Identity Theft
Awareness, Deterrence and Recovery

Ian Howe
Assistant Attorney General
Consumer Protection Division

Opinions presented are those of the speaker and not an official opinion of the Office of the Texas Attorney General.

Identity Theft Presentation Overview

- Awareness
  - What is identity theft?
  - How is stolen personal information used?
- Deterrence**:** What can you do to deter an identity thief?
- Recovery**:** How do you recover from identity theft?

What Is Identity Theft and How Often Does It Happen?

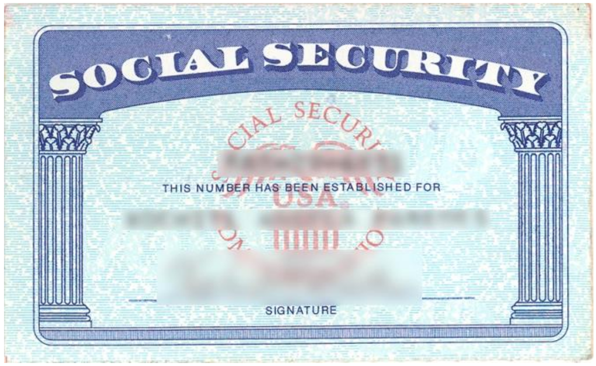
- What is identity theft?
  - Identity theft occurs when someone uses your **personal information** without your permission to obtain something of value
- How often does it happen?

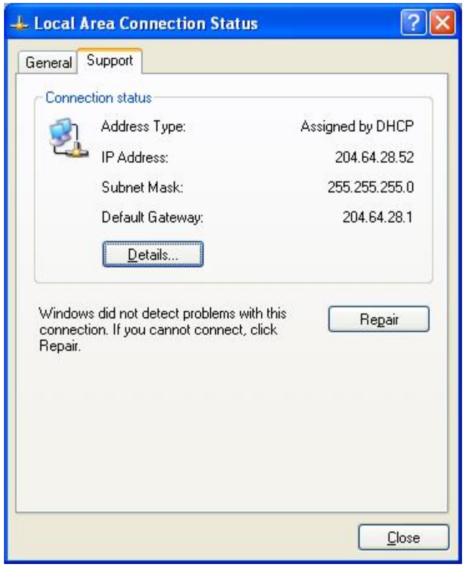
Identity Theft Complaints

Rank	Victim State	Complaints Per 100,000 Population[1]	Complaints
1	Florida	361.3	69,795
2	Georgia	193.9	19,232
3	California	122.7	46,658
4	Michigan	122.2	12,075
5	New York	110.1	21,538
6	Nevada	109.9	3,032
7	Texas	108.6	28,299

Source – *Consumer Sentinel Data Book for January – December 2012*.
Federal Trade Commission, February 2013.
Available at: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf

Types of Personal Information





How is Stolen Personal Information Used? (Slide 1 of 3)

Identity Theft Complaints Count from Texas Victims = 25,843

Identity Theft Types Reported by Texas Victims

Rank	Identity Theft Type	Complaints	Percentage[1]
1	Government Documents or Benefits Fraud	9,422	36%
2	Credit Card Fraud	3,880	15%
3	Phone or Utilities Fraud	2,952	11%
4	Loan Fraud	2,166	8%
5	Employment-Related Fraud	2,071	8%
6	Bank Fraud	2,012	8%
	Other	5,340	21%
	Attempted Identity Theft	1,069	4%

[1]Percentages are based on the 25,843 victims reporting from Texas. Note that CSN identity theft complaints may be coded under multiple theft types.

Source – *Consumer Sentinel Network Data Book for January – December 2014*.
Federal Trade Commission, February 2015.

Available at: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2014

How is Stolen Personal Information Used? (Slide 2 of 3)

- Credit card and account fraud
  - New account fraud
  - Existing account fraud
- Empty your bank accounts
- Get a job
- Apply for IDs (driver’s license, passport, etc.)
- File bankruptcy

How is Stolen Personal Information Used? (Slide 3 of 3)

- Obtain or use medical insurance
- Buy a car
- Apply for government benefits
- Enroll in school and obtain student loans
- File income tax returns
- Get arrested

Protecting Your Identity

- The best way to protect your identity is to **be alert** and **consistently** safeguard your information.

