This information was partly from a presentation by Dan Campos, Detective Sergeant of the property/high crime unit in Santa Cruz County Sheriff's office on February 12 at the Santa Cruz County Seniors Commission. The rest of it is from a presentation by Santa Cruz PD Detective Mark Eveleth, as part of a series of classes for the Citizens Police Academy.

Identity theft is a big problem and rapidly becoming a HUGE problem. It not only funds the drug habits of small time addicts acting locally but also large scale operations in the US and outside the US which are impossible to bust. Here are a few tips on protecting yourself.

1. Shred EVERYTHING! Shred all mail including envelopes that contain your name and address. This is the first stop on the way to gaining control of your identity. Shred all preauthorized credit card offers, applications, credit card company checks, everything that has an account number, your name, your address, even your phone number.

2. Do not sign the back of your credit cards. Instead, put "PHOTO ID REQUIRED."

3. When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the "For" line. Instead, just put the last four numbers. The credit card company knows the rest of the number, and anyone who might be handling your check as it passes through all the check processing channels won't have access to it. Better yet – use the online bill pay service available through most banks. See #16 below.

4. Put your work phone # on your checks instead of your home Phone, or no phone number at all. Use a PO Box address instead of your home address. If you do not have a PO Box, use your work address. Never have your SS# printed on your checks. You can add it if it is necessary. But if you have it printed, anyone can get it. Don't use your full name on checks. Use initials and request to pick up your checks at the branch where you bank.

5. NEVER carry your Social Security Card or Number in your wallet. Do not try to disguise it by adding a number at the beginning or end to make it look like a phone number such as: SSN 234-56-7890 disguised as 1-234-567-8901. They know this trick and will try different combinations until the crack your code.

6. Place the contents of your wallet on a photocopy machine and copy both sides of everything in your wallet/purse. Do both sides of each license credit

card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to Call and cancel. Keep the photocopy in a safe place. I also carry a Photocopy of my passport when I travel either here or abroad. We've all heard horror stories about fraud that's committed on us in stealing a name, address, Social Security number, credit cards.

7. We have been told we should cancel our credit cards immediately. But the key is having the toll free numbers and your card numbers handy so you know whom to call. Keep those where you can find them.

8. File a police report immediately in the jurisdiction where your credit cards, etc., were stolen. This proves to credit providers you were diligent, and this is a first step toward an investigation (if there ever is one).

9. Call the three national credit reporting organizations immediately to place a fraud alert on your name and also call the Social Security fraud line number. I had never heard of doing that until advised by a bank that called to tell me an application for credit was made over the internet in my name. The alert means any company that checks your credit knows your information was stolen, and they have to contact you by phone to authorize new credit. You will not be able to apply for a store credit card to take advantage of an "additional 15% savings." This stops all new activity on your account for up to 90 days. I renew my fraud alert every 90 days. If you are ever the victim of fraud, the police report will enable you to put a permanent fraud alert on your credit.

10. When you register a product online, such as a new equipment purchase or software, or register to use a free service online, use a made up email address. The one I like is YouWish@NoWay.com. That way you won't receive junk email when your email address and information is sold to a third, forth, fifth, etc. party. Also, NEVER use any personal information that is true when registering online. Use mail in registrations whenever possible.

11. Routinely examine credit card statements and bank account statements carefully. Many professionals will repeatedly hit accounts for smaller amounts such as $25, $50 or $100 until it they are detected.

12. Hand-held credit card scanners are used to gain your credit card information right in front of you without your knowledge. When you use a credit card at a store or restaurant, don't let the card leave your sight. A hand-held "swiping" scanner fits in the fold of the fingers and is very difficult to see. The user swipes the card across the scanner held in the opposite hand and the information is later downloaded onto another computer. The card can be

scanned without your knowledge. Insist that you pay at the register as you leave if the card has to be taken out of your sight.

13. This has been around the internet numerous times as Urban Myth but I assure you it's true. When staying in a hotel that uses a plastic insert card to open guest room doors, take it home when you leave and destroy it. It can have personal information on it, especially at older facilities in the US and at many facilities outside the US. The information most likely found is your date of arrival, date of departure, credit card number, name, home address, and home phone.

14. Buy a locking mail box, bring in the mail as soon as possible after it is delivered and take all outgoing mail INSIDE the post office to be mailed, not at the post office street mailbox and especially not from your home mailbox. Devices are used to reach down into post office mailboxes to "fish" out mail. Just as an example, when paying a bill, there is a copy of a check with your name, address, phone number, anything you've written on the check, your bank account number and your signature. By putting your red flag up at your home mailbox it is just that – a big red flag, inviting trouble.

15. Never pay anyone by check that you don't know well unless you use a gel pen. This may sound ridiculous but the reason is checks can easily be "washed" when a ball point pen is used, but not if you use a gel pen. If you write your checks with ball point pen, the pen marks can be removed with acetone. This is very common. Then copies of the checks can be made and rewritten. Also, with only your bank account number from the bottom of your check, a check writing program and a printer, hundreds of very legitimate looking checks can be printed and your checking account cleaned out in one day.

16. The best way to pay bills is with the bill pay service available through your bank online. Also request online bills instead of paper bills from your creditors each month. This is not only more environmentally friendly, but you don't have to keep all that information in a file somewhere. It's readily available online, and copies of checks sent by the bank on your behalf to pay creditors can be electronically sent as proof the bill was paid on time if ever needed. These services are available through most banks, they are usually free and they usually have employees to help you get started.

17. When you are registering at a hotel, make sure no one can hear your name, room number, or other personal information. This trick is common where the thief stands near the person checking in to hear the personal information then uses that information to gain access to the room later.

18. Password protect your computer, all your programs, your wireless internet access and every website that requires them with passwords containing at least 3 letters, upper and lower case, and 6 numbers. DO NOT USE your birthday, your social security number, any part of your address, your spouse's or kids' birthdays, or any other obvious combination. Pick something random and if you must write it down in a safe place. Wireless access points can be password protected and should be to prevent hacking into your system or using your system to commit crimes.

Now, here are the numbers you always need to contact about your wallet, etc., has been stolen:

1.) Equifax: 800-525-6285

2.) Esperian (formerly TRW): 888-397-3742

3.) TransUnion: 800-680-7289

4.) Social Security Administration (fraud line): 800-269-0271

Here are some websites with more information:

California Department of Consumer Affairs: www.privacy.ca.gov

Federal Trade Commission: www.consumer.gov/idtheft/index.html

Santa Cruz County Sheriff: www.sheriff.com

Consumer Information: www.privacyrights.org

Royal Canadian Mounted Police: www.phonebusters.com