

Grand Theft Identity: Information You Can Use to Protect Yourself

*Vanderbilt University School of Medicine
January 17, 2007*

Think About Tomorrow™





Welcome

Jennifer M. Schott

Client Manager

American Student Assistance

100 Cambridge St., Suite 1600

Boston, MA 02114

800-999-9080 ext. 6263

jschott@amsa.com



Session Objectives

- Discuss current identity fraud research
- Identify how identity theft occurs and how your personal information is used
- Identify what to do when your personal information has been lost or when you have been a victim of identity theft
- Identify how to minimize your risk for identity theft

Current Research



Current Research

2006 Identity Fraud Survey Report

- Provides a detailed, comprehensive analysis of identity fraud in the United States
- Co-released by the Better Business Bureau and Javelin Strategy and Research
- Issued as a longitudinal update to the Javelin *2005 Identity Fraud Report* and the Federal Trade Commission's (FTC) *2003 Identity Theft Survey Report*

Major Findings

	2003	2005	2006
US adult victims of identity fraud	10.1M	9.3M	8.9M
Fraud victims as % of population	4.70%	4.25%	4.00%
Total one year fraud amount	\$53.2B	\$54.4B	\$56.6B
Average fraud amount per fraud victim	\$5,249	\$5,885	\$6,383
Median fraud amount per fraud victim	\$750	\$750	\$750
Average consumer cost	\$555	\$675	\$422
Median consumer cost	\$0	\$0	\$0
Average resolution time	33 hours	28 hours	40 hours
Median resolution time	5 hours	5 hours	5 hours

Other Findings – Preventative Measures

Known information breach:

- 30% lost or stolen wallets, credit/debit cards and checkbooks
- 15% trusted associates
- 9% stolen mail or garbage
- 9% home computers

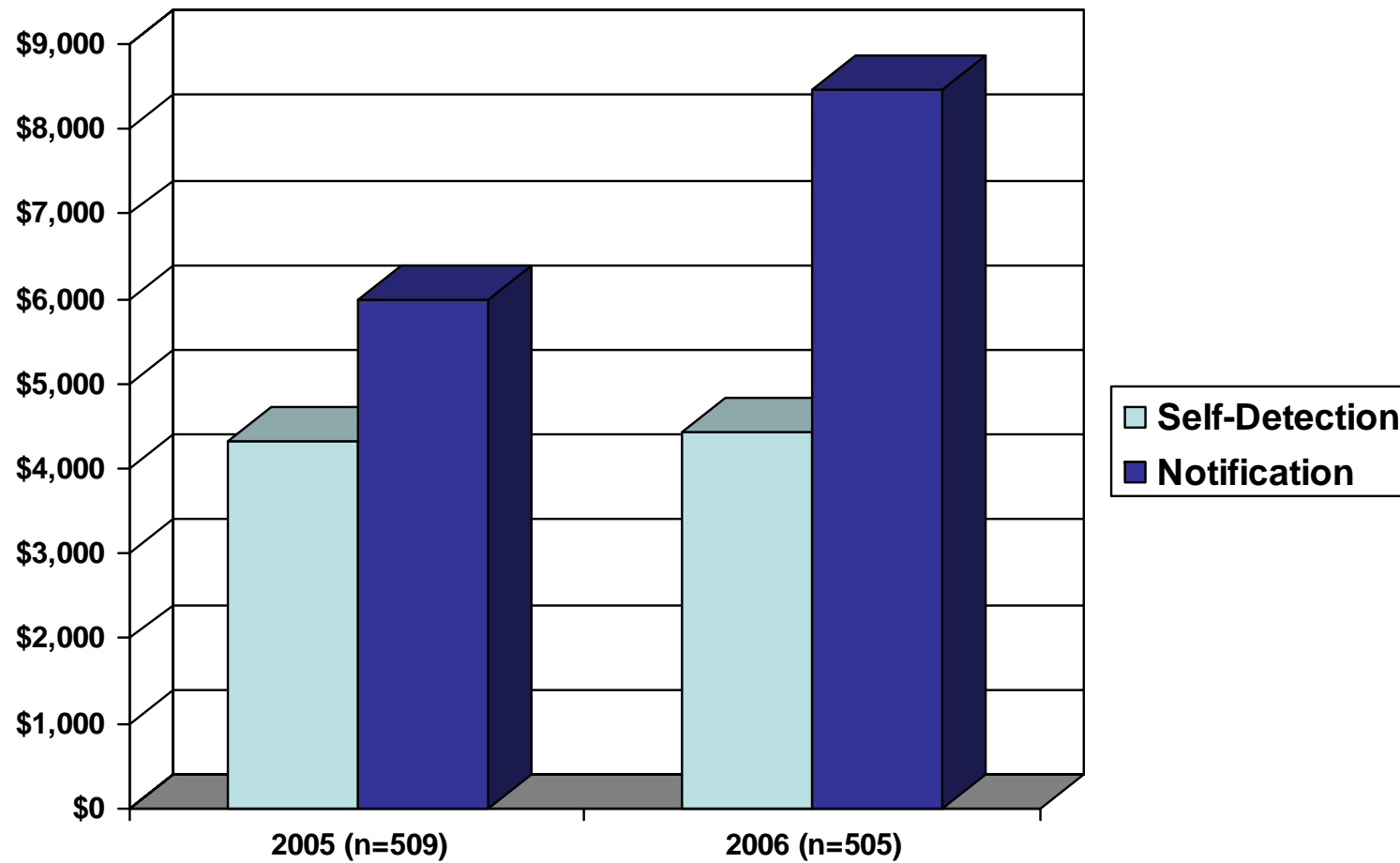
Fraud amounts from these cases equal 73% of the total fraud amount or \$41.5 billion!!




