is eventually transferred to an off-shore account in the control of the con artist. From there, the victim's money is used for the perpetrator's personal

expenses or is laundered in an effort to make it disappear.

While foreign banks use instruments called "bank guarantees" in the same manner that U.S. banks use letters of credit to insure payment for goods in international trade, such bank guarantees are never traded or sold on any kind of market.

Tips for Avoiding Prime Bank Note Fraud:

- Think before you invest in anything. Be wary of an investment in any scheme, referred to as a "roll program," that offers unusually high yields by buying and selling anything issued by "prime banks."
- As with any investment, perform due diligence. Independently verify the identity of the people involved, the veracity of the deal, and the existence of the security in which you plan to invest.
- Be wary of business deals that require non-disclosure or non-circumvention agreements that are designed to prevent you from independently verifying information about the investment.

Ponzi Schemes

Ponzi schemes promise high financial returns or dividends not available through traditional investments. Instead of investing the funds of victims, however, the con artist pays "dividends" to initial investors using the funds of subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."

This type of fraud is named after its creator—Charles Ponzi of Boston, Mass. In the early 1900s, Ponzi launched a scheme that guaranteed investors a 50 percent return on their investment in postal coupons. Although he was able to pay his initial backers, the scheme dissolved when he was unable to pay later investors.

Tips for Avoiding Ponzi Schemes:

- Be careful of any investment opportunity that makes exaggerated earnings claims.
- Exercise due diligence in selecting investments and the people with whom you

invest—in other words, do your homework.

- Consult an unbiased third party—like an unconnected broker or licensed financial advisor—before investing.

Pyramid Schemes

As in Ponzi schemes, the money collected from newer victims of the fraud is paid to earlier victims to provide a veneer of legitimacy. In pyramid schemes, however, the victims themselves are induced to recruit further victims through the payment of recruitment commissions.

More specifically, pyramid schemes—also referred to as franchise fraud or chain referral schemes—are marketing and investment frauds in which an individual is offered a distributorship or franchise to market a particular product.

The real profit is earned, not by the sale of the product, but by the sale of new distributorships. Emphasis on selling franchises rather than the product eventually leads to a point where the supply of potential investors is exhausted and the pyramid collapses. At the heart of each pyramid scheme is typically a representation that new participants can recoup their original investments by inducing two or more prospects to make the same investment. Promoters fail to tell prospective participants that this is mathematically impossible for everyone to do, since some participants drop out, while others recoup their original investments and then drop out.

Tips for Avoiding Pyramid Schemes:

- Be wary of "opportunities" to invest your money in franchises or investments that require you to bring in subsequent investors to increase your profit or recoup your initial investment.
- Independently verify the legitimacy of any franchise or investment before you invest.

Market Manipulation or "Pump and Dump" Fraud

This scheme—commonly referred to as a "pump and dump"—creates artificial buy-

ing pressure for a targeted security, generally a low-trading volume issuer in the over-the-counter securities market largely controlled by the fraud perpetrators. This artificially increased trading volume has the effect of artificially increasing the price of the targeted security (i.e., the "pump"), which is rapidly sold off into the inflated market for the security by the fraud perpetrators (i.e., the "dump"); resulting in illicit gains to the perpetrators and losses to innocent third party investors.

Typically, the increased trading volume is generated by inducing unwitting investors to purchase shares of the targeted security through false or deceptive sales practices and/or public information releases.

A modern variation on this scheme involves largely foreign-based computer criminals gaining unauthorized access to the online brokerage accounts of unsuspecting victims in the United States. These victim accounts are then utilized to engage in coordinated online purchases of the targeted security to affect the pump portion of a manipulation, while the fraud perpetrators sell their pre-existing holdings in the targeted security into the inflated market to complete the dump.

Tips for Avoiding Market Manipulation Fraud:

- Don't believe the hype.
- Find out where the stock trades.
- Independently verify claims.
- Research the opportunity.
- Beware of high-pressure pitches.
- Always be skeptical.

Identity Theft

Identity theft occurs when someone assumes your identity to perform a fraud or other criminal act. Criminals can get the information they need to assume your identity from a variety of sources, including by stealing your wallet, rifling through your trash, or by compromising your credit or bank information. They may approach you in person, by telephone, or on the Internet and ask you for the information.

The sources of information about you are so numerous that you cannot prevent the theft of your identity. But you can minimize your risk of loss by following a few simple hints.

Tips for Avoiding Identity Theft:

- Never throw away ATM receipts, credit statements, credit cards, or bank statements in a usable form.
- Never give your credit card number over the telephone unless you make the call.
- Reconcile your bank account monthly, and notify your bank of discrepancies immediately.
- Keep a list of telephone numbers to call to report the loss or theft of your wallet, credit cards, etc.
- Report unauthorized financial transactions to your bank, credit card company, and the police as soon as you detect them.
- Review a copy of your credit report at least once each year. Notify the credit bureau in writing of any questionable entries and follow through until they are explained or removed.
- If your identity has been assumed, ask the credit bureau to print a statement to that effect in your credit report.
- If you know of anyone who receives mail from credit card companies or banks in the names of others, report it.

Fraud Against Senior Citizens

Senior Citizens especially should be aware of fraud schemes for the following reasons:

- Senior citizens are most likely to have a "nest egg," to own their home, and/or to have excellent credit—all of which make them attractive to con artists.
- People who grew up in the 1930s, 1940s, and 1950s were generally raised to be polite and trusting. Con artists exploit these traits, knowing that it is difficult or impossible for these individuals to say "no" or just hang up the telephone.
- Older Americans are less likely to report a fraud because they don't know who to report it to, are too ashamed at having been scammed, or don't know they have been scammed. Elderly victims may not report crimes, for example, because they are concerned that relatives may think the victims no longer have the mental capacity to take care of their own financial affairs.
- When an elderly victim does report the crime, they often make poor witnesses. Con artists know the effects of age on memory, and they are counting on elderly victims not being able to supply enough detailed information to investigators. In addition, the victims' realization that they have been swindled may take weeks—or more likely, months—after contact with the fraudster. This extended time frame makes it even more difficult to remember details from the events.
- Senior citizens are more interested in and susceptible to products promising increased cognitive function, virility, physical conditioning, anti-cancer properties, and so on. In a country where new cures and vaccinations for old diseases have given every American hope for a long and fruitful life, it is not so unbelievable that the con artists' products can do what they claim.

