<u>Crime Prevention Tips - Identity Theft & Scams</u>

The North Castle Police Department routinely receives updates on trending crime patterns. In this age of enhanced technology, criminals utilize information found on the internet for their illegal endeavors. These criminals often tend to target elderly citizens. One of the goals of the North Castle Police Department is to ensure that the public is made aware of some of these trending crimes so as to better protect themselves from these predators.

There has recently been an increase in complaints regarding telephone and internet scams. In order to help prevent you from becoming a victim of one of these fraudulent acts, we would like to provide you with some basic tips that you can use.

As always, it is important for you to protect your personal information, especially when online. Ensure that you use trusted and legitimate websites for any online purchases that you make. No one is more familiar with your accounts with financial institutions and businesses than you are. You know their customer service processes. So be certain that you are speaking with a legitimate company representative anytime you share your personal or account information. Verify caller information with the company that they claim to represent. If the caller is legitimate, they will not have any issue with you contacting the company to verify their identity and purpose for the call.

Some of the recent scams that are occurring include:

- Arrest Scam: the caller states that they are a representative of a police agency and that a relative of yours has been arrested and needs bail money to be released. They will ask you to obtain funds and then wire the funds to them in order to get your relative out of jail. This is a scam. Police agencies will not ask you to wire funds to them. Further, if it is legitimate, your relative will be allowed to make the phone call and you should be able to easily recognize the voice. Ask for the name of the police agency, the telephone number, the officer's name and badge number. This will allow you to check if the information is valid. If there is any hesitancy by the caller to provide this info, the call is a hoax.
- IRS Scam: the caller identifies themselves as an agent of the IRS and accuses the potential victim of failing to properly file and/or pay their taxes. They will attempt to gain personal information, such as your social security number and birth date, which, if provided, would allow the caller to obtain credit cards and other items in your name. The caller may also attempt to have you wire funds to them in order to resolve your tax problem. On occasion the caller will threaten to contact the local police to have you arrested. Sometimes this request will come in the form of an email. Both of these requests are scams.

- Solicitation for funds: there are persons soliciting funds for various organizations, both charitable and for-profit, and this often occurs via a telephone call. You should always verify the caller's information and the organization for which they are raising funds. At times they may state that they are raising funds for your local police department. This is easily verified by contacting your local PD. The North Castle Police Department does not subscribe to fundraising efforts by telephone, so any calls of this nature are not legitimate.
- Utility company scam: the victims are contacted by a caller who states that they work at a utility company and are collecting money that is past due. The caller informs the victim that they can avoid having their utility service disconnected if they immediately pay the past due amount using a Green Dot MoneyPack card that can be purchased at a local store. The caller instructs the victim to purchase a Green Dot MoneyPack card in a specified amount and provides the victim with a telephone number to be called back when the MoneyPack has been obtained. The victim purchases a Green Dot card at a local store and proceeds to call back the number they were given. The victim is instructed to scratch off and read the MoneyPack card serial number to the perpetrator. Once the scammer has the Green Dot MoneyPack serial number, they are able to transfer funds onto a prepaid debit card and the victim has now lost their money.
- Nigerian 419 scam: a "Nigerian" scam is a form of upfront payment or money transfer scam. They are called Nigerian scams because the first wave of them came from Nigeria, but they can come from anywhere in the world. The "4-1-9" part of the name comes from the section of Nigeria's Criminal Code which outlaws the practice. The scammers usually contact you by email or letter and offer you a share in a large sum of money that they want to transfer out of their country. They may tell you about money trapped in central banks during civil wars or coups, often in countries currently in the news. They may tell you about massive inheritances that are difficult to access because of government restrictions or taxes in the scammer's country. Scammers ask you to pay money or give them your bank account details to help them transfer the money. You are then asked to pay fees, charges or taxes to release or transfer the money out of the country through your bank. These "fees" may even start out as guite small amounts. If paid, the scammer makes up new fees that require payment before you can receive you "reward". They will keep making up these excuses until they think they have got all the money they can get out of you. You will never be sent the money that was promised.

The frequency of these scams is increasing and residents are reminded to make every effort to protect their personal information. In short, if something does not seem right, it is probably a scam. Whether received by telephone call or email, these scams can

have a long-lasting effect on your personal finances and credit should you fall victim to their efforts. Do not give out personal information over the phone, or via email, to an unknown person or company. Obtain the caller's name, telephone number and company so that you can try to verify the authenticity of the request.

If you have any questions, or would like to report an incident that has occurred, please contact the North Castle Police Department at 914-273-9500. You can also stop in to NCPD HQ at 15 Bedford Road, Armonk, to report an incident. Should you become an unfortunate victim of one of these scams, Identity Theft packets are available at HQ to facilitate filing reports with the appropriate credit and financial institutions.