

“Consumer Considerations”

The Crime of Identity Theft

Becky J. Palmer
Director of Education
Consumer Credit Counseling Service of NH-VT
November 2008



ID Theft



Definition: : the illegal use of someone else's personal information (as a Social Security number) in order to obtain money or credit

Added: 1991

But that's not the whole story...

The Real Deal with ID Theft

- In the last 12 months 9.3 million Americans were victims of ID theft.
- The average fraud amount per victim rose to \$6,278.
- The average time a victim spends handling ID theft related matters is 40 hours.

Source: Javelin Strategy & Research Survey - February 2007

The Real Deal with ID Theft

- 68.2% of information obtained off-line versus 11.6% obtained online (*In cases where the method was known.*)
- Total annual US fraud cost is \$52.6 billion dollars
- Over 245 million data records of US residents have been exposed since January 2005

Source: Javelin Strategy & Research Survey - February 2007 and privacyrights.org

What They Want

Your data...

- Name, address & date of birth
 - Social security number
 - Driver's license number
 - Credit card numbers
 - ATM cards (with or without PIN numbers)
 - Telephone calling cards
 - Medical information
 - Insurance information
 - Anything else of interest
-

Why They Want It

- Open new credit accounts and charge without paying bills
 - Take over existing credit accounts
 - Open phone and/or utility accounts in your name
 - Open a checking account in your name and write bad checks
 - Drain your accounts by authorizing electronic transfers
 - Obtain a driver's license or ID with your name
 - Claim government benefits under your name
 - Secure employment using your Social Security number
 - Rent a house or get medical services using your name
 - Give your information to police during an arrest. If they don't show up for court, a warrant for arrest would be issued in your name
-

How They Get It

Let us count the ways

- Stealing wallets, backpacks, purses
 - "Dumpster diving"
 - Stealing from mailboxes
 - Fraudulent credit report access
 - Pretexting
 - "Shoulder surfing" at ATM's or other public places
 - Internet sources such as public record sites & fee-based information broker sites
-

Trash or Treasure

What do you throw away?

- Pre-approved credit card offers
 - Loan applications
 - Bank statements
 - Checks
 - Medical records
 - School records
-

ATM

The Scam

- Plastic strip placed into card insert
 - Machine can't read the card
 - Continuously asks to re-enter PIN
 - Thief watches PIN being entered over & over
 - Victim thinks ATM is broken & has the card
 - Thief removes plastic strip, enters PIN & gets \$
-

Shopping for Trouble

Department Store Scam

- Try to buy using card
 - Phone near register rings
 - Caller is "store security" – says you are a suspect in credit card fraud
 - Requires clerk to verify credit card info
 - May ask clerk to get address & social security number
 - Call came from a thief working with the clerk to con people
-

Dinner...deal or no deal

Skimming Scam

- Wait staff takes your credit/debt card after dinner
 - Uses hand held device called a “skimmer” to swipe card
 - Takes seconds
 - Credit card info is stored in the skimmer
 - Card is returned
 - Thief makes a counterfeit card or uses to purchase items via phone or Internet
-

Check Please

Counterfeit Checks

- Thief uses software program, blank checks & a printer
 - Creates checks & writes away
 - Info comes from a stolen check
 - Counterfeiting bank checks
 - Same tools to create fake bank checks
 - Locates item being offered for sale and offers to buy, sends check for more than purchase price
 - Consumer deposits the fake check
 - The bank is unable to immediately tell it's fake but will find out
 - Consumer obligated to reimburse the bank for the full amount
-

On-line Fraud

Let Us Count the Ways

- Crackers
 - Other computer users try to gain access to your hard drive remotely over the internet
 - Passwords, encryption, a firewall can help
- Viruses & Worms
 - Malicious programs installed without your knowledge or permission
 - May be part of or enclosed in an email
 - Once installed may replicate & propagate using your computer
 - Perform unwanted acts (affect stored data) such as recording keystrokes & “phone home” or otherwise steal sensitive data

On-line Fraud

Let Us Count the Ways

- Spyware
 - Program which records your activities and “phones home”
 - May be mostly benign or may collect & transmit sensitive data
 - Always read the EULA
- Phishing
 - Email looks like it's from your bank, credit card company, etc.
 - Asks you to update records
 - May say fraud has been detected
 - Provides a hyperlink to a webpage
 - Link goes to thief's website disguised to look like the companies

