ID THEFT
THE NAME GAME

- Don't Get Played!

Identity Theft: The Name Game

- Identity Theft continues to be a major law enforcement problem in this country
- Learn the basics- What it is, how it works, who the perpetrators are and how to defend against them.

10 Key Data Points on Identity Fraud

Identity fraud trends

1. **The number of adult victims of identity fraud has declined marginally between 2003 and 2006, from 10.1 million people to 8.4 million people, in the United States**
2. **The average fraud amount per case has increased**
3. **The vast majority of identity fraud victims (68%) incur no out-of-pocket expenses.**

10 Key Data Points on Identity Fraud

4. Victims are spending more time to resolve identity fraud cases. (about 40 hrs)
5. Most data compromise - 90 percent - takes place through traditional offline channels and not via the Internet, when the victim can identify the source of data compromise.
6. Lost or stolen wallets, checkbooks or credit cards continue to be the primary source of personal information theft. (30 percent).

10 Key Data Points on Identity Fraud

7. Almost half (47%) of all identity theft is perpetrated by friends, neighbors, in-home employees, family members or relatives - someone known - when the victim can identify the perpetrator of the data compromise.
8. Nearly 70% of consumers are shredding documents, so that trash as a source of data compromise is now less than 1 percent.

10 Key Data Points on Identity Fraud

9. The 65+ demographic age group has the smallest rate of identity fraud victims (2.3%).
10. Over half the victims were 18-39 years old (29% for ages 18-29). The 35-44 demographic age group has the highest average fraud amount ($9,435).

NOTE:

47% of victims could identify the source of the data compromise.

36% of victims could identify the person who misused their information.

The Criminals

- **"<u>Low tech" Identity Criminals</u>**
- Dumpster Divers (commercial and residential trash)
- Theft of wallets, purses, and mail

The Criminals

- **<u>High Tech Identity Criminals</u> get info from:)**
- **Internet (company databases and web sites)**
- **Public Domain public filings, like deeds and some court records).**
- **Collusive Employees (large scale theft from billing centers, financial institutions government agencies employees**
- **Hacking**
- **Email and telephone scams (phishing).**
- **Careless online shopping and banking**

Main Types of Identity Theft

Financial ID Theft

- **Criminal ID Theft**
- **Identity Cloning**
- **Corporate ID Theft**
- **Child ID Theft (Yes, your child's identity can also be stolen!!)**

Financial ID Theft

The weapon? Personal information, such as:

- **Name**
- **Address**
- **Date and place of birth**
- **Mother's maiden name**
- **Social Security number (the most coveted number of all, which cannot be changed even after it's been stolen)**

"Once they have this information, they own you…. They are you

Financial ID Theft

- **"Phishing" scams - criminals send out bogus e-mails telling recipients that they need to confirm certain account details to reactivate their accounts or claim prizes.**
- **"Skimming" - a data storage device that captures credit card information.**
- **"VISHING" (VOIP) Voice over internet Protocol**

BUT NOTE: Legitimate businesses and organizations do not send emails or pop-ups to request personal information from you.

Financial ID Theft

PayPal

Thank You for Your Attention!

Because **PayPal** is maintaining physical, electronic and procedural safeguards that comply with federal guidelines to guard your personal information against unauthorized access, we restricted some of our services for our clients, in order to be able to complete this process.

At this time we need you to renew your online profile and update our existing database, in order to be able to use all the PayPal services with no restriction. As soon as our database will be updated we will make a few anouncements to our customers regarding this notification, so please renew your online profile with no delay.

This process is compulsory for all our customers. Please continue to the link below:
http://www.paypal.com/cgi-bin/webscr?cmd=p/ema/index-outside

We will verify the information with your financial institution.

PayPal is dedicated to providing you with exceptional service and to ensuring your trust. If you have any questions regarding our services, please call our customer service.

Warmly ,
PayPal Security Center

Copyright © 1998-2006 PayPal. All Rights Reserved.

Financial ID Theft

Phishing Example

The Bank of America User Agreement states that Bank of America, at its sole discretion, reserves the right to limit an account for any violation of the User Agreement, including the Acceptable Use Policy.

Under the Acceptable Use Policy, Bank of America may not be used to send or receive payments or donations for obscene or certain sexually oriented goods or services.

We are hereby notifying you that, after a recent review of your account activity, it has been determined that you are in violation of Bank of America Acceptable Use Policy. Therefore, your account has been temporarily limited for: ifriends.com cam shows

Please sign in to your Bank of America account and update your billing information:

Click here to update your account

Please follow the system instructions, everything takes 1 minute.