Counterfeit Prescription Drugs

Tips for Avoiding Counterfeit Prescription Drugs:

- Be mindful of appearance. Closely examine the packaging and lot numbers of prescription drugs and be alert to any changes from one prescription to the next.

- Consult your pharmacist or physician if your prescription drug looks suspicious.
- Alert your pharmacist and physician immediately if your medication causes adverse side effects or if your condition does not improve.
- Use caution when purchasing drugs on the Internet. Do not purchase medications from unlicensed online distributors or those who sell medications without a prescription. Reputable online pharmacies will have a seal of approval called the Verified Internet Pharmacy Practice Site (VIPPS), provided by the Association of Boards of Pharmacy in the United States.
- Be aware that product promotions or cost reductions and other "special deals" may be associated with counterfeit product promotion.

Funeral and Cemetery Fraud

Tips for Avoiding Funeral and Cemetery Fraud:

- Be an informed consumer. Take time to call and shop around before making a purchase. Take a friend with you who may offer some perspective to help make difficult decisions. Funeral homes are required to provide detailed general price lists over the telephone or in writing.
- Educate yourself fully about caskets before you buy one, and understand that caskets are not required for direct cremations.
- Understand the difference between funeral home basic fees for professional services and any fees for additional services.
- Know that embalming rules are governed by state law and that embalming is not legally required for direct cremations.
- Carefully read all contracts and purchasing agreements before signing and make certain that all of your requirements have been put in writing.
- Make sure you understand all contract cancellation and refund terms, as well as your portability options for transferring your contract to other funeral homes.
- Before you consider prepaying, make sure you are well informed. When you do

make a plan for yourself, share your specific wishes with those close to you.

- As a general rule governing all of your interactions as a consumer, do not allow yourself to be pressured into making purchases, signing contracts, or committing funds. These decisions are yours and yours alone.

Fraudulent Anti-Aging Products

Tips for Avoiding Fraudulent "Anti-Aging" Products:

- If it sounds too good to be true, it probably is. Watch out for "Secret Formulas" or "Breakthroughs."
- Don't be afraid to ask questions about the product. Find out exactly what it should and should not do for you.
- Research a product thoroughly before buying it. Call the Better Business Bureau to find out if other people have complained about the product.
- Be wary of products that claim to cure a wide variety of illnesses—particularly serious ones—that don't appear to be related.
- Be aware that testimonials and/or celebrity endorsements are often misleading.
- Be very careful of products that are marketed as having no side effects.
- Question products that are advertised as making visits to a physician unnecessary.
- Always consult your doctor before taking any dietary or nutritional supplement.

Reverse Mortgage Scams

The FBI and the U.S. Department of Housing and Urban Development Office of Inspector General (HUD-OIG) urge consumers, especially senior citizens, to be vigilant when seeking reverse mortgage products. Reverse mortgages, also known as home equity conversion mortgages (HECM), have increased more than 1,300 percent between 1999 and 2008, creating significant opportunities for fraud perpetrators.

Reverse mortgage scams are engineered by unscrupulous professionals in a multi-

tude of real estate, financial services, and related companies to steal the equity from the property of unsuspecting senior citizens or to use these seniors to unwittingly aid the fraudsters in stealing equity from a flipped property.

In many of the reported scams, victim seniors are offered free homes, investment opportunities, and foreclosure or refinance assistance. They are also used as straw buyers in property flipping scams. Seniors are frequently targeted through local churches and investment seminars, as well as television, radio, billboard, and mailer advertisements.

A legitimate HECM loan product is insured by the Federal Housing Authority. It enables eligible homeowners to access the equity in their homes by providing funds without incurring a monthly payment. Eligible borrowers must be 62 years or older who occupy their property as their primary residence and who own their property or have a small mortgage balance. See the FBI/HUD Intelligence Bulletin for specific details on HECMs as well as other foreclosure rescue and investment schemes.

Tips for Avoiding Reverse Mortgage Scams:

- Do not respond to unsolicited advertisements.
- Be suspicious of anyone claiming that you can own a home with no down payment.
- Do not sign anything that you do not fully understand.
- Do not accept payment from individuals for a home you did not purchase.
- Seek out your own reverse mortgage counselor. If you are a victim of this type of fraud and want to file a complaint, please submit information through our electronic tip line or through your local FBI office. You may also file a complaint with HUD-OIG at

www.hud.gov/complaints/fraud_waste.cfm or by calling HUD's hotline at 1-800-347-3735.

Long Term Care Insurance Scams

- Selling unsuitable policies. Dishonest insurance providers knowingly sell expen-

sive policies to people who can't afford the high premiums. Another scam involves selling two expensive and overlapping policies when only one is needed. Low-income people and seniors on fixed incomes often are targeted. Sales pitches may aggressively prey on people's fear that high medical costs will leave them destitute or a burden on family members.

- Churning policies. You're urged to cancel a perfectly good policy and "trade up" to a "better" policy from your current insurer or another company. The replacement policy may be more expensive and offer little or no improvement. You're also forfeiting years of premiums you've paid for your previous policy. You also may be denied key benefits under the new policy based on pre-existing conditions if your medical needs have changed.
- Deceptively watered coverage. To close the sale, the seller may deceptively eliminate or reduce vital policy features so you can afford the premium. You aren't told that critical benefits such as inflation protection were watered down or eliminated. Nor are you told how such changes could affect your medical care or expose you to high out-of-pocket costs.
- Overstating benefits. You might be told the policy covers "all" of your long-term medical expenses. But this may not be true — read the policy's fine print. For example, does the policy adequately adjust current benefits for future inflation when you need care in future years? Are you aware of other stated policy limits and restrictions? If not, you may have to pay a large portion of medical expenses out of pocket.
- Making misstatements on applications. Deliberate misstatements about your current medical condition, age, past medical history or other key information are entered onto the policy application to secure the coverage or lower the premium. Agents or policy applicants might use this fraudulent tactic.
- Selling phony policies. Watch out for fake coverage, especially bogus home health care coverage. These schemes steal your premiums and leave you without vital protection when you need it the most.

Telemarketing Fraud

When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud.

