Scams - Detecting and Avoiding

Information is the Best Defense

Anyone can be a victim, even those with an advanced education, substantial assets and lengthy business experience. In fact, some of the most sophisticated scams are targeted toward wealthy individuals or businesses, because, as Willie Sutton reportedly replied when asked why he robbed banks, “That’s where the money is.”

Many con artists seek potential victims among the elderly and those who live alone. These criminals seek out those whose background and status in life naturally make them more trusting or dependent, or victims whose sense of charity or even loneliness make them more vulnerable to the con artist’s story.

Government Agency Scams

You receive a threatening collection call from someone claiming to be with the Attorney General’s office, a Court, law enforcement, a law office, or some other official sounding name. The caller typically indicates he is calling to collect on an unpaid payday loan or other debt. The caller will threaten that the consumer will be charged with a crime, a warrant may be issued and the consumer may be arrested by local law enforcement if payment by credit card or electronic money transfer is not made within 24 hours. These calls have been made by people posing as Internal Revenue Service or Department of Revenue representatives, calling to collect unpaid taxes. Versions of this scam can be sent to consumers in an email, claiming the sender has been watching them and their family, threatening to harm the consumer or a member of the consumer’s family unless money is paid be a remote payment mechanism.

Grandparent Scam

You receive a call or text from someone claiming to be your grandchild or relative, indicating they are in an emergency situation that requires you to wire money or purchase pre-paid gift cards in order to help them. A new twist on this scam is called "virtual kidnapping," where a parent or grandparent receives a phone call from a screaming child, claiming to be the person's child or grandchild, claiming they've been kidnapped. With the child screaming in the background, an adult will then come on the line and demand the parent or grandparent withdraw money from their bank and transfer it to another bank account for ransom. The caller will threaten the child will be harmed or killed if the parent or grandparent does not comply with the caller's demands.

Electricity Scams

You receive a call from someone claiming to be with the electricity distribution company, threatening to discontinue electrical service if you do not immediately pay by credit card or electronic money transfer. Local electrical distributors have reported a rash of such scam calls to their customers, some of whom have been victimized by the scheme. We have also seen a variation of this phone scam involving the caller claiming the consumer's telephone bill or other utility bill is past due and must be paid immediately. There is a variation on this scam where the caller will claim the consumer overpaid on their utility account, with the caller asking for the consumer's debit or account number so the overpaid funds can be refunded back to the consumer's account.

Tech Support Scams

You see a pop-up message on your computer or receive a call from someone claiming to be affiliated with software, technology companies or service companies, claiming your computer is compromised. The caller or pop-up message's purpose is to gain remote access to your computer so malicious software and spyware ("malware") can be installed. Once accomplished, your computer will be held hostage until you pay the caller a ransom. Another version of this scam is the caller claims you have illegally downloaded something onto your computer and you must now pay a fine or penalty to avoid further legal prosecution.

Internet Sales Scams

These scams may lurk in innocent-appearing advertisements, "pop-ups," Craigslist, internet auctions & classified ads. Although legitimate sellers use the internet to promote their products and services, there are a considerable number of scam purveyors who mask themselves in the cloak of technology and consumers should always approach internet sales with considerable caution.

Remember that scam artists can easily misappropriate graphics and pictures from other websites and appear to be selling or leasing something to which they have no claim. For example, scam artists have been known to "lift" the pictures and details about summer vacation rental properties and connect them to their own contact information, charge and collect a deposit for the rental and direct the lessee to pick up the key at the rental property the day he is taking occupancy. It is only then that the lessee discovers someone else has lawful occupancy of the property and the lessee has been scammed!

Some scam schemers have replicated the logos and website designs of legitimate retailers and set up fake surveys and contests to collect consumer information, with the promise of coupons redeemable at the retailer.

Electric & Gas Generation Supplier Sales

Sales representatives solicit energy customers to "switch" from their current electric or natural gas distribution company ("EDC" or "NGDC") or electric generation or natural gas supplier ("EGS" or "NGS"), promising better deals and lower rates. Many of these salespeople have misrepresented who they are and why they are approaching utility customers, claiming to be from the utility itself in order to gain access to account information needed to "switch" the customer to a new supplier. In some extreme situations, the salesperson was not affiliated with a supplier at all, but was masquerading as one, to get into the consumer's home and get personal information for the purposes of identity theft.