If you decide to close your account and you have a remaining balance, you may withdraw the funds to your bank account. Information on how to withdraw funds from your Bank of America account can be found at our Help Center.

Phishing Example

Financial ID Theft

- ☑ Forward the phishing email to spam@uce.gov and to the company, bank, or organization impersonated in the email.
- ☑ You also may report phishing email to the Anti-Phishing Working Group at reportphishing@antiphishing.org. This is a consortium of internet service providers, security vendors, financial institutions and law enforcement agencies, which use these reports to fight phishing.

Financial ID Theft (PREVENTION)

- ✖ Don't open or reply to email or pop-up messages that ask for personal or financial information.
- ✖ Don't click on links in the message.
- ✖ Don't cut and paste a link from the message into your Web browser. (Phishers can make links look like they go one place, but actually send you to a different site.)

Financial ID Theft (PREVENTION)

- ✖ Don't rely on a phone number or area code in the message (phone technology allows scammers to use an area code different from where they really are)
- ✖ Don't e-mail personal or financial information.
- √ Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them.

Financial ID Theft (PREVENTION)

DO:

1. **Use virus and security protection.**
2. **Completely erase the hard drive of any computer you plan to give away.**
3. **Use one credit card exclusively for Internet shopping. If your information falls into the wrong hands (through hacking, intercepted mail, etc.), you can just cancel the card and continue using another one in the "real world."**

Criminal ID Theft

- **The imposter in this crime provides the victim's information instead of his or her own when stopped by law enforcement. Eventually when the warrant for arrest is issued it is in the name of the person issued the citation- yours.**

Identity Cloning

- **In this crime the imposter uses the victim's information to establish a new life. They work and live as you.**
- **Examples: Illegal aliens, criminals avoiding warrants, people hiding from abusive situations or becoming a "new person" to leave behind a poor work and financial history.**

Identity Theft and Children

About this crime:

Typically falls into all three categories:

- Financial
- Criminal
- ID Cloning

Telephone and internet applications (information is taken at face value)

The age of an applicant becomes official with the first credit application

STAY ALERT (WARNING SIGNS)

- To help stay on top of the situation, continue to monitor your credit reports and read your financial account statements promptly and carefully.
- You may want to review your credit reports once every three months in the first year of the theft, and once a year thereafter. And stay alert for other signs of identity theft, like:

STAY ALERT (WARNING SIGNS)

- **failing to receive bills or other mail.**
- **receiving credit cards that you didn't apply for.**
- **being denied credit, or being offered less favorable credit terms, such as a higher interest rate, for no apparent reason.**
- **getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.**

What Should I Do To Avoid Becoming A Victim

- To reduce or minimize the risk of becoming a victim of identity theft or fraud, the Identity Theft Resource Center recommends. For starters, just remember the word "**SCAM**":

What Should I Do To Avoid Becoming A Victim

S - Be stingy with your personal information – don't give it to others unless you have a reason to trust them, regardless of where you are.

C - Check your financial information regularly, and look for what should be there and what shouldn't. You generally have 60 days to dispute items on your bank statement.

A - Ask periodically for a copy of your credit report. (Online at https://www.annualcreditreport.com, or call 1–877–322–8228, or TDD at 1–877–730–4104.)

M - Manage and maintain your personal information in a safe place.

What Should I Do If I've Become A Victim

- ☑ **Get an ID Theft Victims Kit**. (Call the Kentucky Attorney General's Office at 1-888-432-9257, or get it online at http://ag.ky.gov/consumer/.)
- ☑ **Report the incident to law enforcement.** (Your local police department or the Kentucky State Police.)
- ☑ **Call the fraud units of the three main credit bureaus** and ask that your credit reports be "flagged with a fraud alert".
  - Equifax, 1-800-525-6285, TDD: 800-255-0056.
  - TransUnion, 1-800-680-7289, TDD: 877-553-7803.
  - Experian, 1-888-EXPERIAN, TDD: 800-972-0322

What Should I Do If I've Become A Victim

There are two types of alerts:

An <u>initial alert</u> stays on your credit report for at least 90 days. (If you suspect you have been, or are about to be a victim.)

An <u>extended alert</u> stays on your credit report for seven years.(If you are a victim.)

