Identity Theft and Fraud Prevention

Jill Mecklenburg, Crime Prevention Specialist
Richfield Police Department

Statistics

- In 2011, over 11.2 million Americans were victims of identity theft.
- The total U.S. cost is over $54 Billion
- Many thieves still obtain personal information through traditional rather than electronic channels.
- Conventional methods such as lost or stolen wallets, misappropriation by family and friends, and theft of paper mail.
How Does It Happen?

- Personal information is obtained from:
  - credit cards, financial statements, checks, driver’s license, receipts, bank documents, bills, medical records, and surveys
- New accounts are opened without your knowledge

Common Ways Thieves Steal

- Your Mailbox
  - Credit card offers
  - Bills
  - Bank statements
  - Pay checks
  - New Checks
  - Outgoing mail
Common Ways Thieves Steal

- The Trash
  - Home
  - Bank
  - Business Records
  - Dr.’s Office
  - Car wash
  - Work

Common Ways Thieves Steal

- Your Car
  - Documents
  - Mail
  - Wallet / purse
  - Insurance card
  - Bank receipts
  - Papers from work
  - Cell phone
  - Planner / calendar
Common Ways Thieves Steal

**In Your Home and Office**
- Cleaning/Service Persons/Babysitters...
- Files should be locked
- Employer files
- Paychecks
- Planner / address book

**On The Phone**
- A thief may pose as a bank or credit card company employee
- NEVER give out information without verification, EVER!
- Don’t let someone manipulate you over the phone
**Common Ways Thieves Steal**

- Using Cell Phone Cameras/Videos at:
  - Banks
  - ATMs
  - Hotel Front Desks
  - Retail Counters

**Your Best Kept Secret Should Be...**

Your Social Security Number

Treat it as though it were a million dollars!

- Avoid giving it out and ask:
  * Why do you need it?
  * What is it used for?
  * Is there a law that I have to give it to you?
  * What will happen if I don’t give it to you?
  * How will it be protected?
  * Who has access to it?
Don’t Be An Easy Target

- Guard your personal information
- Send mail from the post office, never put up the red flag on your box
- Tear out mailing labels & order forms before disposing of catalogs
- Stop the junk mail

Prevention

- SHRED your documents
- Black out your SS# on existing cards you must carry
- If possible, cancel paper bills and pay online. Monitor your account activity electronically (weekly)
- Check your credit report (yearly)

- If you don’t use online accounts, monitor your billing cycles for missing bills or statements.
- Review paper bank and credit card statements monthly
Credit Cards

- Monitor your credit card statements
- Reduce the number of credit cards you use and carry
- Cancel unused cards
- Your credit card # should NEVER be used for verification purposes
- Never give out your cc # over the phone unless you know with whom you’re doing business

Identity Theft Don't Get Hooked!
Phishing

In the computing world, phishing is an attempt to criminally and fraudulently acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Scammers send out mass emails claiming to be financial institutions. The emails generally indicate that the financial institution has experienced problems with their records. The email typically indicates that the recipient’s account may be frozen if he/she does not act quickly by clicking on an Internet link on the page.
**Phishing**

By clicking on the link, the recipient is navigated to an official-looking website which asks the individual to disclose their account information and other personal information in order to "verify" their identity. The crooks are then able to make unauthorized withdrawals from the account in question or apply for credit in the account-holder's name.

---

**Off & On-Line Safety**

- Generally, you can operate safely on the Internet but use common sense.
- It's okay to be skeptical.
- Make sure that your operating system and software are updated on a frequent basis (keep patches current).
- **PATCH! PATCH!! PATCH!!!**
- Use a firewall.
Take care of your computer

• If you have to leave your computer unattended, LOCK IT!
**Shop Smartly On-line**

- Use a secure browser - one with **https**: and it has the lock icon.
- Shop with companies you know
- Check the company’s on-line privacy policy
- Keep a record
- Opt out of sharing info

**Take care of your computer**

- Use strong passwords: Think “pass-phrase”
- Use a combination of numbers, letters (upper and lower-case), and special characters
- Do not use the same password for every account.
- Consider changing your passwords periodically.
If You’re A Victim of ID Theft…

- Contact the fraud departments of the three major credit bureaus
- Call creditors/banks/loan officers
- File a police report