On-line Fraud

Let Us Count the Ways

- Pharming
 - More sophisticated than phishing
 - Thief creates website that looks like a legitimate business's website
 - Thief then hacks into the legitimate site or the DNS server to redirect the companies customers to his site
 - Hard for a thief to do, but also very hard for a consumer to detect
 - Internet Gambling
 - Possible exposure to ID theft
 - Use of credit/debit cards to pay and collect
 - Rely on gambling site to be "trustworthy" and use proper security procedures
-

Play it Safe

Computer Safety

- Password protect your computer & encrypt files with sensitive personal data
 - Install a firewall to prevent access to your hard drive
 - Secure your wireless network
 - Install & update virus protection software
 - Delete email without opening it if you don't know the sender
 - Use a strong "wipe" utility program before disposing of a computer or physically destroy the hard drive
-

Play It Safe

On-line Safety

- Understand that NO bank, credit card issuer or financial institution will EVER ask you to “verify” or otherwise supply account info via email.
 - Make sure websites are secure before purchasing
 - Shop at sites you know or trust
 - Use one specific credit account for making online purchases
 - Monitor your checking account and/or credit accounts online regularly
-

Protecting Yourself

General Prevention Tips

- Check your credit reports - www.annualcreditreport.com
 - Opt out to reduce or eliminate pre-screened offers
 - Follow up if bills don't arrive on time
 - Review statements carefully and regularly
 - Purchase & use a shredder
 - Use a secured mailbox
 - Don't put your SSN on checks or carry it in your wallet/purse
 - Don't use obvious passwords – alpha-numeric is best
 - Keep personal info in a safe place
-

ID Theft Monitoring Services

- Monitoring primarily protects against new account fraud
 - Generally can't protect against
 - Existing account fraud
 - Debit or check card fraud
 - Social security number fraud
 - Criminal identity or medical identity fraud
 - Consumers can add a credit security freeze
 - If not a victim of ID Theft it's \$10 for each credit bureau to add or have removed
-

If You Become a Victim

Taking Action

- Notify your bank & creditors
 - Close compromised accounts
 - Place a "Fraud Alert" on your credit reports immediately & review your reports
 - Complete the ID Theft Affidavit at [ftc.gov/idtheft](https://www.ftc.gov/idtheft)
 - File a police report
 - Report the theft to the Federal Trade Commission and the USPO
 - Keep all paperwork & records
 - Continue to monitor your credit report & accounts
-

ID Theft Contact Sheet

- Identity Theft Resource Center
 - 858-693-7935 or www.idtheftcenter.org
 - Federal Trade Commission
 - 800-IDTHEFT or www.consumer.gov/idtheft
 - Credit Bureau Fraud Units
 - TransUnion: 800-680-7289
 - Experian: 888-397-3742
 - Equifax: 800-525-6285
 - Fraudulent Check Contacts
 - Checkwrite: 800-766-2748
 - Chexsystems: 800-428-9623
 - Equifax Telecredit: 800-437-5120
 - National Processing Co.: 800-526-5380
 - SCAN: 800-262-7771
-

Additional Resources

- Credit Reports
 - www.annualcreditreport.com
 - Do Not Call Registry
 - www.donotcall.gov/
 - www.consumer.gov/idtheft
 - OPT Out
 - www.optoutprescreen.com
 - Privacy Rights Clearinghouse
 - www.privacyrights.org
 - NH Consumer Protection & Antitrust Bureau
 - www.doj.nh.gov/consumer/
-

Keys to Success

- Reduce risky behavior
 - Monitor your credit reports at least annually
 - Monitor & protect your computer and your records
 - Be aware of your surroundings & remember it's not just strangers who commit ID theft
 - Take immediate action if necessary
-

Assess Your Risk

Take the test...

- <http://www.privacyrights.org/itrc-quiz1.htm>

How do you measure up?

- 100+ points
 - Trouble knows your name and it's time for change
 - 50 – 99 points
 - Who's average...you & that's your risk
 - 0 – 49 points
 - ID IQ Guru...keep up the good work
-

Wrap It Up

Contact Information

Becky Palmer

bjp@cccs.mv.com

phone: 800-327-6778, ext. 120

Special acknowledgement and recognition goes to the Consumer Protection & Antitrust Bureau of the NH Attorney General's Office for contributing to the content of this program.

Website: www.doj.nh.gov/consumer/