Who Steals Identities?

- Domestic and international criminals
  - Opportunistic people
  - Drug users
  - Organized black market distributors of information
- Acquaintances
- Family
- Neighbors

Dumpster Diving

Stealing Mail

Theft


ARTICLE
WHERE THIS ARTICLE WAS FOUND
INVESTIGATING OFFICER
EXHIBIT NO.
DATE
EVIDENCE
Office of the
Attorney
General
Austin

Internet, Phishing and Data Breaches

- Internet
- Phishing
- Data breaches

Well-Placed Employee

Skimmers

Automated Teller Machines

Pretexting

Relaxed Security: Assuming Your Information Is Safe

Identity Theft and Business Responsibilities

- Many businesses store and use our personal information.

- State and federal laws require most businesses to safeguard personal information and to properly dispose of it by destruction so that it is unreadable or undecipherable.

- **With some exceptions**, if your personal information is compromised by a breach, the business must notify you.
  - Subscription to credit monitoring service may be offered.
  - <u>**Do not**</u> provide personal information in response to a breach notice.

Safeguard Your Personal Information

Three-Pronged Approach

- Limit exposure
- Remain vigilant
- Be wary

Limit Exposure (Slide 1 of 3)

- Store your Social Security card somewhere safe.
  - **Do not** carry it in your wallet.
- Don’t leave personal information in the open, even at home.
- Don’t share your personal information—unless **you** initiated the contact.
- Shred all documents containing personal information with a **cross-cut shredder** before disposing of them.

Limit Exposure
(Slide 2 of 3)

- Only carry with you credit cards you intend to use.

- Only use one credit card for online purchases.
  - **Do not** use a debit card.

- Be careful with your credit card receipts.
  - If your receipt shows more than the last four digits, report it to the Office of the Attorney General.

Limit Exposure
(Slide 3 of 3)

“Opt Out”

- The Direct Marketing Association
  - www.dmachoice.org
- The Network Advertising Initiative
  - www.networkadvertising.org
- No Call List
  - www.donotcall.gov
- Pre-screened and pre-approved credit and insurance offers
  - www.optoutprescreen.com

Limit Exposure: Online Safety (Slide 1 of 2)

- Use a non-administrator account as your main user profile.
- Use anti-virus, spyware and malware protection.
- Update web browsers.
- Update operating system.

Limit Exposure: Online Safety (Slide 2 of 2)

- Anti-phishing toolbars
- Wireless safety
- Use secure websites
- Use strong passwords

Limit Exposure

- Fraud alert?
- Security freeze?

Remain Vigilant

- Monitor your credit report.
  - www.annualcreditreport.com
- Reconcile checking and credit card accounts each month.
- Know when bills and financial statements normally arrive each month.
- Use a secure mailbox.
- Take note of email messages informing you that you've changed your password or anything related to your account.

Be Wary
(Slide 1 of 2)

These Tips Apply Online and Offline.

- Ask if it is necessary to use your Social Security number and why.
- Ask what information is collected, who has access to it and why.
- Ask what protective measures are in place to protect your information and ask for and review a copy of their privacy policy.

Be Wary
(Slide 2 of 2)

- Review your IRS and Social Security accounts for accuracy.
- Check to see if your minor children have a credit report.
- Help seniors check credit reports.

Identity Theft Recovery (Slide 1 of 3)

- Identity theft happens.
- You or someone you care about may become a victim of some form of identity theft.
- Reacting quickly and appropriately can save you time, money and frustration.

Identity Theft Recovery (Slide 2 of 3)

- The Identity Theft Victim’s Kit can be found on the Office of the Attorney General identity theft website.

www.TexasFightsIDTheft.gov

- The victim’s kit will help guide you through the recovery process.

Identity Theft Recovery
(Slide 3 of 3)

1. Obtain a fraud alert or security freeze on your credit report.
2. Contact creditors and close affected accounts.
3. File a report with the police.
4. File a complaint with the FTC.

Thank You!

Ian Howe
Assistant Attorney General
Ian.howe@texasattorneygeneral.gov
(512) 936-2234