Identity Theft and You

Updated May of 2007
Identity Theft

It’s not just in fairy tales any more!

Created By: Chipola College’s Information Systems
According to the Department of Justice, “Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.”
Identity Theft Statistics

Identity theft is one of the fastest growing consumer crimes in the U.S.
Identity Theft Statistics

In 2005, the Consumer Sentinel – a complaints database operated by the Federal Trade Commission – recorded over 680,000 fraud and identity theft complaints.
Of those complaints, over 430,000 were specifically listed as identity theft complaints.

That number continues to grow each year, as seen in this chart.
Sentinel Complaints by Calendar Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Fraud Complaints</th>
<th>Identity Theft Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>CY-2003</td>
<td>327,479</td>
<td>215,177</td>
</tr>
<tr>
<td>CY-2004</td>
<td>431,118</td>
<td>246,847</td>
</tr>
<tr>
<td>CY-2005</td>
<td>431,118</td>
<td>255,565</td>
</tr>
</tbody>
</table>
Since January of 2005, more than 100 million records that contain sensitive personal information have been involved in data exposures.
In 2006, there were at least 315 incidents of data exposures, which potentially affected more than 20 million individuals.

Disclosures of Data Incidents
Calendar Year 2006

Disclosures of Data Incidents

Calendar Year 2007

- Governmental or Military Agencies: 30.0%
- Educational Institutions: 19.1%
- General Business: 30.9%
- Health Care: 14.5%
- Banking: 5.5%

Surveys conducted by the Better Business Bureau, the Federal Trade Commission and other organizations produced this information:
Survey Findings

The mean fraud amount rose from 53.2 billion dollars in 2003 to 54.4 billion dollars in 2005 to 56.6 billion dollars in 2006.

http://www.privacyrights.org/ar/idtheftsurveys.htm
Survey Findings

The mean resolution time is at a high of 40 hours per victim in 2006 compared to 28 hours in 2005 and 33 hours in 2003.
How do these incidents occur?

Exposure of data occurs due to theft of computer files, theft of laptops, hacking into computer networks or web servers, and carelessness of employees.
Examples of Data Exposures

Some of the actual incidents that occurred during 2006 include:
Intrusion Software:

An employee with the Oregon Department of Revenue used an office computer to surf porn and downloaded a Trojan horse that was not yet identified to detection software.

The Trojan worked for 5 months, capturing and relaying data back to the hackers.

Confidential information of more than 1,300 taxpayers was placed at risk.
Employee Negligence:

Two Massachusetts newspapers, the *Boston Globe* and the *Worcester Telegram & Gazette*, reported that credit card and banking information of as many as 202,000 customers was accidentally delivered with the bundles of papers in Worcester.
The Los Angeles County Department of Public Social Services reported that documents were left next to a recycling bin outside one of their offices.

The documents contained names, addresses, phone numbers, Social Security numbers and medical information of people who received services.

A potential 94,000 people are affected.
Equifax, a leading credit reporting agency, announced that an employee’s laptop computer was stolen while the employee was riding a train in London. The laptop contained the names and Social Security numbers of all of Equifax’s 2,500 U.S. employees. The data was not encrypted but was stored in a jumble, which supposedly makes it more difficult to match numbers with names.
Theft of Computers, Devices, Files:

The Colorado Mental Health Institute reported that files containing personal information of 287 employees, patients and former patients were stolen.

The paper files were in a briefcase taken from a hospital employee’s car.
The Transportation Security Administration (TSA) lost an external, portable computer hard drive that contained SSNs, bank data and payroll information for about 100,000 employees who worked for the Homeland Security Agency between 2002 and 2005. Authorities are unsure if the device is still in the building or if it was stolen.
Loss of Computers, Devices, Files:

A thumb drive containing the names and SSNs of about 1400 past and current employees of the Maryland State Department of Natural Resources is lost and presumed missing. It was used by an employee to take work home with him. The affected individuals are primarily law enforcement officers.
At Kent State University in Ohio, cybercrooks accessed a database containing the names and Social Security numbers of 19,000 applicants.