Here are some warning signs of telemarketing fraud—what a caller may tell you:

- "You must act 'now' or the offer won't be good."
- "You've won a 'free' gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.
- "You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.
- "You don't need to check out the company with anyone." The callers say you do not need to speak to anyone including your family, lawyer, accountant, local Better Business Bureau, or consumer protection agency.
- "You don't need any written information about their company or their references."
- "You can't afford to miss this 'high-profit, no-risk' offer."

If you hear these or similar "lines" from a telephone salesperson, just say "no thank you" and hang up the telephone.

It's very difficult to get your money back if you've been cheated over the telephone. Before you buy anything by telephone, remember:

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware—not everything written down is true.

- Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.
- Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.
- Before you give money to a charity or make an investment, find out what percentage of the money is paid in commissions and what percentage actually goes to the charity or investment.
- Before you send money, ask yourself a simple question. "What guarantee do I really have that this solicitor will use my money in the manner we agreed upon?"
- Don't pay in advance for services. Pay services only after they are delivered.
- Be wary of companies that want to send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.
- Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.
- Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- Before you receive your next sales pitch, decide what your limits are—the kinds of financial information you will and won't give out on the telephone.
- Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor. It's never rude to wait and think about an offer.
- Never respond to an offer you don't understand thoroughly.
- Never send money or give out personal information such as credit card numbers

and expiration dates, bank account numbers, dates of birth, or Social Security numbers to unfamiliar companies or unknown persons.

- Be aware that your personal information is often brokered to telemarketers through third parties.
- If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.
- If you have information about a fraud, report it to state, local, or federal law enforcement agencies.

Telemarketing Fraud

If you are age 60 or older—and especially if you are an older woman living alone—you may be a special target of people who sell bogus products and services by telephone. Telemarketing scams often involve offers of free prizes, low-cost vitamins and health care products, and inexpensive vacations.

There are warning signs to these scams. If you hear these—or similar—"lines" from a telephone salesperson, just say "no thank you," and hang up the telephone:

- "You must act now, or the offer won't be good."
- "You've won a free gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.
- "You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.
- "You don't need to check out the company with anyone." The callers say you do not need to speak to anyone, including your family, lawyer, accountant, local Better Business Bureau, or consumer protection agency.
- "You don't need any written information about the company or its references."
- "You can't afford to miss this high-profit, no-risk offer." Fraud Target: Senior Citizens

Tips for Avoiding Telemarketing Fraud:

It's very difficult to get your money back if you've been cheated over the telephone. Before you buy anything by telephone, remember:

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware—not everything written down is true.
- Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center, or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.
- Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.
- Before you give money to a charity or make an investment, find out what percentage of the money is paid in commissions and what percentage actually goes to the charity or investment.
- Before you send money, ask yourself a simple question. "What guarantee do I really have that this solicitor will use my money in the manner we agreed upon?"
- Don't pay in advance for services. Pay services only after they are delivered.
- Be wary of companies that want to send a messenger to your home to pick up money, claiming it is part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.
- Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.

- Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- Before you receive your next sales pitch, decide what your limits are—the kinds of financial information you will and won't give out on the telephone.
- Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor. It's never rude to wait and think about an offer.
- Never respond to an offer you don't understand thoroughly.
- Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or Social Security numbers to unfamiliar companies or unknown persons.
- Be aware that your personal information is often brokered to telemarketers through third parties.
- If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.
- If you have information about a fraud, report it to state, local, or federal law enforcement agencies.

Automobile Insurance Fraud

The National Insurance Crime Bureau trade group tracks fraud for insurers and ranks California, Florida, Texas, New York and Maryland as the top five states for fishy auto insurance claims.

The cost to motorists is tough to pin down because fraud often goes unreported, but it's definitely a "major-league crime involving a wide variety of schemes," says Jim Quiggle, a spokesman for the Coalition Against Insurance Fraud in Washington, D.C.

Nationally, experts believe overall insurance fraud costs tens of billions of dollars every year.

Learn how to protect yourself as we uncover the worst auto insurance frauds.

- **Air Bags**

Each year, about 1.5 million air bags inflate during crashes, saving thousands of lives. But, during the repair process, at least a small percentage of those deployed air bags will be replaced with counterfeits -- which can be life-threatening.

"Crooked repair shops frequently replace the bags with cheap knockoffs, or in some cases just fill the area with junk and garbage," says Quiggle. "The insurer pays for phony work, and the driver ends up with a car that isn't safe."

If your car is being fixed after the air bags have been deployed, it's critical to work with a trusted, reputable mechanic, says Quiggle. He advises drivers to go with shops that have been approved by their insurance company, because those will have been heavily vetted.

If you're buying a used car, it's always a good idea to get a vehicle report, which will tell if the car has been damaged in a crash or has been salvaged. Then, pay close attention to the air bag light, which should appear briefly and then turn off. If the light never appears, if it flashes steadily or if it stays on, the car should be checked immediately.

- **Staged Accidents**

Staged accidents are rising at an alarming rate, according to the National Insurance

Crime Bureau. Insurers across the U.S. reported a 102 percent increase in suspected cases of this type of fraud from 2008 to 2011, the bureau says.

Nationwide Insurance says common types of staged crashes include:

Swoop and squat: Two vehicles trap a victim in a rear-end collision.

Drive down: When waiting to make a left turn, the victim is lured into turning early by an oncoming fraudster who waits and then proceeds just in time to collide.

Wave down: Two vehicles set up a crash with a victim who's given a wave that it's safe to pull out of a parking lot or side street.

Enhanced damages: In a legitimate accident, the not-at-fault driver causes additional damage to his or her own vehicle to pump up the claim.

Florida lawyer Russel Lazega advises anyone who has been in a wreck to gather as much evidence as possible right away.

"Often car crash cases don't make it to court until years later, when witnesses are gone and cars have been fixed," he says. "Demand a police report, take lots of pictures and get the contact information for any witnesses."

- **Insurance Agents**

Most agents are honest, but if you buy your auto insurance coverage through an agent who isn't on the up and up, it can cost you. The Coalition Against Insurance Fraud says one of the worst-case scenarios involves a shady agent who just steals your premiums outright. The unscrupulous agent pockets your money but doesn't actually set up the coverage, so when an accident occurs, you find that you have no insurance to pay your claim and must cover the loss on your own.