Whether you receive a knock on your door or a telephone call from someone claiming to be from an energy supply company, you should be aware that the Public Utility Commission has established marketing and sales guidelines for the activities of the EGSs and NGSs, whether communicated orally (in person or by telephone), electronically or in writing.

EGS and NGS representatives who engage in door-to-door solicitations must wear identification badges and identify themselves and their relationship with the supplier. Consumers must be informed of the three-business-day right of rescission; must authorize the transfer of their account to the new supplier (the authorization may be written, oral or electronic); and any authorization by the consumer to transfer the account must be verified by a third party.

You should always be wary about letting strangers into your home. If they are offering a worthwhile product, they should be willing to provide you with

written material explaining the offer. If they are not willing to do that, alarm bells should sound.

Telemarketers must also clearly identify themselves and upon whose behalf they are calling. They may not suggest that the consumer must choose a competitive energy supplier. They must explain the supplier's verification process, the mailing of the disclosure statement and explain the consumer's three-business-day right to cancel the transaction after receiving the disclosure statement.

As with all telemarketing calls, where you cannot know the true identity of the person calling you, if you think the deal sounds like something you are interested in, ask for written information to be sent to you, rather than committing to anything over the telephone.

Home Security Systems

The sale and installation of home security systems and monitoring is another area that frequently involves both door-to-door and telephone solicitations. Just as with the marketing of energy suppliers, the people perpetrating scams can appear just as "legitimate" as the authentic home security dealers. Consumers should be wary of representatives who claim to be affiliated with an existing security company; to have just purchased the consumers' existing security company; or that an existing security system needed to be updated or replaced.

Work-At-Home Schemes

Many newspapers, magazines and computer bulletin boards contain advertisements about consumer work-at-home plans which often promise fantastic monetary returns for a small investment.

Two frequently used schemes are:

- Addressing or stuffing envelopes - Often, you must pay for the cards or envelopes used. You may not get any money unless someone buys the product being advertised in the cards or envelope.
- Assembly or craft work - The company sells you instructions and materials for making items within your home and promises to purchase the finished product, provided your work is acceptable. The company may reject the product for not being up to its standards, leaving you the burden of selling the product yourself.

Learn to recognize a work-at-home scheme. Generally such projects include:

- Promises of large profits for apparently little work or money.
- The payment of money to obtain additional information about the opportunity or to purchase products to be sold.
- Promises of exclusive territories and individualized training programs.

Some tips:

- Find out exactly what you must do in order to benefit from all that is promised in the advertisement.
- Get a complete description of all initial and future changes which you must pay.
- Get a description of any help the selling company will provide.
- If the advertisement was on a computer bulletin board, obtain a name, street address and telephone number, and then find out about the person or company.

- Learn about the company's procedures for handling complaints.
- Obtain a description of the conditions under which the contract may be changed by either party.
- Before committing yourself to any deal, talk with a lawyer and anyone who has been involved in a business similar to the one that interests you.
- Don't fool yourself: never believe you are going to make a lot of money without doing much work.

Contact the Better Business Bureau in the region where the business is located to see if it has any complaints on file. Call the Bureau of Consumer Protection if you need assistance finding the phone number of the correct Better Business Bureau.

Living Trust Mills and Annuity Scams

Unfortunately, when it comes to living trusts, unscrupulous con artists are ready to play on consumers' fears of the unknown. In some cases, consumers – mostly elderly – are solicited by phone or mail to attend seminars or to set up in-home appointments to discuss living trusts.

Living trusts are then marketed through high-pressure sales pitches which prey on the fear that assets will be tied up indefinitely or that estates are prone to heavy taxes and fees if a living trust is not in place. Con artists often rely on unfamiliar legal terminology to convince consumers that a living trust is right for them, even though many of the complex rules and fees that can complicate estate distributions do not

exist in Pennsylvania.