A U.S. Department of Defense computer was accessed by an intruder and confidential health care insurance information of more than 14,000 people was compromised.
In Rhode Island, thousands of credit card numbers were stolen from a state government web site that allows residents to register their cars and buy state permits.

A private company actually runs the state’s website, and they announced that 4,118 credit card numbers had probably been taken.
Programming Glitches:

Old Dominion University in Virginia reported that 601 students’ names and Social Security numbers were inadvertently placed on a university web server two years ago.

At Pekin High School in Illinois, more than 2,000 high school students’ personal information was made accessible on the school district’s web site.
Employee Theft:

In Michigan, investigators reported that a Fifth Third Bank employee gained access to the personal information of female television personalities and nearly 1,000 other customers.

The employee would then use the personal information to stalk the female television personalities.
The New Jersey Department of Labor and Workforce Development reported that the personal information of nearly 500 unemployed New Jerseyans was mailed to the homes of other jobless people in the state due to a malfunction in a mail process machine.
Glitch in Business Process:

The names and SSNs of 139 Champaign, Illinois, current and former police officers were left on a computer that was donated to charity. The problem surfaced in April of 2007 when the city’s Information Technologies department received a call from Simplified Computers, the company that purchased the computer in question.
Data Exposures in 2007

Similar incidents have occurred already in 2007.
Data exposure can affect you!

As you can see by some of the previous examples you are at risk of becoming a victim of identity theft.
Data exposure can affect you!

Data exposures can occur at any company, institution or agency regardless of the level of security in place at the time. A simple act of carelessness on the part of an employee can put you at risk.
Are you at risk of identity theft?

Even an individual with few assets and little money is not safe from identity thieves.
Identity thieves steal your name and reputation to use for their own financial gain.
Basically, identity thieves will steal your future, leaving you in debt with damaged credit and the responsibility of fixing the mess.
What else makes you a target?

Your daily activities may also expose you to this crime.

For example:

Do you use a personal computer for online banking?
Do you use a personal computer to buy merchandise or purchase tickets for travel, concerts, etc.?
Do you receive credit card offers in the mail?

Do you shred credit card offers before discarding them?
Do you store personal information in your computer?

Do you use a cell phone?
Do you use your Social Security number for identification?
Each of these routine actions places you at risk of being a victim of identity theft because each requires you to share personal information, such as your bank and credit card account numbers, Social Security number, etc.
The stories of identity theft victims are horrifying and ongoing, with most victims spending thousands of dollars and fighting for several years to get their lives back.
Furthermore, you should know that there is no ONE central law enforcement agency established to handle identity theft.
However, a cybertool is available to assist law enforcement agencies. Consumer Sentinel offers access to the public as well as a restricted site to law enforcement agencies.
The U.S. Federal Trade Commission claims that Consumer Sentinel is an “innovative, international law enforcement fraud-fighting program”.

Restricted site access is provided to law enforcement agencies.

http://www.consumer.gov/sentinel/members.htm
The U.S. Federal Trade Commission claims that Consumer Sentinel is an “innovative, international law enforcement fraud-fighting program”.

Restricted site access is provided to law enforcement agencies.

http://www.consumer.gov/sentinel/members.htm
Tour Consumer Sentinel to see how it may help you.

http://www.consumer.gov/sentinel/tour.htm

The tour requires a browser and media player from the following:

**BROWSER**
- Internet Explorer 5.0
- Netscape 4.7 or higher

**MEDIA PLAYER**
- QuickTime 4 (for Macintosh Users)
- Real Player
- Windows Media Player
Tour Consumer Sentinel to see how it may help you.

http://www.consumer.gov/sentinel/tour.htm

The tour requires a browser and media player from the following:

**BROWSER**
- Internet Explorer 5.0
- Netscape 4.7 or higher

**MEDIA PLAYER**
- QuickTime 4 (for Macintosh Users)
- Real Player
- Windows Media Player
Note that most states have passed some sort of “identity theft” law that may punish the offender, but that law does not prevent you from being a victim.
You will have to rely upon yourself and a few tips from the experts.

First, an overview of the methods used by identity thieves.
Some of the methods used by identity thieves are very low tech.

