From: Karen Richmond <karenri@plano.gov>
Date: June 13, 2013, 1:28:45 PM CDT
To: Undisclosed recipients:;
Subject: Identify Theft Information

DON'T BECOME A VICTIM OF FRAUD OR SCAMS!

Although frauds and scams are as varied as the criminal imagination will allow, the Plano Police Department would like you to be aware of common themes and how to avoid becoming a victim. Identity theft happens when someone steals your personal information and uses it without your permission. They may open lines of credit or order credit cards, take out loans or even rent a hotel room, apartment or car, or purchase a home or a car. They print fake checks, fake IDs, and any other documentation they need to impersonate you. If they have your bank account information, they may take over your account and withdraw your money. Some ID Thieves do this in person, and many just commit their crimes online. It's a serious crime that can wreak havoc with your finances and credit history, and can take time, money, and patience to resolve. An ID thief may start with a piece of mail or a receipt or invoice he/she has found or stolen. The rest of your personal information (date of birth, Social Security#, drivers license#, etc.) is available for purchase through unscrupulous means and even on social networking pages. The theft of mail from residential mailboxes is a common starting point for most Identity Thieves. An ID Thief has an easier time if you have an unlocked mailbox or if you have lost your wallet and carried all your personal information in it, or you use social networks. Many profiles include email addresses or phone numbers, or information about family members and even pets and mother's maiden name — popular security questions used by websites to authenticate a user's identity, and therefore can be used by ID thieves. There are still a great number of Facebook users that have a "public" profile that allows anyone to see such information. Accepting "friend" requests from strangers also puts you at higher risk of Identity Theft. Additionally, users of LinkedIn, the popular employment-oriented website, often includes past and current jobs and other useful data for Identity Thieves to fill out fraudulent credit applications.

How to Avoid:

- Shred all personal documents, bills, receipts, and invoices that are not needed
- Don't carry your Social Security number or passport in your wallet
- Keep your wallet safe and close to you
- Don't mail outgoing payments from your home mailbox. Use the post office.
- Buy a locking mailbox insert for your home mailbox so no one can steal your mail.
- Contact your bank or account issuers if you do not receive a statement on time.
- Do not store your personal or account information online or in your email account or computer.
- Don't share by email or fax your personal information unless necessary.
- Don't put personal identifying information on your social networking

pages (see below)

- Monitor your credit report or have a credit monitoring service assist you. Place a recurring fraud alert on your credit if you have been a victim. Every person may get a free copy of their credit report annually at https://www.annualcreditreport.com/cra/index.jsp or from:

  Experian: 1-888-EXPERIAN (397-3742);www.experian.com
  Equifax: 1-800-525-6285; www.equifax.com
  TransUnion: 1-800-680-7289; www.transunion.com

Read more at: http://www.consumer.ftc.gov/features/feature-0014-identity-theft
https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/mailtheft/IDProtectName.aspx
http://www.idtheftcenter.org/