Sometimes victims are sold worthless "kits," costing several thousand dollars, which are nothing more than standard forms that may or may not be valid, as laws concerning living trusts vary from state to state. In other cases, false promoters simply want to gain access to consumers' financial information so they can sell them other products, like insurance annuities.

Tips to avoid becoming victims of Estate Planning scams:

- Watch out for companies that market trusts and also sell annuities or other investments.
- Estate planning is a complex task and usually involves the advice of more than one expert, such as an attorney and tax accountant.
- Living trust mill agents are not attorneys and are not experts in estate planning. Their goal is to sell their products and earn commissions, not protect the interests of seniors.
- Documents in trust packages may not comply with Pennsylvania law.
- Do not give in to high-pressure sales tactics. Legitimate offers will be around long enough for you to properly research them.
- Sales agents may fail to disclose possible adverse tax consequences or early withdrawal penalties that may be incurred when transferring stocks, bonds, CDs or other investments to annuities.
- Shop around. Check out offers with a trusted attorney or estate planner.
- Verify any stated government affiliation or endorsement.
- Before withdrawing money from an existing

investment to buy an annuity or to make any other investment, get copies of the sales offer documents and review them with people you trust, such as your financial advisor, attorney or family member before signing anything.

- The Cooling-Off Rule states that if you buy a living trust in your home or somewhere other than the seller's permanent place of business (like a hotel seminar), you have three business days to cancel the deal.

Lottery or Sweepstakes Scam

You receive an official-looking notice by mail or email saying you've won a large sum of money, possibly even including a check. To claim your valuable prize, you are asked to deposit the check and send a money transfer to cover taxes and processing fees. Be aware: if you don't remember entering a lottery, you didn't win. And never send money to receive money. No legitimate lottery or sweepstakes asks for money up front.

The Mystery Shopper Scam

You get hired to be a mystery shopper. Your first task: evaluate the customer service of a retail store. You're given a check to cash and use for purchases in the store, yet the amount of the check is more than it should be. The scammer tells you to wire back the amount they've overpaid. The original check turns out to be counterfeit, and you can't get back the money you sent by wire transfer, so you lose both amounts.

Investment Scams

Because many seniors find themselves planning for retirement and managing their savings once they finish working, a number of investment schemes have been targeted at seniors looking to safeguard their cash for their later years.

From pyramid schemes like Bernie Madoff's (which counted a number of senior citizens among its victims) to fables of a Nigerian prince looking for a partner to claim inheritance money to complex financial products that many economists don't even understand, investment schemes have long been a successful way to take advantage of older people.

Online financial fraudsters send e-mail spam, or they approach you on a social media website or in a web forum. An internet advertisement may also lead you to a website, designed to gather your personal information, which they will use to approach you directly or to steal your identity.

Things to remember: Don't expect to get rich quick. Be careful with your personal information. Don't be lured by claims of 'insider information'. Delete and block spam emails. Do your own research. Make sure you get all the information you need before you invest (don't be rushed into an investment). Keep printed copies of all correspondence and investment information.

Before investing, contact the Pennsylvania Department of Banking and Securities at 1-800-PA-BANK-SECURITIES (800-722-2657) to request more information.

Travel Scams

These scams are most active during the summer months. You receive an email with the offer to get amazingly low fares to some exotic destination but you must book it today or the offer expires that evening. If you call, you'll find out the travel is free but the hotel rates are highly overpriced.

Some can offer you rock-bottom prices but hide certain high fees until you "sign on the dotted line." Others, in order to give you the "free" something, will make you sit through a timeshare pitch at the destination. Still others can just take your money and deliver nothing.

Also, getting your refund, should you decide to cancel, is usually a lost cause, often called a nightmare or mission-impossible.

Your best strategy is to book your trip in person, through a reputable travel agency or proven legitimate online service.