To avoid premium theft, drivers should work with trusted agents and always verify their coverage independently with the carrier.

Also common is a practice known as "sliding," in which an unethical agent slips extra coverage that you didn't want into your policy. This particularly sneaky form of auto insurance fraud can add a few hundred dollars a year to your premiums while padding the agent's commission.

Vigilant drivers who investigate their agents ahead of time and keep a close eye on

what they're buying won't fall victim to sliding scams.

- **Windshield Replacement**

A stranger approaches you at a parking lot and says he's with a vehicle glass company. He tells you that you need a new windshield, which he can provide free of charge if you provide your insurance information. Sounds good, right? Well, it's probably too good to be true. According to Farmers Insurance, the windshield replacement offer is almost always a scam. And the risks may be greater than many people realize.

For starters, the quality of the replacement windshield and the repair work usually aren't all that good, which means you could be putting your safety at risk. This scam also can do a number on your insurance coverage, says Quiggle.

"Once they have your insurance information, a scammer will often submit false claims under your policy," he says. "You'll have to go through the headache of clearing up those false claims, but in the meantime they can raise your premium and -- if there are enough false claims -- you can even lose your coverage."

Experts say the best thing is to walk away from the offer. If you do need your windshield replaced, call your insurance agent in advance to see what is and isn't covered.

- **Towing**

At first glance, a friendly tow truck happening by after an accident or breakdown can seem like a godsend. But if you didn't call for a tow, there's a good chance it's what authorities call a "bandit" tow truck, which means you'll get your tow and an eye-popping bill. There are a couple of easy ways to protect yourself. If you have AAA or belong to another roadside assistance program, that's where you should turn when you need a tow because you'll benefit from lower pre-negotiated rates.

Or, your auto insurance policy may offer roadside assistance. If you use it when an accident renders your vehicle undriveable, it's a good idea to ask about the policy's limits on towing and storage before you leave the scene.

If you must use an independent tow truck, it's best to call for one rather than go with a truck that's just passing by. It's also critical that you read the fine print before signing any towing contract. Experts say you should get a printed price or invoice of all towing and storage charges and any miscellaneous fees. The contract also should specify to where your vehicle is being towed.

Medical and Insurance Fraud

Medical Equipment Fraud:

Equipment manufacturers offer "free" products to individuals. Insurers are then charged for products that were not needed and/or may not have been delivered.

"Rolling Lab" Schemes:

Unnecessary and sometimes fake tests are given to individuals at health clubs, retirement homes, or shopping malls and billed to insurance companies or Medicare.

Services Not Performed:

Customers or providers bill insurers for services never rendered by changing bills or submitting fake ones.

Medicare Fraud:

Medicare fraud can take the form of any of the health insurance frauds described above. Senior citizens are frequent targets of Medicare schemes, especially by medical equipment manufacturers who offer seniors free medical products in exchange for their Medicare numbers. Because a physician has to sign a form certifying that equipment or testing is needed before Medicare pays for it, con artists fake signatures or bribe corrupt doctors to sign the forms.

Once a signature is in place, the manufacturers bill Medicare for merchandise or service that was not needed or was not ordered.

Tips for Avoiding Health Care Fraud or Health Insurance Fraud:

- Never sign blank insurance claim forms.
- Never give blanket authorization to a medical provider to bill for services rendered.
- Ask your medical providers what they will charge and what you will be expected to pay out-of-pocket.

- Carefully review your insurer's explanation of the benefits statement. Call your insurer and provider if you have questions.
- Do not do business with door-to-door or telephone salespeople who tell you that services of medical equipment are free.
- Give your insurance/Medicare identification only to those who have provided you with medical services.
- Keep accurate records of all health care appointments.
- Know if your physician ordered equipment for you.

Dental

- Worthless treatment. Dishonest dentists perform useless surgery on perfectly healthy patients to hike their own insurance billings. The dentists remove healthy teeth, do root canals that aren't needed, and drill for cavities that don't exist. Sometimes children's teeth are even drilled without painkiller. Often the surgery is botched: Shoddy crowns or fillings fall out. Patients have found surgical debris embedded in their gums. Patients also become painfully infected and disfigured, and need more surgery to correct the treatments.
- Inflated billings. Dishonest dentists do minor procedures such as routine tooth cleanings, but bill your insurance plan for costlier treatments such as phantom root canals or cavity fillings.
- Phantom treatment. Dentists bill insurers for treatments they never perform. They send the insurer forged bills for fake treatment, medicine and supplies they never used. They may bill the policies of current patients, or invent "patients" they've never even met.
- Unlicensed dentists and employees. Sometimes dentists illegally treat patients despite losing their licenses for previous infractions. Some dentists also have hygienists, assistants or other staff perform treatments — even though they aren't licensed or qualified. The dentists then bill insurers as if the dentists performed the treatment themselves. And you could receive shoddy treatment.

- Fake dental plans. Con artists sell fake dental insurance to people and businesses. This leaves you dangerously unprotected when you need costly dental treatment. Typically the plan operators are shady businesspeople, not dentists.

Medical Identity Scams

- Illegal and bogus treatment. Medical ID thieves bill your health plan for fake or inflated treatment claims. The crooks often are doctors and other medical personnel who know how the insurance billing system works. Organized theft rings also are involved. They buy stolen patient information on the black market, and set up fake clinics to make bogus claims against the health policies of honest consumers.
- Medical personnel with access to your data may use your identity to obtain prescription drugs to sell, or feed their own addictions. Dishonest pharmacists might bill your policy for narcotics, or nurses may call in prescriptions in a patient's name but pick it up themselves.
- Medical ID thieves who don't have their own health coverage often receive free medical treatment, courtesy of your policy. They assume your identity at a hospital or clinic, and your policy receives the bills.

False Medical Claims

- Phantom treatments. Dishonest medical providers will bill health insurers for expensive treatments, tests or equipment you never received - and for illnesses or injuries you don't even have.
- Double billing. Unethical providers may double- or triple-bill health insurers for the same treatments, hoping the insurer won't discover the overruns in the big stack of bills.
- Shoddy care. You might receive shoddy or substandard treatment for real and urgent medical problems. One eye doctor shined pen lights into patients' eyes and said he'd performed cataract surgery. Surgeons have used defective pacemakers and catheters during heart surgeries, which have killed patients or required more surgeries to correct the problems.