Other Findings – Detection

- The average number of days to self-detect identity fraud has increased by 98% from 2005 to 67 days
- The average number of days to be notified about identity fraud has increased by 58% from 2005 to 101 days
- The faster a fraud case is detected, the lower the fraud amount and consumer costs

Other Findings – Fraud Amounts





Other Findings – “Friendly Fraud”

Known fraud operator:

- Consumer costs increase as the relationship of the victim to the fraud operator gets closer
- Fraud perpetrated by friends, neighbors or in-home employees can cost the consumer rises to \$1,209 (with an average fraud amount of \$12,571)


How it Happens



How Identity Theft Occurs

Identity thieves can:

- steal your mail, including bank and credit card statements, credit card offers, new checks and tax information
- rummage through your trash, the trash of businesses, or public trash dumps
- steal your credit/debit card numbers by capturing the information in a data storage device (“skimming”)



How Identity Theft Occurs

Identity thieves can:

- steal your wallet or purse
- complete a “change of address form” to divert your mail to another location
- steal personal information found in your home
- steal personal information from you through email or phone by posing as legitimate companies and claiming they have a problem with your account (“phishing”)



Means of Access

Primary Business Controlled

- Taken by corrupt business employee (15%)
- Misuse of data from an in-store/online/mail/telephone transaction (7%)
- Some other way (7%)
- Stolen from a company that handles your financial data (6%)

Primary Consumer Controlled

- Lost or stolen wallet, checkbook or credit/debit card (30%)
- By friends, acquaintances, relatives or in-home employees (15%)
- From stolen paper mail or by fraudulent change of address (8%)
- Computer viruses, spyware, or hackers (5%)
- Phishing (3%)
- Garbage (1%)



How Your Information Is Used

Identity thieves can:

- call credit card issuer to change billing address
- open new credit cards in your name
- establish phone or wireless accounts in your name
- open bank account in your name
- buy a car by taking out an auto loan in your name
- get identification issued with their picture, in your name
- give your name to the police during an arrest



How to Know if You Have Been a Victim

- Failure to receive bills or other mail
- Receiving credit cards for which you didn't apply
- Being denied credit, or being offered less favorable credit terms, for no apparent reason
- Noticing suspicious charges on your credit card bills
- Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy

What to do When...



What to Do When...

Your personal information is lost or stolen


- Financial Accounts – close accounts
- Social Security Number – call toll-free fraud number of any of the three consumer reporting agencies and place an initial fraud alert on your credit reports
- Driver's License or Government-Issued Identification – contact the agency that issued the document and follow its procedures to cancel it and get a replacement



What to Do When...


