Melrose Park Police Department Crime Awareness Announcement:

The following are some of the most common scams and tips to help prevent you from being victimized.

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.

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.

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 <u>local FBI office</u>, or the U.S. Postal Inspection Service. You can also register a complaint with the <u>Federal Trade Commission's Complaint Assistant</u>.
- 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.

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 to local or federal law enforcement authorities.

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.

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.

Pigeon Drop Scam

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.

Tips for Avoiding Pigeon Drop Scam:

- Go inside the business get away from the person(s)
- Try to get a description and any information (vehicle description, direction of travel, License Plate, etc..)

IRS Telephone Scam

Victims are told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card or wire transfer. If the victim refuses to cooperate, they are then threatened with arrest, deportation or suspension of a business or driver's license. In many cases, the caller becomes hostile and insulting.

This scam has hit taxpayers in nearly every state in the country. We want to educate taxpayers so they can help protect themselves. Rest assured, the IRS do not and will not ask for credit card numbers over the phone, nor request a pre-paid debit card or wire transfer. If someone unexpectedly calls claiming to be from the IRS and threatens police arrest, deportation or license revocation if you don't pay immediately, that is a sign that it really isn't the IRS calling. The first IRS contact with taxpayers on a tax issue is likely to occur via mail

Other characteristics of this scam include:

- Scammers use fake names and IRS badge numbers. They generally use common names and surnames to identify themselves.
- Scammers may be able to recite the last four digits of a victim's Social Security Number.
- Scammers spoof the IRS toll-free number on caller ID to make it appear that it's the IRS calling.
- Scammers sometimes send bogus IRS emails to some victims to support their bogus calls.
- Victims hear background noise of other calls being conducted to mimic a call site.
- After threatening victims with jail time or driver's license revocation, scammers hang up and others soon call back pretending to be from the local police or DMV, and the caller ID supports their claim.

Tips for Avoiding IRS Telephone Scams:

- If you know you owe taxes or you think you might owe taxes, call the IRS at 1.800.829.1040. The IRS employees at that line can help you with a payment issue if there really is such an issue.
- If you know you don't owe taxes or have no reason to think that you owe any taxes (for example, you've never received a bill or the caller made some bogus threats as described above), then call and report the incident to the <u>Treasury Inspector General for Tax Administration</u> at 1.800.366.4484.
- If you've been targeted by this scam, you should also contact the Federal Trade Commission and use their "FTC Complaint Assistant" at FTC.gov. Please add "IRS Telephone Scam" to the comments of your complaint.
- Taxpayers should be aware that there are other unrelated scams (such as a lottery sweepstakes) and solicitations (such as debt relief) that fraudulently claim to be from the IRS.
- The IRS encourages taxpayers to be vigilant against phone and email scams that use the IRS as a lure. The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels. The IRS also does not ask for PINs, passwords or similar confidential access information for credit card, bank or other financial accounts. Recipients should not open any attachments or click on any links

contained in the message. Instead, forward the e-mail to phishing@irs.gov.

These are some of the scams that the Melrose Park Police Department has investigated, but there is a new scam developed everyday. If you have any questions or feel you were a victim of a scam; please report it to our department.