Identity Fraud
Prevention and Resolution

Protecting your identity from theft is just as important as protecting your home, car and other valuables. You need to **think of your identity as a valuable.** If you fall victim to identity theft, it can cost you more than just money. Some of the consequences to your credit rating are higher interest rates, considerable time trying to resolve debts that you didn't create, extensive emotional distress resulting in loss of work and financial difficulty from false accounts are all results of identity theft. In addition, if someone is caught committing a crime and uses your identification when arrested, you could end up with a criminal record and possibly a warrant for your arrest. Criminal records can prevent or disrupt job opportunities.

The following guide is our outline of identity prevention and resolution options. In an ongoing effort to better our efforts and maximize services to our community and clients, we welcome any additional suggestions and comments on the following material.

Identity Fraud Prevention

Ongoing Personal Data Review: The best way to avoid becoming an identity fraud victim is to make ongoing, proactive efforts to know what is on all of your credit reports. You can't fix what you don't know and for most victims not making a proactive effort, by the time you do know, it's too late!

Obtain and review copies of all three of your credit reports with credit scores. You're entitled to at least one free copy of each credit report per year but you have to pay for the scores. Free reports may be obtained by either going to www.annualcreditreport.com or calling the credit bureaus automated lines: Equifax 1-800-685-1111, Experian 1-888 (NOT 800)- 397-3742, TransUnion 877-322-8228. For reports with scores, you'll need to go to any of the bureaus websites at: Equifax.com, Experian.com, Transunion.com and pay with credit/debit card. The best report is the tri-merged (all 3 bureaus) with scores. Use the bureau with the lowest fee. Don't assume that what's on one report is what's on all of them as they can be very different.

Review and resolve ALL credit issues on your reports immediately. If you do not agree with any item(s) on the reports, follow the dispute instructions on the reports and dispute them directly with the bureaus. If necessary, seek the services of your local Consumer Credit Counseling Service agency. Also, it will probably be faster and more thorough to dispute any items directly through the company reporting the data as that is the point of origin for resolution by the credit bureaus.

Sign-up for an ongoing credit monitoring service through one of the credit bureaus. There are so many credit monitoring services available now that you'll immediately get lost in the options. "How do I select the best credit monitoring service for me?" Start by asking friends and family if they use a credit monitoring service and if so, which one they use and like. If they don't use a monitoring service, please suggest that they sign-up for a service immediately. All of the credit bureaus offering monitoring service.

Do's and Don'ts of avoiding putting yourself at risk of identity fraud:

Do's

a. **Do use a post office box for all mail**. Your mail should never be sitting in an unlocked box at the road. Drive any outgoing mail to the post office.
b. **Do use a shredder to properly dispose of ANY piece of paper that has any personal data** including but not limited to name, address, telephone number, date-of-birth, social security number, mother's maiden name, children's name(s), any account number(s) from any company or service, bank account information, credit card number, prescription labels, catalog order forms, magazine subscriptions, employee paperwork, health insurance explanation of benefits, auto, home or life insurance papers, children's school and health records, credit card offers and pet health records.
c. **Do use a land line telephone (not cordless and not cellular) when making calls that contain personal or financial data**. Cordless phone conversations can often be overheard by other cordless phones, baby monitors, and other devices.
d. **Do use a firewall software service for your home computer** and if you use wireless at your home or in public, make sure that the service is encrypted for added protection. Ask for help if you don't know how to install a firewall.
e. **Do call your phone company and tell them to block unidentified calls.** Always make note of the number that someone is calling from and don't erase any phone numbers that you do NOT recognize. You might need the number(s) later if fraud is committed!

f. **Do sign-up for** www.optoutprescreen.com to reduce pre-approved credit offers, which can often be redirected to other addresses by criminals if not shredded.

g. **Do keep your debit card, credit card & checks out of sight while waiting to pay.** Technology has become a criminal's best friend! One fraud method is to take a picture on a cell phone camera of someone's checkbook, debit or credit card as they stand in line waiting to pay.

h. **Do keep your keys, wallet, checkbook and other valuables out of sight when people are working in your home or apartment.**

Don'ts

a. **Don't use paper checks!** The risk of having your bank account information compromised is greatly increased with the use of paper checks. Embrace technology in this, the 21st century! If you have a checkbook you have a debit card and only use your debit card as a debit if you need cash back. Otherwise, use your debit card as a credit card. Some companies hire people that, as part of their job duties, have to manually process your paper checks giving them all of the information they need to drain your bank account(s). Also, many companies hire people without doing a criminal background check. Much of the credit card and check fraud that takes places is committed by people that we come in contact with while doing everyday activities (e.g., shopping, dining, repairs, travel, etc.). Although your bank might eventually give back money from fraudulent transactions, the time that it takes them to research and return the money might prevent you from being able to pay your bills on time, or at all if the bank doesn't believe you. Use online bill pay from your bank if possible instead of checks.