Other methods require more of an investment on the part of the thieves and a little more knowledge of technology.
Some people believe that an identity thief has to be a computer hacker.

Others believe that as long as they have not purchased items online or used e-commerce for banking or paying bills, then they are safe from identity theft.
The truth is that your personal information is already in the public domain.

Companies have your personal info and are just as susceptible to identity thieves as you are.
Additionally, your information exists in so many places – electronically and on paper – that you cannot possibly account for it.
Identity thieves can gain access to your personal and financial information through a variety of methods, such as:

- mail theft
- dumpster diving
- account takeovers
- eavesdropping
- shoulder surfing
- phishing
- pharming
- skimming
- pretexting
- scamming
MAIL THEFT is an easy and low-tech method of committing identity theft.

It is as easy as retrieving incoming or outgoing mail from your unsecured and very accessible mailbox.
Some examples:

Pre-approved credit card applications can be removed from your mailbox, and the card holder’s address can be altered. The thief then mails your card application back to the credit card company. He can potentially obtain a new credit card in your name, sent to his address.

Account numbers can be obtained from stolen credit card statements, and purchases made with the stolen numbers.
A new ATM or credit card can be removed and used.

And a thief can obtain enough information to open new accounts in your name.
DUMPSTER DIVING is also a low-tech and efficient method of committing identity theft.

Dumpsters behind businesses are usually more profitable for an identity thief, especially a business such as a CPA or a retailer that might retain customer information without shredding it.
It doesn’t sound very appealing but dumpster diving can be quite lucrative.

Think of all the personal papers that you discard. Do you shred them beyond repair?

And what about your old credit cards?
And what did you do with the hard drive from your last computer or your old floppy disks or CDs?
SHOULDER SURFING is another low-tech way to steal high-tech information.

A thief can watch as you key your PIN or credit card number into a keypad or listen as you recite the card number to an operator.
Sophisticated thieves may use binoculars or telescopes to spy on you.

Others may use recording devices to record the tones of the numbers you key.

Those tones can be analyzed and reproduced.
Some law enforcement officers believe 90 percent of the credit card thefts occur at airports, hotels and train stations.

They say it is a common practice for a thief to stand on a mezzanine level and observe the phones with binoculars or to use a camera with a zoom lens to record the keys punched in.
Cell and cordless phones, while incredibly convenient, are not secure.

We have become so used to being connected all of the time, that we forget others may be listening.
An example of electronic eavesdropping occurred in 1998 and involved a case of a mobile data terminal intercept.

The perpetrator used a device connected to a scanner. It was set to receive and translate emergency frequencies, like those employed by police departments and fire services.
The U.S. Attorney’s Office prosecuted the perpetrator for capturing the digital stream of information that was transmitted from a police department to a police cruiser’s mobile data terminal.

The scanner was connected to a peripheral device then to a laptop, which had software that could decode the transmission.
The transmission included people’s social security information, dates of birth, and possibly criminal histories. That information was illegally sold on the internet.
Placing credit card orders or giving out any confidential information via a cell phone or cordless phone is not secure.

Cordless phones transmit over radio frequencies. Conversations over some cordless phones can be picked up with devices like a baby monitor or a radio scanner.
PHISHERS and PHARMERS trick you through spoofed e-mails (e-mails that have forged sender addresses or headers) and redirected websites that request your account number, password and other info.
These scammers can then gain access to your financial info and accounts.
A frightening example of one phishing scheme involved the Department of Labor’s web portal, GovBenefits.gov, a website that 16 federal agencies use, including the Internal Revenue Service. The programming glitch was the byproduct of programmers trying to make navigation easier for users. The result allowed phishers to redirect users to another site that requested social security and credit card numbers.
Another scheme where the identity thieves posed as the government....
In September of 2005, the FBI reported an ongoing scheme that involved jury service. Individuals would contact citizens by phone and advise them that they had been selected for jury duty. They would then request the citizens to verify names and social security numbers and then ask for credit card numbers. If the citizens refused, they were threatened with fines.
SKIMMING refers to the process of quickly and temporarily stealing a credit card and running it through a skimmer.

A skimmer is a credit card reader that has been reprogrammed to steal information off of a card.