You are a victim of identity theft

- Place a fraud alert on your credit reports and review them
- Close accounts that you know, or believe, have been tampered with or opened fraudulently
- File a report with your local police or the police in your community where the identity theft took place
- File a complaint with the Federal Trade Commission (877-IDTHEFT)



Fraud Alerts – Two Types

- Initial Alert
 - stays on your credit report for at least 90 days
 - appropriate if personal information is lost or stolen
 - consumer entitled to one free credit report from each of the three consumer reporting companies



Fraud Alerts – Two Types

- Extended Alert
 - stays on your credit report for seven years
 - appropriate if identity theft has occurred
 - consumer entitled to two free copies of credit report from each of the three consumer reporting agencies within 12 months
 - consumer's name removed from marketing lists of pre-screened credit offers for five years



ID Theft Affidavit

- Developed by credit grantors, consumer advocates and attorneys at Federal Trade Commission
- Provide information in this affidavit anywhere a new account was opened in your name
- Two parts - ID Theft Affidavit and Fraudulent Account Statement

Resolving Specific Problems



Fraudulent Electronic Withdrawals

- The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card, or another electronic way to debit or credit an account
- You have 60 days from the date your bank account statement is sent to you to report in writing any money withdrawn from your account without your permission
- Report lost/stolen ATM or debit cards immediately



Fraudulent Checks

- Stop payment on check and close checking account
- Request that banking institution contact the check verification service with which they do business so that retailers can know not to accept these checks
- Federal laws do not limit consumer losses, but state laws may – most state laws hold the banking institutions responsible for losses



Fraudulent New Checking Accounts

- Chex Systems, Inc. produces consumer reports specifically about checking accounts and is subject to the Fair Credit Reporting Act:

Chex Systems, Inc.

ATTN: Consumer Relations

7805 Hudson Road, Suite 100

Woodbury, MN 55125

800-428-9623

602-659-2197 (fax)

www.chexhelp.com

Protecting Yourself

Access to Your Personal Data

- Do not carry extra credit cards, your Social Security card, birth certificate or passport in your wallet or purse
- Remove your name from the marketing lists of the three credit reporting bureaus; call 888-5-OPTOUT or go online to www.optoutprescreen.com.
- Sign up for the FTC's National Do Not Call Registry and the Direct Marketing Association's Telephone Preference Service; call 888-382-1222 or go online to www.donotcall.gov
- Reduce the amount of junk mail you receive; send your name and address to the Mail Preference Service, PO Box 643, Carmel, NY 10512
- Install a locked mailbox at your residence or use a post office box or a commercial mailbox service
- Pick up new check orders at the bank rather than having them mailed to you



Credit Cards and Credit Reports

- Reduce the number of credit cards you use to a minimum.
- Keep a list of all your credit cards, bank accounts, and investments – the account numbers, expiration dates and telephone numbers – in a secure place so that you can quickly contact them
- Never give out your SSN, credit card number or personal information over the phone, by mail or on the internet
- Always take credit card receipts with you; never toss them in a public trash container
- Monitor your mail for billing statements and new or reissued credit cards; contact the financial institution if they do not arrive
- Check and review all three of your FICO scores and your credit reports at least once a year



Protecting Yourself: Passwords and PINs

- Use unique passwords including combinations of letter, number and special characters
- Change your passwords regularly
- Memorize your passwords; do not write them down
- Ask your financial institution to add extra security protection to your accounts



Internet and Computer Safeguards

- Purchase anti-virus software
- Keep your Operating Software updated
- Install a firewall on your home computer
- Take precautions with wireless networks
- When shopping online, do business with companies that provide transaction security protection and have strong privacy and security policies
- Before disposing of your computer, remove data by using a strong “wipe” utility program



How to Obtain Credit Report

Credit Agencies:

- Equifax www.equifax.com
- Experian www.experian.com
- Trans Union www.transunion.com

One free report from each agency every 12 months:

www.annualcreditreport.com



Resolving Mistakes on Your Credit Report

- Fully understand each listing in your credit report and be certain that you understand what's an error and what is not
- Create a list of the errors in your credit report
- Notify each credit reporting agency of all the errors in writing
- Notify the lender that has reported the erroneous information and ask them to correct their entry on your credit report
- Keep a copy of your correspondence

Online Resources



Online Resources

- Department of Justice Identity Theft and Fraud
www.usdoj.gov/criminal/fraud/idtheft.html
- FBI Crime Smart Information
www.fbi.gov/becrimesmart.htm
- FDIC Consumer Information
www.fdic.gov/consumers/index.html
- Federal Trade Commission
www.ftc.gov/idtheft/



Online Resources

- Identity Theft Resource Center
www.idtheftcenter.org
- National Consumers League
www.nclenet.org
- National Fraud Information Center
www.fraud.org
- Privacy Rights Clearinghouse Identity Theft Resources
www.privacyrights.org/identity.htm