What Should I Do If I've Become A Victim

- **<u>Active Duty Alerts For Military Personnel</u>**
- If you are a member of the military and away from your duty station
- In effect for one year (can be extended)
- Removes you from marketing list for pre-screened credit card offers for two years

What Should I Do If I've Become A Victim

- **Consider putting a "security freeze" on your credit report with each credit bureau**. This limits the sharing of your credit report with others, such as potential creditors, without your authorization. It costs $10 each time you place, lift or remove a freeze. For information, call Equifax at 800-685-1111, TransUnion at 888-909-8872, and Experian at 888-397-3742.
- **Opt out of receiving pre-screened or pre-approved credit offers**. Do it online at www.optoutprescreen.com, or call 888-5OPTOUT. This stops offers that go through the credit bureaus, but may not stop other offers. It's good for five years or you can make it permanent.

What Should I Do If I've Become A Victim

- **To stop junk mail**, do it online at the Direct Marketing Association's website: (www.dmaconsumers.org/cgi/offmailinglist) for a $1 fee charged to your credit card, or send a letter and a $1 check or money order to Mail Preference **Service, Direct Marketing Association, PO Box 643,Carmel, NY 10512.**
- **When ordering your free annual credit report, go to annualcreditreport.com.** Some other websites use the word "free" in the website address, but then only offer the free credit report as part of a package that you pay for.

What Should I Do If I've Become A Victim

- **Consider Putting a Security Freeze on Your Credit Report (effective July 12, 2006.)**
- A security freeze means that your credit report or credit score cannot be shared with others, such as potential creditors, without your authorization.

What Should I Do If I've Become A Victim

- This can help prevent further identity theft, because most businesses will not open credit accounts without first checking your credit report.
- Additionally, if someone tries to change certain information in a frozen credit report (like your name, address, birth date, or SSN), the credit bureau must send written confirmation of the change to you within 30 days.

What Should I Do If I've Become A Victim

- Each credit bureau may charge you up to $10 for security freezes, but there is no fee for an identity theft victim who provides a valid police report upon request. (The amount of the fee is subject to a yearly CPI adjustment.)

What Should I Do If I've Become A Victim

- Keep complete records (keep detailed notes and records of all telephone conversations with credit bureaus, creditors, debt collection agencies or law enforcement agencies) ID THEFT VICTIMS KIT

What Should I Do If I've Become A Victim

- Contact all creditors with whom your name or identifying data have been fraudulently used.
- Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge.

What Should I Do If I've Become A Victim

- **Contact the major check verification companies if you have had checks stolen or bank accounts set up by an identity thief:**
  Telecheck: 1-800-710-9898
  Certegy: 1-800-437-5120

- **To find out if a thief has been passing bad checks in your name:**
  Call SCAN: 1-800-262-7771

It's the Law

- **Federal Law**

The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028) is the federal law making identity theft a crime

It's the Law

- Kentucky's law
  KRS 514.160
  KRS 514.170 (trafficking)
  Violation code 23310

Specific Problems

- Criminal Violations

If wrongful criminal violations are attributed to your name:

1. **Contact the arresting or citing law enforcement agency**

1. **File an impersonation report.**

Specific Problems

- Have your identity confirmed:

Police department takes a full set of your fingerprints and your photograph, and copies any photo identification documents like your driver's license, passport or visa.

Specific Problems

- Fake Driver's License

If you think your name or SSN is being used by an identity thief to get a driver's license or a non-driver's ID card, contact your DMV.

Note: **In Kentucky your drivers license can be flagged if you are a victim of identity theft.**

Specific Problems

- **Mail Theft**
  U.S. Postal Inspection Service (USPIS)
- **Social Security Number (SSN) Theft and Misuse**
  call: 1-800-269-0271; fax: 410-597-0118

Internet Resources

Try these web sites for more information about ID theft:

- Kentucky Attorney General Office of Consumer Protection www.ag.ky.gov/consumer/
- Better Business Bureau www.bbbonline.org/IDTheft
- Privacy Right Clearinghouse www.privacyrights.org/identity.htm
- Federal Trade Commission www.ftc.gov/idtheft www.onguardonline.gov/
- ScamBusters www.scambusters.org
- Identity Theft Resource Center www.idtheftcenter.org
- Experian www.experian.com
- Equifax www.equifax.com
- Trans Union www.transunion.com

Identity Theft

- **No matter what type of identity theft is involved. The result is a long and sometimes arduous road to recovery.**
- **As in all crimes, preventing the crime from occurring in the first place is key**.

Identity Theft is a Crime