b. **Don't give personal information to anyone that called you on the phone.** Many clever thieves will call and pose as people with companies that you do business with such as your bank, pharmacy, insurance company, employer, utility company or even law enforcement agency. If someone calls you and says that they're with a company that you know and do business with, ask for their name and what department they're in and tell them that for security reasons you'll have to call them back. Then, do **NOT** call them back at the number they gave you. Call back to the regular customer service number on your transaction card (e.g., debit, credit, etc.) and tell them who called you and what they said so that you can have them transfer you to the correct person or department. If someone is trying to hurry you or pressure you over the phone, it's most likely because they want to confuse or distract you into giving them information. Feel free to just hang-up if someone is hurrying you. You're not trying to make friends you're trying to protect yourself and your identity.

c. **Don't open your door for anyone that you do not know** unless you see a fire truck or police car sitting in front of your home. There are many VERY bold criminals that want you to open your door so that they can force their way in. Once in, your risk of being scammed, robbed or assaulted are greatly increased especially if you are elderly or live alone. Many criminals are people that seem very nice and trustworthy. Red flags would be people that are very anxious and insistent that you do something immediately.

d. **Don't open an email from someone you don't know and don't open forwarded attachments even if it's someone you do know.** Anyone with a computer has had a friend or family member send them something that they found to be interesting or funny. This is a very easy way to get a computer virus

and to have log-in and personal information stolen. If you get an email from a company that you do business with asking you to verify personal information, don't click on the link. Call their customer service number and ask them to transfer you to the security department to discuss what the email says.

e. **Don't have cell phone conversation in public places when the conversation contains personal or financial data.** Not only is this a high risk situation but those honest people around you would most likely prefer that you have your conversations in private.
f. **Don't use outdoor ATM machines if you can use an ATM inside a store or get cash back from a debit card transaction.** You're less likely to be robbed!
g. **Don't give your bank account information to a creditor for direct debits** (excluding online bill pay that you control). This presents a risk since you don't know if the person you're giving the information to has been through a criminal background check. In addition, if your income changes suddenly, you won't have time to stop these drafts. Unpaid overdraft fees can destroy your credit.

Place a fraud alert or credit "freeze" on your file if you even think you're at risk. Fraud alerts are messages listed on your credit files telling companies considering extending credit that you may be at risk for fraud and to call you to verify. However, as mentioned in the "Don'ts section, paragraph B above, if you get a call from someone stating they're with any company and you know that you did not apply for credit, tell them that you did not apply and to contact the police but **do not provide any of your personal information** not even to "verify your identity for your protection". Call back to the regular customer service number on your transaction card (e.g., debit, credit, etc.) and tell them who called you and what they said so that you can have them transfer you to the correct person or department. Credit bureaus don't usually call you and ask you to verify personal data.

Password protect all credit, banking, utility and cell phone accounts. To add a password to a credit or utility account (including cell phones), call the company and ask to add a password. Having a password will make it more difficult for someone to use your identity to open new accounts or tamper with your existing accounts. Always keep passwords private.

File a report with your local Better Business Bureau. The Better Business Bureau (www.bbb.org) is an excellent resource for not only researching companies and their services but also to help report scams and other fraudulent activity not just in your area but nationwide. If you do not have access to the internet, please call 1-703-276-0100 or your local BBB office.

Most people are not as diligent or concerned as they should be about being a victim of fraud until after it happens to them or someone they know. Anyone who has been a victim will tell you that they may have been able to avoid the hassle, stress and the time and money spent to resolve matters of fraud by being more informed and more proactive. **Always remember that identity fraud prevention is much easier to manage than identity fraud resolution.**

Identity Fraud Resolution

Review and resolve ALL credit issues on your reports immediately. If you do not agree with any item(s) on the reports, follow the dispute instructions on the reports and dispute them directly with the bureaus and the reporting creditor. If necessary, seek the services of your local Consumer Credit Counseling Service agency. Also, it will probably be faster and more thorough to dispute any items directly through the company reporting the incorrect data as that is the point of origin for resolution by the credit bureaus. Notify all of your creditors of possible fraudulent activity on any account

Change account numbers. Seeking the assistance of your banking or other financial institution(s) will be essential to preventing loss of your money and credit rating now and in the future. However, there is only so much that institutions can do in terms of protecting existing account numbers. If your banking information as been compromised or is at risk, consider asking for new account numbers with bank accounts, credit cards and if necessary investment accounts. It may be an inconvenience but don't let sentiment prevent you from resolving your fraud issues. For example, "*I've had this account since I was a teenager. I don't want to get a new account number!*" It's just an account number. If it's been compromised, the only sentiment it now holds are bad memories of being a victim of a crime.