Often this takes place in a hectic retail store, where the action is less likely to be noticed.
Thieves can place a fake front over an ATM machine.

They may attach a hidden camera angled to capture the image of the screen and the PIN you type.
The hidden camera can transmit wireless photos of the keypad and the monitor up to 200 meters away.

The camera hidden in the pamphlet box includes its own battery and transmission antenna.
PRETEXTING is the illegal act of acquiring a consumer’s personal information under false pretenses.

Some methods to acquire this information include phone surveys, electronic sweepstakes, the ‘Free Credit Report’ scam, and other e-mail scams.
A pretexting e-mail scam that all of us may have seen is the ‘Nigerian’ scam.

LAGOS, NIGERIA.

ATTENTION: THE PRESIDENT/CEO

DEAR SIR,

CONFIDENTIAL BUSINESS PROPOSAL

HAVING CONSULTED WITH MY COLLEAGUES AND BASED ON THE INFORMATION GATHERED FROM THE NIGERIAN CHAMBERS OF COMMERCE AND INDUSTRY, I HAVE THE PRIVILEGE TO REQUEST FOR YOUR ASSISTANCE TO TRANSFER THE SUM OF $47,500,000.00 (FORTY SEVEN MILLION, FIVE HUNDRED THOUSAND UNITED STATES DOLLARS) INTO YOUR ACCOUNTS. THE ABOVE SUM RESULTED FROM AN OVER-INVOICED CONTRACT,
With the Nigerian scam, a foreigner poses as a wealthy family member and solicits a consumer’s assistance via e-mail to help transfer millions of dollars from his homeland to the United States.

In return, the consumer is to be rewarded with a percentage of the fortune.
For all of these methods, the experts have suggestions of things we can do to protect ourselves.
The methods mentioned here are certainly not all of the ways in which someone can extract personal and confidential data. According to the FBI, “the sources of information about you are so numerous that you cannot prevent the theft of your identity. But you can minimize your risk of loss by following a few simple hints.”

1http://www.fbi.gov/majcases/fraud/fraudschemes.htm
Identity Theft
What should you do?

The following are some tips to follow and websites to visit.
FBI TIPS...

To Avoid Impersonation/Identity Fraud:

✓ Never throw away ATM receipts, credit card statements, credit cards, or bank statements in a usable form.

✓ Never give your credit card number over the telephone unless you make the call.

✓ Reconcile your bank account monthly and notify your bank of discrepancies immediately.

✓ Keep a list of telephone numbers to call to report the loss or theft of your wallet, credit cards, etc.
✓ Report unauthorized financial transactions to your bank, credit card company, and the police as soon as you detect them.

✓ Review a copy of your credit report at least once each year. Notify the credit bureau in writing of questionable entries and follow through until they are explained or removed.

✓ If your identity has been assumed, ask the credit bureau to place a statement to that effect in your credit report.

✓ If you know of anyone who receives mail from credit card companies or banks in the names of others, report it to local or federal law enforcement authorities.
WHAT ELSE CAN YOU DO?

✓ Educate yourself and stay alert.
✓ Protect your information and that of your co-workers.
✓ Use long and complicated passwords for your banking, e-mail, and other computer accounts.
✓ Know what to do in the event of an exposure or incident.
MORE TIPS....

✓ Shop only on websites that offer Secure Socket Layer (SSL) (https:) protection, VeriSign Secured protection, or other reputable means of encrypting your confidential data.

✓ Avail yourself of the resources available on the internet and elsewhere.
During tax time, take these extra precautions with your mail:

✓ During January, check your mailbox for tax-related information, such as your W-2 form or the 1099 form. These forms typically have your Social Security Number listed, as well as the name of your employer, your bank, mutual fund, etc.
Use a mailbox that locks or use a Post Office Box.

Try to retrieve your mail as soon as possible after it has been delivered. Never leave mail in your box overnight.

If you go on vacation, have your mail held at the Post Office or have a trusted neighbor retrieve it.
If you moved during the year, notify any payers of your new address. Do not rely on the Postal Service’s change of address service.