- Unneeded care. You might receive dangerous and even life-threatening treatment you don't need. One surgeon performed heart surgery on patients who didn't need it.
- Bogus insurers. Insurance agents or brokers sell you low-cost health coverage from fake insurance companies. Then they take your premiums and disappear. You're left without vital health coverage, and don't even know it until you make a claim.
- Identity theft. Cheaters steal your medical ID number, then use it to bill health programs tens of thousands of dollars for phantom treatment. Crooks steal your health info from dumpsters behind medical clinics, break into doctor offices and steal files, and hack into computer databases containing your records.
- Rolling labs. Mobile diagnostic labs give needless or fake tests or physical exams to consumers, then bill health insurers for expensive procedures.
- Runners. A person hired by a medical provider to drum up business trolls through neighborhoods, often low-income areas, enticing people to come to a clinic for tests. These runners will even round up children for unneeded tests and procedures.

Discount Cards for Insurance

- Pretend insurance. Discount medical plans aren't health insurance. But their ads use insurance-like terms such as "health benefits" and "protection." People are conned into signing up, trusting they have real health coverage.
- Bogus provider list. Shady plans lie that they have large networks of medical providers willing to provide discounted services. Often the providers don't even know their names are falsely on the list. Thus they're unlikely to provide the advertised discounts when plan members call.
- Hidden fees. Added fees are stashed in the fine print of your contract.
- Fake plan. Sometimes the discount plan is totally fake, offers no services or discounts, and has no intention of making good on its promises. The plan exists only to fool people into paying fees that line the pockets of the sham operation's masterminds.

Obamacare Scams

- Fake navigators. They pretend they're official navigators helping you find coverage. They may knock on your door, or cold-call via telephone. They also forge official-looking badges and other ID. Among the potential navigator ruses:
- Charge an illegal "signup fee" and ask for your credit card and banking numbers. Navigators aren't allowed to take money or charge.
- Show you fake online insurance applications or a bogus online signup portal on their laptop. The portal may request your sensitive financial information to "sign you up for the exchange."
- Sell fake insurance. You're left with large medical expenses when the worthless policy refuses to pay the bills.
- Phony exchange websites. Bogus sites might look real — you'll see the state seal, the word "Exchange" and your state name on the homepage. The thief also might copycat a real exchange site.
- Email pitches. Spam emails arrive, supposedly from your exchange. But they could be rigged. You open the link and it takes you to a fake exchange or other "official" signup engine that requests your sensitive financial information. Opening the link also might install malware on your computer.

Seniors. Cheaters lie that the federal government needs to provide them a new Medicare card as "required" by the Affordable Care Act. The fake federal employee just needs to "verify" the senior's bank account, credit card and SSN. Another version: The scammer wants to sign up the senior for "Obamacare" insurance.

- The big lie: The ACA doesn't require new Medicare cards. Medicare doesn't call seniors. And seniors with Medicare already have insurance. So they don't need to seek coverage in the Health Insurance Marketplace.
- Contact your nearest Medicare Patrol to learn about "Obamacare" scams, and report them.
- Stay informed about healthcare reform. It's your best defense. AARP has a wide variety of helpful info for seniors.

Obamacare signup cons. Crooks knocked on doors and cold-called before the October 2013 open enrollment began. They lied that they were federal employees sent to sign consumers up for a "required national Obamacare health card." They demanded a "signup fee" and sensitive financial information to properly "register." Look out for new versions of this scam.

Medicare Scams

Crooks posing as representatives of Medicare or private prescription plans may offer to "explain" the new coverage to seniors, and "help" seniors sign up. They may fraudulently….

- Request your sensitive personal financial information such as Social Security, Medicare, credit card and checking account numbers. Truth: Crooks can use this information to steal your identity and charge large purchases in your name -- without your permission. Real Medicare drug plans won't request this information.
- Approach you door to door. Truth: Medicare forbids such tactics unless you invite the marketer into your home.
- Ask you to enroll or pay signup fees over the phone. Truth: Medicare doesn't permit phone payments. Approved plans can only do general marketing via telephone, and they can enroll you over the phone ONLY if you make the call. Marketers also can make appointments to visit your home to discuss their discount plans. Medicare-approved plans also must comply with federal and state "Do Not Call" laws.
- Ask you to pay signup fees via a website. Truth: Medicare doesn't permit online payment. Plans must send you a bill if you sign up online.
- Illegally market drug plans before October 1, 2005. Truth: Marketing can't begin until October 1.
- Try to illegally enroll you before November 15, 2005. Truth: Enrollment can't begin until November 15.
- Insist you're required to sign up for the drug coverage or else you'll lose Medicare benefits. Truth: Signup is strictly voluntary. You'll keep your Medicare benefits whether or not you sign up.

- Say they're "official" Medicare representatives, or present "official" Medicare marketing material advertising the new drug coverage. Truth: Medicare employees don't personally market a drug plan, recommend specific drug plans, or offer government marketing literature. Only private companies market their own Medicare-approved drug plans. They also use their own material; Medicare doesn't have any. You will receive the Medicare & You handbook from Medicare beginning in October. The handbook provides general information about Medicare and the new drug coverage.

Workers Compensation

Dishonest employees will knowingly make bogus claims for workplace injuries against their employer's workers comp policies.

Free money is the biggest motive. Crooked workers often secretly take a second job or open a side business while falsely claiming they're too injured to work their current job. Thus they receive lost wages from their workers comp policy — and illegally earn extra money from their secret job.

A free vacation is another lure. Dishonest workers collect insurance money and claim they're disabled while pursuing hobbies, sports or other personal activities. Like skydiving, playing soccer, weight lifting or fixing up their home while supposedly injured.

How fake claims work:

- Hurt off the job. Workers get injured off the job, but say they're hurt at work so their workers comp policy covers the medical bills. A person might hurt his neck lifting a heavy box while cleaning the attic. Or maybe sprains an ankle during a softball game. Then he pretends the injury happened at the loading dock at work.
- Inflated injuries. A worker has a fairly minor job injury - maybe a slight twinge in her lower back — but insists her back is seriously sprained. This lets the worker collect more workers comp money and stay off the job longer.
- Fake injuries. Some workers simply invent injuries. Soft-tissue injuries such as muscle problems with the back and neck are popular scams. They're hard to dis-

prove, and thus are easier to get away with.