Check accounts daily until everything is resolved and weekly once resolved. Time is of the essence! The sooner that you notice a fraudulent transaction, the more likely you are to get it resolved and avoid having it multiply into several problems.

If necessary, Contact the President or CEO of any creditor that is not helping you. Every company has a resolution process in place and most start with customer service. However, many customer service representatives have not been trained on identity fraud resolution. At the customer service level, you'll most likely need to ask to speak with a supervisor. If after making these attempts your resolution is not meeting your needs or satisfaction, feel free to write a certified return receipt letter (mark it "*urgent-personal-confidential"*) to the President and/or CEO of your creditor. In some case, the President and CEO may be the same person. The two fastest ways to find the name and mailing address for the President/CEO is to ask a customer service representative or supervisor or go on their website. If you use the website method, look for a link that says something like "*about us*", then search for "*corporate governance*". Most, if not all, publicly traded (sells shares of stock in their company) companies will have this information on their website. It might also be listed under "*investor relations*". The President and CEO are there to assist when you're not getting the services their customers need and deserve. Don't be shy about asking for their assistance. It's their job to help customers! You most likely won't hear back directly from the President/CEO but you'll probably hear back from someone in greater authority than customer service. Remember that the flow of resolution is very swift coming from the top!

Keep a list of all phone calls made when trying to resolve fraud. You always want to be able to provide anyone willing to assist you with a list of all dates and times of phone calls along with the name of the person you spoke with. Anytime you call anyone for assistance, start by asking "What is your name?" The more organized and detailed you are, the more credible you will appear.

File a police report if you have been a fraud victim to help protect your resolution rights . Many credit card companies and banks will require a police report to return money or reverse transactions that you are stating are fraudulent. Which law enforcement agency handles such reports can vary from state-to-state and county-to-county but a good place to start is the local sheriff's or police department that serves your home address.

As per www.fbi.gov

Common Fraud Schemes

EXTRA

The FBI is warning the public about an ongoing scheme involving jury service. Please be aware that individuals identifying themselves as U.S. court employees have been contacting citizens by phone and advising them that they have been selected for jury duty. These individuals ask citizens to verify names and social security numbers and then ask for their credit card numbers. If the request is refused, citizens are then threatened with fines

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.

Warning signs -- 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 phone.

Some Tips to Avoid Telemarketing Fraud:
It's very difficult to get your money back if you've been cheated over the phone. 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?"

You must not be asked to pay in advance for services. Pay services only after they are delivered.

Some con artists will 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.

It's never rude to wait and think about an offer. Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor.

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.

Your personal information is often brokered to telemarketers through third parties.

If you have information about a fraud report it to state, local, or federal law enforcement agencies.

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 facsimile 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 until the victim's assets are taken in their entirety. 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, in addition to 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."

Some Tips to Avoid 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 Consumer Sentinel.

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.

Impersonation/Identity Fraud

Impersonation fraud 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, such as the theft of your wallet, your trash, or from 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.

Some Tips to Avoid Impersonation/Identity Fraud:

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 to local or federal law enforcement authorities.

Advance Fee Scheme

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.

Some Tips to Avoid the 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 intend to spend, 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, or of dealing with persons who do not have a direct telephone line, 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 noncircumvention 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 noncircumvention agreements to threaten their victims with civil suit if they report their losses to law enforcement.

Common Health Insurance Frauds

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.

Some Tips to Avoid the 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.

Redemption/Strawman/Bond Fraud

Proponents of this scheme will claim that the U.S. Government or the Treasury Department controls 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 Warrants.” 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.

Some Tips to Avoid 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.

Investment Related Scams:

Letter of Credit Fraud

Legitimate letters of credit are never sold or offered as investments.

Legitimate letters of credit 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.)

Some Tips to Avoid 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

International fraud artists have invented an investment scheme that offers extremely high yields in a relatively short period of time. In this scheme, they purport to have access to "bank guarantees" which 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 ten 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 nondisclosure and noncircumvention 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 that is 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.

Some Tips to Avoid Prime Bank Note Related 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 nondisclosure or noncircumvention agreements that are designed to prevent you from independently verifying information about the investment.

What is a "Ponzi" Scheme?

A Ponzi scheme is essentially an investment fraud wherein the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays "dividends" to initial investors using the principle amounts "invested" by 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 scheme is named after Charles Ponzi of Boston, Massachusetts, who operated an extremely attractive investment scheme in which he guaranteed investors a 50 percent return on their investment in postal coupons. Although he was able to pay his initial investors, the scheme dissolved when he was unable to pay investors who entered the scheme later.