Tips to help you avoid being taken by a travel scam:

- Avoid offers that sound "too good to be true," particularly if you have been solicited by phone or have received a postcard or certificate in the mail.
- Never give your credit card number or information about your bank accounts over the phone to a solicitor.
- Get the complete details in writing about any trip before paying.
- Be cautious with companies that require you to wait at least 60 days to take your trip or require that you select several dates of departure for your trip.
- Avoid mailings using words like "grand finalist," "urgent" or "winner" that appear to be sent by special mail or courier.

- Be wary of "900" phone numbers. The calls will cost you and may not result in any benefit to you.
- Don't be pushed into a decision. It's the surest sign that someone's up to no good. Never feel that you have to make a decision on the spot.

Rx Scams

Most commonly, counterfeit drug scams operate on the Internet, where seniors increasingly go to find better prices on specialized medications.

The danger is that, besides paying money for something that will not help a person's medical condition, victims may purchase unsafe substances that can inflict even more harm. This scam can be as hard on the body as it is on the wallet. If you are considering purchasing antibiotics or any prescription drug online, keep in mind the following tips:

> Pennsylvania law requires that prescription drugs be dispensed to Pennsylvania consumers only by a state licensed pharmacist or medical practitioner. A pharmacy must obtain a permit before operating or advertising in the Commonwealth. In addition, a physician must be licensed in Pennsylvania to practice medicine in the Commonwealth.

An actual examination may be necessary to determine which - if any - medicine and dosage is right for you. Factors such as pre-existing conditions, family history and individual symptoms are all relevant to which prescription is appropriate for you. Watch out for web sites offering an online "consultation" with a physician. These consultations may not be reviewed by a doctor and, even if they are, consumers have no way of knowing the doctor's background or history.

Obtaining any prescription medicine from an unfamiliar source and then self-medicating can be dangerous. Online prescription drugs from un-established businesses can originate from foreign, unregulated markets and may be more

likely to be bogus, impure or adulterated. Also, taking prescription drugs like an antibiotic when a person does not have an illness can result in a buildup of immunity to that drug and more virulent strains of the disease, making future treatments more difficult.

Often the prices charged by online pharmacies are extremely high and may include "hidden" charges or excessive shipping and handling costs. Other sources may offer cheaper or generic drugs for the same illness or treatment. Additionally, many web sites require consumers to agree to a waiver of liability which asks them to give up or relinquish all of their legal rights. Consumers should never agree to liability waivers to receive goods or services.

Finally, some sites may simply be scams - you may find yourself paying for something which you never receive or end up giving out credit card and other information only to be ripped off again. As with any online purchase, only complete the transaction on a "secure" site, using a credit card for added protection. If you have any suspicions or concerns about an offer, contact our office.

How to detect a scam?

Scams are designed to separate you from your money or something of value, for instance, your identity. The perpetrator may be looking for a "quick hit," or may be willing to invest more time and energy on maximizing the return. Keep in mind that the more skilled a criminal, the more believable will be the scheme.

So, what should set off warning bells in your mind?

First and foremost, urgency–if anyone is pressuring you to act immediately, that person should be approached with skepticism and suspicion, especially if you are cautioned to keep the transaction secret. It does not matter if the contact is by telephone, email or by someone at your door: if you are being urged to act now or lose an opportunity or have an unfortunate fate befall you, stop and think. Separate yourself from the person and think critically about what you are being asked to do. If something is truly a good deal or – in the case of a family member needing your help, truly an emergency – you should be able to verify the information you have been given before doing anything further.

Second, special types of payment – if you are being asked to pay through a novel money transfer method, such as remotely created checks or payments orders, wire transfers, cash-to-cash money transfers or cash reload mechanisms, beware. Unlike with conventional payment methods, such as credit or debit card transactions, there is no legal recourse for a consumer to seek a refund once funds are transferred through these "novel" transfer methods, regardless of how fraudulent the transaction.

As technology changes, criminals' use of technology evolves. In the case of the cash reload products, the scam artist will urge the consumer to buy them (there are many different "name brand" products available), and then provide the protected code number. The criminal is then able to access the funds by activating the card over the telephone or internet or loading the funds onto his own prepaid card. Once the scammer has withdrawn the cash from the card, the funds – and the perpetrator – are untraceable and anonymous.