- Old injury. Sometimes a worker with an old injury that never quite healed will claim he just got hurt on the job. A damaged knee or shoulder, for instance.
- Malingering. Basically, this is goldbricking. Staying at home longer by pretending you're still disabled, even though you've healed enough to return to work.

Stolen Premiums

Dishonest business owners will illegally reduce the workers comp premiums they owe.

Premium swindles can be hard to discover. Businesses often hide their premium scams behind dummy companies, fake accounting, tax records and other cover-ups.

These cons often are complex and well-hidden. They can take much time, effort and financial expertise to discover, and convict in court.

Bogus injury claims far outnumber premium scams, but most premium scams are much larger.

Just one premium swindle can steal several hundred thousand dollars in unpaid premiums in one year. Some premium swindles last for several years - thus stealing millions. A worker's bogus injury claim, however, normally steals $2,000-$50,000 total.

How premium scams work:

- Safer jobs. A crooked business tells the workers comp insurer that many employees work safer jobs than they really do. Example: A construction firm classifies crane operators as file clerks.
- Hidden employees. A business says it has fewer employees or a lower payroll than it actually does. Example: A business owner hides employees by saying they work for a seemingly legitimate dummy firm he created. The owner may falsely claim the workers are independent contractors, and thus don't count toward his workers comp premiums.
- Avoiding coverage. A business simply doesn't buy state-required workers comp

insurance, hoping state officials won't notice. This leaves workers dangerously exposed if they're injured without insurance.

Crooked doctors & lawyers

- Dishonest medical clinics (also called medical mills) and lawyers often team up to scam workers comp insurance. These often are well-organized criminal gangs. One gang can steal millions of dollars a year.

How doctor & lawyer scams work:

- Inflated injuries. Clinics may inflate the seriousness of real injuries to workers, then bill insurers for costly and worthless treatments and tests. A given treatment may be more expensive than needed, or clinics may order more treatments than necessary.
- Phantom injuries. Clinics may bill insurance for treatment of injuries that never happened.
- Bogus lawsuits. Shady lawyers working with crooked clinics encourage uninjured workers to seek useless treatment for scams. The lawyers then may threaten to sue unless the insurance company settles the phony claim quickly. They gamble that the insurer will decide it's cheaper to settle than face an expensive lawsuit involving a jury that may be sympathetic to a worker.
- Illegal kickbacks. Crooked clinics and lawyers hire recruiters (also called runners) to bring workers into the scams. The runners receive illegal kickbacks for referring patients to the lawyers or clinics. Sometimes the workers are part of the swindle, and sometimes they don't realize a swindle is taking place.
- Fake clinics. Some clinics are bogus. They have no licensed doctors. The office also has little useful medical equipment, and gives almost no helpful or needed treatment. The clinic is merely a staging ground for bogus workers comp claims.

Travel Industry Fraud

Two Weeks in Hawaii for $350! Maybe it's a "certificate" for a bargain vacation. Claims of inexpensive travel are easy to believe, because real bargains are available if you shop carefully.

Check out all travel offers with a reputable travel agency or online. If they want your money right away, before you can think the offer through, odds are it's a scam. Have you ever been tempted to buy one of those bargain-priced travel packages sold over the telephone? Be careful. Your dream adventure may be a misadventure if you fall victim to one of the travel scams sold over the phone. While some of these travel opportunities are legitimate, many of them are scam operations that are defrauding consumers out of millions of dollars each month.

These schemes take many forms. Often, schemes involve vacation travel packages. A consumer pays hundreds of dollars or more to receive a travel package that includes round-trip air transportation for one person and lodging for two people in Hawaii, London, or another vacation place for a week. The catch? You must purchase a high-priced, round-trip ticket for the second person from the fraudulent travel operation or you must pay for costly accommodations in less-than-ideal timeshares or resorts. You may end up paying more than what it would cost if you purchased your own tickets in advance or bought them through an airline or reputable travel agency.

Another scam starts by sending you a postcard stating: "You have been specially selected to receive a free trip." The postcard instructs you to call a phone number, usually toll-free, for details about the trip. Once you call, you are given a sales pitch for a supposedly luxurious trip that is not free at all. Sometimes, a credit card number is requested so that your account can be billed for the package. Only after you pay are you sent the vacation package with instructions on requesting reservations for your trip. Usually, your reservation request must be accompanied by yet another fee. The catch here? New charges are being added at every step of the way. And, you never get your "free" trip because your reservations are not confirmed or you must comply with hard-to-meet hidden or expensive "conditions."

Telemarketing travel scams usually originate out of "boiler rooms." Skilled salespeo-

ple, often with years of experience selling dubious products and services over the phone, pitch travel packages that may sound legitimate, but often are not. These sales pitches usually include some of the following techniques:

- Oral Misrepresentations. Whatever the particular scheme may be, telephone salespeople are likely to promise you a "deal" they cannot deliver. Unfortunately, you often do not realize this until after you have paid your money.
- High Pressure/Time Pressure Tactics. These scam operators are likely to tell you they need your commitment to buy right away or that this special offer will not be available tomorrow. Often, they will brush aside your questions with vague answers.
- "Affordable" Offers. Unlike telephone fraud operators who try to persuade people to spend thousands of dollars on a particular investment scheme, travel scam operators usually pitch their membership or vacation offers in the range of hundreds of dollars. Because this amount is often in the price range of those planning vacations, offers may appear to be reasonably-priced.
- Contradictory Follow-up Material. Some firms may agree to send you written confirmation of the deal. You will find, however, that the literature bears little resemblance to the offer you accepted. Often, the written materials will disclose additional terms, conditions, and costs. No one wants unpleasant surprises on a vacation. Therefore, it pays to thoroughly investigate a travel package before you commit to purchase.

While it is sometimes difficult to tell a legitimate sale pitch from a fraudulent one, there are some things you can do to protect yourself. Be wary of "great deals." One tip-off to a scam is that the offer is very low-priced. Few legitimate businesses can afford to give away things of real value or to undercut substantially everyone else's price. Do not be pressured into buying now. Generally, a good offer today will remain a good offer tomorrow.