Mail your tax return at the Post Office or at an official USPS blue mail collection box BEFORE the last collection time. Do not place such mail in a mailbox that has no more pickups that day.
Monitor your credit report from all three credit reporting agencies at least once a year.

Equifax
www.equifax.com

Experian
www.experian.com

Trans Union
www.transunion.com
Contact all three of the credit reporting agencies if you believe you have been the victim of fraud.

Equifax - 888-525-6285
www.equifax.com

Experian - 888-397-3742
www.experian.com

Trans Union - 800-680-7289
www.transunion.com
FREE ANNUAL CREDIT REPORT

You are entitled to a free copy of your credit report from each credit agency at your request every 12 months.

To read more details about this free credit report, visit:

http://www.ftc.gov/bcp/conline/pubs/credit/freereports.htm
Fair Credit Reporting Act

It is recommended that you check your credit report frequently if you believe or have been told your personal information has been exposed.

Identity theft may not occur right away. Your information could be changing hands for a period of months or years before you discover a problem.
One suggestion from the experts is to stagger your requests -- that is, request a report from a different agency every 4 months.

Using that method, you will be able to keep a close check on your credit history for free and would be able to request a new report from the same agency at 12-month intervals.

annualcreditreport.com
Only one website is authorized to fill orders for this free annual credit report.

Other sites may be imposters, so only use the website and/or contact information listed here or the info on the www.ftc.gov website.

annualcreditreport.com
Or call: 1-877-322-8228
Stop telemarketing calls.
Register for free on the FTC’s National Do Not Call Registry.

REGISTER YOUR HOME OR MOBILE PHONE NUMBER

Follow the registration steps below. Click here for detailed registration instructions.

1. Enter up to three phone numbers and your email address. Click Submit.
2. Check for errors. Click Register.
3. Check your email for a message from Register@donotcall.gov. Open the email and click on the link to complete your registration.

If you share any of these telephone numbers with others, please remember that you are registering for everyone who uses these lines.

STEP ONE

Area Code:  
Phone:  

Email Address:  
Confirm Email Address:  

Your email address MUST be correct to process your registration.

Enter phone numbers with or without a dash. Do not use spaces or periods.
Your landline phone or cell phone can be listed so that most telemarketers will not call you. The Federal Trade Commission, the Federal Communications Commission and the states are enforcing this registry. It should stop most, but not all, telemarketing calls.

National Do Not Call Registry

www.donotcall.gov
You register your phone numbers for 5 years. Most telemarketers should not call the numbers once the numbers have been on the registry for 31 days. You can file a complaint at the website if they do.

Note: You will need an e-mail address in order to confirm the registration.
Opt-Out

Opt-Out of having pre-approved credit offers sent to you for two years.
Stop agencies and companies from sharing your information for promotional purposes.
Stop direct mail marketing from many national companies for five years.

Visit this FTC site to learn how:
www.ftc.gov/bcp/conline/pubs/alerts/optoutalert.htm
Check your scanned Public Records. For any state where you may have a legal document recorded, peruse each document for your personal information.

www.myfloridacounty.com
This is an example of the very public nature of Florida’s Public Records.

The document shown here is the recorded signature of former CIA Director Porter Goss and Mrs. Porter Goss. Social security numbers for both are listed on this document, which recorded property they own in Lee County, Florida.

(Note: We have redacted the SSNs with a smudge tool, but the SSNs are actually clearly visible on the internet.)
Did you know that the State of Florida has one of the most open public records laws in the country?

Documents are scanned on a regular basis and made available to the public. Some documents are free, while others require a small fee to access.

Currently, Florida law does not require personal information to be redacted by the agency scanning and posting the documents on the internet.
Review your public records by visiting the [www.myfloridacounty.com](http://www.myfloridacounty.com) website.

Know your rights.... Utilize Florida Statues 119.071 (5)(7b) to have any Florida Clerk of Court redact any of your personal information.
Free to anyone who has access to the internet, the SSDI is a database that allows interactive searches through more than 76 million records of deceased persons.

The SSDI is available on a variety of sites. One of the most user-friendly is ssdi.rootsweb.com.
The Social Security number was clearly visible until we used our smudge tool to block it.

