ID Theft

Summary of Presentation by John Guaraglia, a Graduate of Santa Rosa Police Department's Citizen Academy given to members of Lomita Heights Neighborhood Association (LHNA) and their friends.

This presentation had an emphasis on financial ID theft.

In order for ID theft to occur several items are necessary for this to be accomplished:

- Full name (if not common) and address
- Social Security number
- Credit card numbers
- Date of birth
- Mother's maiden name

How do thieves steal an identity?
Identity theft starts with the misuse of your personal identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold. Skilled identity thieves will use a variety of methods to get hold of your information, including:

- **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
- **Skimming.** They steal credit/debit card numbers by

using a special storage device when processing your card.

- **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
- **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
- **Old-Fashioned Stealing**. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.

The following are suggestions on how to avoid those types of thefts.

Use a shredder for confidential information, utility bills, credit card slips, unsolicited credit card applications, and other documents.

Don't verify anything on the internet. Be cautious of public areas where your computer can be used. Also, information can also be obtained from smart phones.

Don't verify anything over the phone. Be wary of scams such as: a warrant for your arrest because you did not response to a jury summons, instructing you to send money to prevent your arrest; an agent representing a relative who is in distress and is asking for money to be sent. Remember, no stranger calling

on the phone should have any personal information about you or your relatives. If you have to give information such as your credit card number for a purchase over the phone, use your land line phone and not the mobile one. Scanners and ham radio operators can hear your conversations if you use your mobile but not your land line phone.

Be cautious about unsolicited “deals”, such as cabins, resorts. Verify the existence of such advertised items if you are so interested.

Be wary of unsolicited mortgage rates that are “better” than what you have. The caller has no way of knowing your rate. Only you know that rate.

Protect your mail. Get your mail as soon as possible when it is delivered to your home. Don’t leave mail out for pickup since those items usually have very important data such as credit card numbers or a check with the account number printed on it. If you live in a rural area, the red flag on the mail box is an invitation to a thief. Consider a locked mail box. Use the US Post Office blue deposit boxes for outgoing mail.

Protect your Medicare number if you have one. Don’t carry it on your person unless you are going to your physician, lab, or hospital, or going on a trip. If you need to carry it often, make a copy of the card and block out the last 4 numbers.

Limit your credit cards to a reasonable number such as two. Remember that you are liable only for $50 if your credit card is used illegally. However your debit card is a different matter. If someone uses your debit card illegally, they can remove all of your money from your account. Make copies of your cards in case they are lost. Notify all 3 credit agencies (listed at end of summary) if they are lost. Inform your credit card company if you are planning a trip especially if it is out of the country. You can also freeze your credit by calling the 3 agencies. You then can unfreeze your credit if and when you wish to purchase a big ticket item such as a car, etc.

Be aware of new credit cards that have already been issued to some of the card holders. They are called RFID credit cards (RFID stands for Radio Frequency Identification which involves a “RF tag” and a “reader”). These components allow for what the industry calls “contactless payments”. The card has a small chip which allows the holder to simply place the card in front of the card reader. It is not necessary to slide it. This could allow a “reader” in a brief case to get the information from your card in your pocket or purse by passing very close to it --- such as in crowded area (airports). There are wallets and such on the market for protection, but simply covering the card with aluminum foil does the trick. The following names may be on the card to tell you that you have one of these chips: Blink, Pay Pass, or Pay Wave.

Here is a logo that could be on a credit card:

Be cautious if you are considering obtaining ID protection. Such plans are LifeLock and IDTheftSmart. Be very clear what you are buying. Some of these plans are purely an insurance one and not one that protects your ID or monitors your financial activity.

The following are the 3 credit agencies:

Equifax	TransUnion	Experian
P.O. Box 740241 Atlanta, GA 30374 800-685-1111	P.O. Box 1000 Chester, PA 19022 800-888-4213	P.O. Box 2002 Allen, TX 75013 1-888-397-3742

The above was created from notes by Barbara Baker, secretary of LHNA and Ken Howe, president of LHNA.