Legitimate businesses do not expect you to make an instant decision. Ask detailed questions. Find out exactly what the price covers and does not cover. Ask if there will be any additional charges later. Find out the names of the specific hotels, airports, airlines, and restaurants that your package includes.

You may wish to contact these places yourself to double-check arrangements. Find out exact dates and times. Ask about cancellation policies and refunds. If the salesperson cannot give you detailed answers to these questions, this is not the deal for you. Get all information in writing before you agree to buy. Before purchasing a travel package, ask for detailed written information. Once you receive the information, make sure the written material confirms everything you were told by phone. Do not give your credit card number over the phone.

One easy way for a scam operator to close a deal is to get your credit card number and then charge your account. Sometimes scam operators say they need the number for verification purposes only. Never give your credit or charge card numbers - or any other personal information (such as bank account numbers) - to unsolicited telephone salespeople. Do not send money by messenger or overnight mail. Instead of asking for your credit card number, some scam operators may ask you to send a check or money order right away or offer to send a messenger to pick these up. If you use money rather than a credit card in the transaction, you lose your right to dispute fraudulent charges under the Fair Credit Billing Act. Check out the company. Before buying any travel package, check first with various government and private organizations to see if any complaints have been lodged against the travel firm calling you. Be aware that fraudulent firms change their names frequently to avoid detection. If in doubt, say "no." Sometimes an offer appears legitimate, but you still have doubts. In that case, it is usually better to turn down the offer and hang up the phone. Remember, if something goes wrong, the likelihood of your receiving any money back is very slim. If you have problems with a travel package, try resolving your disputes first with the company that sold you the package. If you are not satisfied, try contacting your local consumer protection agency, Better Business Bureau, or state Attorney General. If you charged your trip to a credit card, you may dispute the charges by writing to your credit card issuer at the address provided for billing disputes. Try to do this as soon as you receive your statement, but no later than 60 days after the bill's statement date. In some circumstances under the Fair Credit Billing Act, your credit card issuer may have to absorb the charges if the seller does not resolve your dispute. If you did not authorize the charge, you are not responsible for its payment.

Social Media Fraud

Social Media Protection Tips

- Use caution when you click links that you receive in messages on your social website. Treat links in messages on these sites as you would links in email messages.
- Know what you've posted about yourself. A common way that hackers break into financial or other accounts is by clicking the "Forgot your password?" link on the account login page. If the site allows, make up your own password questions, and don't draw them from material anyone could find with a quick search.
- Avoid giving away email addresses of your friends and do not allow social networking services to scan your email address book.
- Type the address of your social networking site directly into your browser or use your personal bookmarks. If you click a link to your site through email or another website, you might be entering your account name and password into a fake site where your personal information could be stolen.
- Be selective about who you accept as a friend on a social network. Identity thieves might create fake profiles in order to get information from you.
- Choose your social network carefully. Evaluate the site that you plan to use and make sure you understand the privacy policy. Find out if the site monitors content that people post.
- Assume that everything you put on a social networking site is permanent. Even if you can delete your account, anyone on the Internet can easily print photos or text or save images and videos to a computer.
- Be careful about installing extras on your site. Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information.
- Turn the geotagging feature off. This is the most direct solution and you can find out how to do this for most phones.

Computer Fraud

How to Protect Your Computer

- Keep Your Firewall Turned On:

A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.

- Install or Update Your Antivirus Software:

Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.

- Install or Update Your Antispyware Technology:

Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code. It's like buying groceries—shop where you trust.

- Keep Your Operating System Up to Date:

Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

- Be Careful What You Download:

Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know, and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.

- Turn Off Your Computer:

With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

Internet Fraud

Internet Auction Fraud:

- Understand as much as possible about how the auction works, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the website/company takes if a problem occurs and consider insuring the transaction and shipment.
- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.
- Examine the feedback on the seller.
- Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Be cautious when dealing with sellers outside the United States. If a problem occurs with the auction transaction, it could be much more difficult to rectify.
- Ask the seller about when delivery can be expected and whether the merchandise is covered by a warranty or can be exchanged if there is a problem.
- Make sure there are no unexpected costs, including whether shipping and handling is included in the auction price.
- There should be no reason to give out your Social Security number or driver's license number to the seller.

Internet Non-Delivery of Merchandise:

- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.

- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau from the seller's area.
- Check out other websites regarding this person/company.
- Don't judge a person or company by their website. Flashy websites can be set up quickly.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- Inquire about returns and warranties.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Make sure the transaction is secure when you electronically send your credit card numbers.
- Consider using an escrow or alternate payment service.

Credit Card Fraud:

- Don't give out your credit card number online unless the site is a secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but provides some assurance.

- Don't trust a site just because it claims to be secure.
- Before using the site, check out the security/encryption software it uses.
- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau from the seller's area.
- Check out other websites regarding this person/company.
- Don't judge a person or company by their website. Flashy websites can be set up quickly.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Make sure the transaction is secure when you electronically send your credit card number.
- Keep a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s), contact the card issuer immediately.

Internet Investment Fraud:

- Don't judge a person or company by their website. Flashy websites can be set up quickly.
- Don't invest in anything you are not absolutely sure about. Do your homework on the investment and the company to ensure that they are legitimate.
- Check out other websites regarding this person/company.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- Inquire about all the terms and conditions.

Preventing Online Fraud

- Do not order merchandise while on a public computer or in an establishment with a shared Wi-Fi connection. These networks may not be secure and credit card and other personal information could be stolen.
- If an email or a notice on a friend's Facebook "wall" sounds too good to be true, it probably is. No one is giving out a free iPhone just for filling out a form. Instead, a fraudster will probably use this form to gather personal information to sell to spammers, access accounts or steal identities.
- Do not provide personal information to an unsolicited offer. For instance, if an unsolicited email claims it is from your bank and requests account numbers or other personal data, do not provide this information. If you are unsure if an email is legitimate, follow up first with a phone call before providing information online.
- Be wary of anyone with whom you are doing business who does not use good English or who is in another country.
- Do not wire money to someone you do not know. Fraudsters typically request a wire transfer instead of a check or online payment because it is difficult to trace.