Tips to Avoid Being Victimized

- Never give out personal or sensitive information to anyone over the telephone unless you initiated the call to a company you are certain is legitimate.
- Never give out billing information over the phone, especially if you receive an unsolicited telephone call from a stranger.
- Never wire money, purchase iTunes gift cards, purchase prepaid cash cards in response to a telephone appeal, whether it is from a stranger or someone who claims to know you.
- Never let emotion or fear overcome your common sense. If you get a call for money from a friend or relative, slow down and verify everything. Do not let anyone rush you.
- Be careful when responding to any pop-up ad either online or via social media: more often than not, the offer of gift cards or other prizes to customers in the guise of a specific company are set up to get your personal information for nefarious purposes. Remember that appearances can be deceiving: it is easy to reproduce the colors, logos and header of an established organization. Scammers can also make links look like they lead to legitimate websites and emails appear to come from a different sender.

- Legitimate businesses do not ask for credit card numbers or banking information on customer surveys. If they do ask for

personal information, like an address or an email address, be sure there is a link to the company's privacy policy and confirm that the business exists before providing the information.

- Never forget that if an offer or reward sounds too good to be true, it likely is not true! If a survey or contest is real, you may be entered in a drawing to win a gift card or receive a small discount off your next purchase. Few businesses can afford to give away $50 gift cards for completing a few questions.

- Remember that many of the old adages have stood the test of time for a reason – If a deal sounds too good to be true, it likely is a SCAM! If you are promised something for nothing, you will either get nothing or what you get will be worth nothing!

- If you are told you have won a contest, lottery, sweepstakes, grant, etc., first ask yourself if you ever entered the contest, lottery, sweepstakes or applied for the grant. If you have not, this is a scam. If you are being asked to pay taxes or other fees on such winnings, up front, this is a scam. If you are being sent a check and asked to return a certain smaller amount to the sender, this is a scam.

- If someone tells you they are in your neighborhood and have left-over materials that can be used for a home improvement project at a discounted price; or surplus frozen or perishable food at a special price, or a great deal on overstocked clothing, beware. You should always be cautious about dealing with unknown people who may be selling stolen, defective or tainted goods or substandard services or – even more frightening – looking for an opportunity to get into your home to show

you their wares.

- If someone offers to install a security or other home improvement system for free in exchange for your agreement to become a "model" home, beware: there may be hidden costs and fees attached to this "free" offer, in addition to having your home used for unknown purposes by a stranger.

- Beware of strangers: be cautious about letting anyone who solicits goods or services, door-to-door, into your home. Before doing so, make sure the salesperson has clear identification and that you have verified the identification with the company. It is very easy for people to falsify documents and masquerade as a company representative, when they are not.

- Do not be afraid to say "no." Do not be afraid to hang up the telephone or to close the door or to delete the email.

- Do not be intimidated into saying "yes."

- Do not give out personal identifying or financial information until you have had the opportunity to think over the deal, without the pressure of anyone on the telephone, sending you emails or at your door: If something is worth buying or a deal worth entering into, it will be worth it after you have had a chance to think about it.

Consumer Protection Helpline

1-800-441-2555

www.attorneygeneral.gov

- If you decide to enter into a transaction, make sure you get everything in writing. Under Pennsylvania law, any contract for goods or services costing $25 or more, resulting from a contact with you at your home, must be in writing and must give you the ability to cancel within three business days.

What are Card Skimmers?

Skimmers are high-tech devices placed over factory-installed credit and debit card readers, most typically found at bank ATMs or at gas stations. Scammers use these devices, especially in tourist areas, to capture information from the magnetic strips on consumers' cards. They frequently use a nearby concealed camera to record your personal identification number (PIN). With that information, the thieves can get everything they need to drain your account or to make unauthorized purchases. In addition, they may sell your information to others.

Criminals often target automated payment machines in airports, convenience stores, hotel lobbies and public places where the machines may not be regularly inspected by the machine owners. However, card skimming is possible at any ATM or card processing machine, including those on bank premises. As technology makes these devices smaller and more powerful, the risk of card skimming grows.