Some Tips to Avoid Ponzi Schemes:

As with all investments, exercise due diligence in selecting investments and the people with whom you invest.

Pyramid Scheme: 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 there 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.

Some Tips to Avoid 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.

Internet and Identity Fraud Terms:

1. Adware -- Software that serves up ads based on your previous searches. Free software can come with adware that pays for its use. Generally adware differs from spyware in that it notifies the user of how the program works and its intent.

2. Antispyware -- Software that removes or blocks spyware.

3. Antivirus -- Antivirus software protects your computer against malware. It scans the hard drive for viruses and removes them. It also looks for aberrant behavior in programs that can signal an infection.

4. Authentication -- The process of verifying identity.

5. Bot -- Short for robot. A computer program that performs automated tasks. Can be used maliciously to scan for passwords, search browsing history, capture keystrokes, send spam and report information to a third party across the Internet.

6. Dual-factor identification rules -- Requires banks to implement some form of additional password in addition to the standard username and password combination. It's often accomplished by presenting a picture or something else that the consumer chooses in addition to their password in order to recognize the bank.

7. Firewall -- A security system that protects individual computers or networks from intruders. Firewalls can be either hardware or software or a combination of the two.

8. Identity cloning -- When a fraudster lives as the victim, getting married, working, paying taxes and possibly committing crimes.

9. Identity fraud -- Occurs when a transaction happens in a person's name without their knowledge.

10. Identity theft -- An umbrella term used for everything from a one-time fraudulent credit card transaction to identity cloning. Technically refers only to situations when identifying information is taken and used for fraudulent purposes.

11. Image spam -- A spam e-mail whose content contains text embedded inside an image.

12. Malware -- A general term for malicious software. Examples include viruses, Trojan horses, spyware and worms.

13. Nigerian scam -- Also called the 419 after the code in Nigerian criminal law, the Nigerian scam is an advance fee scam in which unsolicited e-mails claim to offer large sums of money in return for helping someone in trouble.

14. Pharming -- is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

15. Phishing -- A scam perpetrated via e-mail wherein the scammer spoofs a well-known brand or entity, for instance a big national bank or the IRS. The e-mails contain a link to a Web page which purports to be the legitimate site and asks for personal information.

16. Plug-in -- Software or hardware that is used to modify or add to an existing program. Flash and QuickTime are both plug-ins for Web browsers, for example.

17. Red flag rules -- Regulations included in the Fair Credit Reporting Act requiring financial institutions to institute a program to identify red flags signaling possible ID theft or fraud.

18. Social Security number tumbling -- Taking a valid Social Security number and changing it slightly. For instance, 123-45-6789 is changed to 123-45-6790. This is a technique used in a new type of identity fraud called synthetic identity theft.

19. Spam -- The transmission of unsolicited electronic messages in bulk. Usually used in reference to junk e-mail.

20. Spim -- Spam over instant messaging.

21. Spit -- Spam over Internet telephony, or VoIP spam.

22. Spoofing -- Mimicking a legitimate e-mail address or Web site for the intent of fraud. Scammers spoof the e-mail address, logos and design of legitimate businesses in e-mail scams trying to steal account numbers or identifying information by copying the look of the business. Links in the e-mail send victims to the spoofed Web site.

23. Spyware -- Software installed either unbeknownst to the user, or without revealing the intent of the program. Spyware collects data on the user and shares it with the parent company. More annoyingly, spyware programs can also take control of the computer, reroute the Web browser to pages to install more programs and change settings.

24. Synthetic identity fraud -- A type of ID fraud in which thieves literally create new identities either by combining real and fake identifying information to establish new accounts with fictional identities or create the new identity from totally fake information. In typical synthetic fraud, a fraudster uses a real Social Security number and combines it with a name other than the one associated with that number. The combination often doesn't hit the consumer's credit report.

25. Trojan horse -- A software program, usually downloaded, which purports to do one thing but actually damages other programs. Trojan horses can arrive as attachments in e-mails, IMs or by download.

26. Virus -- A program which hides inside another program. When that program is run, the virus also runs and can copy itself into other programs.

27. Vishing -- A voice phishing scam that involves getting consumers to dial into a voicemail system that records personal information. **Can involve first a spoofed e-mail that appears to come from a major company or banking institution that directs the recipient to call a number, or a cold call attempting to retrieve sensitive information**. Cold calls may be live or automated. Like phishing scams, the message usually sounds urgent and stresses the existence of a problem with the recipient's account.

28. Worm -- A computer virus capable of copying itself without needing a host program.