- Check your investment accounts, lines of credit, bankruptcy, criminal history, cell phones

Credit Bureaus

**Equifax** www.equifax.com
- To order your report, call: 1-877-322-8228
- To report fraud, call: 800-525-6285

**Experian** www.experian.com
- To order report, call: 888-397-3742
- To report fraud, call: 888-397-3742

**Trans Union** www.tuc.com
- To order your report, call: 800-916-8800
- To report fraud, call: 800-680-7289
Recovery & More “Clean-up”

- Contact the postal inspector if mail fraud has occurred
- Request a “fraud alert” to be placed in your files
- Close all existing accounts
- Request password only access for change of address on all accounts

More Help…

- Federal Trade Commission
  - www.consumer.gov/idtheft
  - or 1-877-IDTHEFT
**Stop Junk Mail (Credit Card Offers)**

- "Opt-Out" on pre-approved credit offers from the three major credit bureaus, call: 1-888-567-8688.

**Stop Junk Mail for $1**

- Remove your name from marketers' unsolicited mailing lists for 3 years through the Direct Marketing Association (DMA).

  - Log onto www.DMAchoice.org or
  - Send a check made out for $1 to: Mail Preference Service Dept. 27478505 Direct Marketing Association P.O. Box 282, Carmel, NY 10512

  **Include:** Primary and secondary names, address and signature.
Stop Junk Mail and Calls

**National Do Not Call Registry**
- The law requires telemarketers to search the registry every three months and avoid calling any phone numbers on the registry.
- You can register at donotcall.gov or by calling 1-888-382-1222 (you must call from the number you want to register.)
- Calls from political organizations, charities and telephone surveyors are still permitted.

Stop Junk Mail and Calls

- Whenever you donate money, order a product, or fill out a warranty card, write in large letters, “Please do not sell, trade or give-away my name & address.”
- If you order by phone, say “Please mark my account so that my name is not traded or sold to other companies.”
- Tell telephone solicitors to “Please permanently place me on the DO NOT CALL list,” then hang up.
Examples of Local Fraud

Metro Grocery Stores

Theft While Shopping

While a resident (usually an older female) is shopping, she leaves her purse in the shopping cart. A well-dressed person approaches and asks several questions pertaining to a specific product. While the shopper is preoccupied with this person, another individual takes the victim’s wallet. The victim’s checks and credit cards are then immediately used.
Preventing Theft While Shopping

- When you take out your wallet, don’t reveal your money or credit cards.

- Don’t leave your handbag in the shopping cart. Use a belly bag to carry your wallet. If you do use a purse, it should be carried close to your body with the clasp or flap towards you.

The Sympathy Plea

“I need $ for my son’s medication.”

A person approaches residents and politely asks for money (usually $20) for their child’s medication, money for a taxi to the hospital, or some other emergency.

Kindly refuse to give the person money and then notify the police (call 911). Give a detailed description of the suspect and direction of travel.
Home Improvement Scams

- Are often targeted at the vulnerable or elderly
- May involve roofing, seal coating, tree trimming and painting
- The crimes usually occur from March to September during the warmer months

The Scam

- The offender tells the victim they are in the area performing work and have extra supplies so they are able to give a “discount” to the victim
- They CONVINCE the victim they need work performed
- They often require a deposit (Legitimate contractors are only paid when the work is completed to the homeowner’s satisfaction)
**Offenders**

- The offenders often drive newer pickups with out-of-state plates
- They often do not have the needed supplies to complete the desired jobs

---

**What To Do??**

Be wary if...

- Someone offers to do work at a discount
- They offer to do repairs with “supplies left over from another job”
- They go house-to-house to solicit business
- Cash payment is requested
- References or a warranty are not available
- The offer is only good for that day
- Remember, they MUST have a PERMIT to solicit door-to-door in Richfield (section 1181)
**Do Your Homework...**

Before work is done...

- Contact several local contractors for an evaluation and estimate
- Compare bids
- Check out the companies by calling references and the Better Business Bureau
- Never pay for work before it’s completed

---

**Protect Yourself...**

Check out a business or offer with:

- the Better Business Bureau at (651) 699-1111 or
- the Attorney General’s Consumer Division at (651) 296-3353
Questions…