This is the death record of the legendary Cary Grant, with the SSN visible on the SSDI website.
Social Security Death Index

The SSDI website displays all of the information that you would need to steal a person’s identity.

In the example displayed in the previous slide, the SSN has been redacted by us through a smudge tool. But on the SSDI site and other commercial sites, the SSNs and dates of birth are clearly visible.
Social Security Death Index

Of note, the Social Security Administration does not publish the “death index.”

But the SSA does make that information available to commercial entities who then publish the information on the internet legally.
Social Security Death Index

From the SSDI site, you can even order a photocopy of the actual application for a Social Security card.

A great tool for genealogists and an even better one for identity thieves.
Of note, the experts say that children and the nation’s seniors – while not targeted in particular – are very susceptible to identity theft.

If you were born in the United States, you were assigned a social security number at birth. Credit can be obtained from that moment in your name.
Parents, namely those involved in domestic abuse situations or divorce, have obtained credit in their child’s name, actually ruining that child’s credit before the child reaches the age of 18.

**Identity Theft and Children’s Credit**

**PROTECT YOUR CHILD FROM IDENTITY THEFT**

- Limit access to your child’s Social Security number by not providing it on sports team sign-ups and other non-essential forms.
- Shred all papers that contain account or Social Security numbers.
- Do not carry your child’s Social Security card or number in your wallet.
- College students should ask their school not to use their SSN as their college ID number.
- Social Security numbers should never be given out over the phone or on the Internet.
- Observe the mail. If bills, statements or credit card offers begin arriving in your child’s name, call the credit reporting bureaus to check on his or her credit record. There should be none.
And now a few words about other security issues, such as the publishing of identifying information to sites such as MySpace.com, Facebook, chat rooms, forums, and blogs....
Social Networking Sites

The internet provides access to hundreds of social networking sites.

As great as these sites are for teens, advertisers, music groups, etc., there are some dangers.
Social Networking Sites
And sexual predators

Sexual predators actively troll these sites, luring people of all ages away from their safe surroundings.

Tidbits of your personal info is enough for most predators to locate you.

And employers are now searching these sites looking for info regarding prospective employees.

It is estimated that between 25 and 50 percent of employers who are engaged in college hiring will use MySpace.com and Facebook as part of the background process.
Social Networking Sites

And your professional career

Employers can base the decision to not hire you on your online profile, the photos that you post, the language that you use, etc.

And they can do this legally.
Social Networking Sites
And your professional career

Information posted on social networking sites and discovered by employers is not covered by the Fair Credit Reporting Act.

Employers do not have to disclose to you what they have found out about you from one of these sites.
Social Networking Sites

And your professional career

Experts recommend that you should remove all profiles from the Internet.

Relying on privacy settings will not deter all employers, especially the ones who can use their child’s e-mail account.

www.privacyrights.org/fs/fs16a-califbck.htm
Visit the websites listed below for more information about identity theft and suggestions on how to protect your identity.

Microsoft.com: Video – What you should know about phishing identity-theft scams
http://www.microsoft.com/athome/security/email/phishing/video1.mspx

Microsoft.com: Recognize phishing scams and fraudulent e-mails
http://www.microsoft.com/athome/security/email/phishing.mspx

Microsoft.com: What to do if you’re a victim of credit card fraud
http://www.microsoft.com/athome/security/privacy/fraudvictim.mspx

Office of the Attorney General of Florida: Identity Theft
http://www.myfloridalegal.com/identitytheft

Office of the Attorney General of Florida: Florida’s Identity Theft Victim Kit

Office of the Attorney General of Florida: Preventing Identity Theft
FTC and other federal agencies’ new site: onguardonline.gov

Identity Theft Resource Center (A Non-Profit Organization): http://www.idtheftcenter.org


Anti-Phishing Working Group: Committed to wiping out Internet scams and fraud http://www.antiphishing.org/phishing_archive/phishing_archive.html


FL Dept of Agriculture and Consumer Services: Identity Theft – don’t be left in the dark http://800helpfla.com/identity.html


United States Department of Justice: Fraud http://www.usdoj.gov/criminal/npftf


This presentation was produced and distributed by:

Chipola College’s Information Systems