- Do not agree to a "work from home" offer where you just have to cash checks or "reship" items. If someone offers to pay you to do something that does not sound like work, then it probably is not a legitimate job.
- Never give out your Social Security number to someone you do not have a confirmed business relationship with.
- If someone you are dealing with online offers to send you a check and allow you to keep part of it in exchange for wiring part of it back (for whatever reason), do not do it. This check will bounce.

Whenever possible, purchase items online with a credit card. Credit card transactions are traceable and many credit card companies provide protection from fraud.

- Do not believe the promise of large sums of money in exchange for your cooperation.

Make sure you use software that protects your computer from viruses and malware. Malware is a malicious software that can steal personal information and disrupt your computer's operations.

- Use strong passwords when conducting any type of online business. A strong password combines symbols and numbers with upper and lower case letters, and is nine or more characters in length. Periodically change your passwords, and never use the same password for multiple accounts.
- Protect the important files and information on your computer by backing up data via a reputable company, backup software or external hard drive.

Home Improvement Fraud

Each year when the weather turns nice, itinerant crews of roofers, pavers and day laborers travel from city to city, driving through neighborhoods and mobile home parks looking for victims -- mostly the elderly. Sometimes they offer to pave your driveway, repair your roof, or paint your house with supplies left over from another job.

This is just a scam. The repair work is completed very quickly, the quality is poor and the "repairs usually cost more than the original estimate. A BUNCO artist working a home improvement scheme usually drives a commercial van or pickup truck through a residential area. Stopping to talk to a person working in a yard, the BUNCO artist offers to spray the roof, coat the driveway or fertilize the lawn with materials left over from another job. Because the price quoted is low, the person does not ask for a written estimate. After the work is done, the BUNCO operator asks to be paid a higher amount than the quoted price. The person is told materials used are stolen, and the BUNCO artist threatens to call the police or uses sheer intimidation if the higher price is not paid.

To make matters worse, the materials used are often inferior. The roof coating might be whitewash, the driveway coating, motor oil, and the fertilizer made of sawdust and oil. Before home repairs are made, deal with and compare estimates from several reputable companies. Verify identification of persons offering to make low priced repairs. If you are suspicious of the repair person, call local law enforcement immediately and give descriptions of the person and vehicle.

Warning Signs:

- The repairperson drives an unmarked truck or van with an out-of-state license.
- The worker has no business identification, local address or telephone number.
- You are offered a "special price" if you sign today.
- The worker wants upfront cost or fees, or accepts only cash.
- No written estimates or contracts are provided.

- The worker does not have any references.
- The offer sounds "too good to be true"
- The vehicles have out of state license plates

The worker cannot provide any contractor's license, permits, insurance, or bonding information. Generally, work that "adds to or subtracts from real estate" requires a registered contractor. Businesses that provide services such as gutter cleaning, pruning, lawn care or window washing generally do not need to be registered. If you are planning to hire a contractor, make sure the contractor is registered, bonded, and insured. Check the contractor's references. Solicit several written bids.

Contractors and Adjusters

- Several bids. Obtain two or three written repair bids, if possible. They should include all costs, what work will be done, schedule for completing the work, and guarantees.
- But... don't accept a bid just because it's the lowest. Lowball bids such as "special hurricane deals" and "limited time offers" could be fraudulent.
- And... don't pay for repair bids. Crooked contractors may simply take your money and disappear. Most reputable contractors won't charge you simply for bidding on your repair work.

Local contractors. Use established local contractors, if possible. But... be careful if the contractor arrives in an unmarked vehicle, seeks your repair work door-to-door, or tries to cut costs by using materials "from another job." These contractors may be unlicensed, dishonest and untrained transients from another state.

- Often they'll use low-grade material.
- Their work may be shoddy and even dangerous.
- They may disappear with your money after finishing only part of the job, or not doing any work.

Licenses. Ask to see a contractor's required state or local licenses, and write down the

license numbers. Also ask contractors for proof that they have liability and workers compensation insurance.

Look professional? Does the contractor have professional-looking business cards and letterhead? If not, you could be dealing with an untrained and incompetent "wildcatter." Signed contract. Get a signed contract — before work begins. But don't sign any contract with blanks. A dishonest contractor could fill in unfair or fraudulent terms later.

- Also... make sure it's a legitimate, printed document — not something scratched out on a piece of paper. Make sure you have a copy for your files.
- No advance payment. Don't pay a contractor in full before work begins, or before it's finished. The contractor could disappear with your money, leaving your repair job unfinished. Normally you should only pay about 20 percent or less upfront.
- Don't pay extra when a contractor says the cost of materials has "suddenly increased." Pay only what's spelled out in your signed contract.
- No cash. Never pay in cash; pay with check or credit card. A contractor who demands cash may be trying to avoid paying taxes or buying legally required insurance.
- Repairs insured? Check with your insurance company to make sure your policy covers the repairs. Also have your insurance adjuster estimate the damage and probable cost to repair. This will give you a reliable basis for negotiating repairs with contractors.
- Inspect damage. If practical, have an adjuster from your insurance company inspect your damage before repairs begin. Your insurance company may require an adjuster's inspection before you rebuild.

Your insurance claim could be denied if you make expensive, permanent repairs before the adjuster inspects the damage.

- Signing off. Sign the certificate of job completion only when all repairs are finished to your satisfaction, and per your signed contract.
- Fight back. Contact your state insurance fraud bureau and local office of consumer affairs right away if you suspect a repair scam.

Sources of Information

Information and tips on holiday crime and scams comes from Texas A&M University Police Department, the AARP, and various sources.

Many of the narratives for electronic or Internet fraud came from the FBI website at www.fbi.gov.

Much of the information on insurance fraud comes from the website of the Coalition Against Insurance Fraud at www.insurancefraud.org.

Most of the information about confidence scams comes from the website of the National Association of Bunco Investigators (NABI) at www.nabihq.com.

The automobile insurance scam information came from www.bankrate.com, an article quoting the National Insurance Crime Bureau and the Coalition Against Insurance Fraud.

Information on online fraud and social media guidelines comes from the website of the National White Collar Crime Center (www.nw3c.org) and their Informant online magazine.

Information on fake check scams comes from the Consumer Federation of America at www.fraud.org.

This project was supported by Grant #2015-RS-CX-0005 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.