

# Part III: Identity Theft

- *The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.*
- Approximately 15 Million people a year will be affected by Identity Theft, with losses over 40 Billion Dollars
  - -Basically 7% of citizens will be victims
  - -Average loss of \$3,500 per person
- We all place our identities at risk on a daily basis
  - -Bank Accounts
  - -Credit Card Accounts
  - -Retail store breaches
  - -Mail Fraud
  - -Telemarketing Scams
  - -Medical Records

# Medical Info Theft

- Thieves can steal your identity and use it for medical insurance claims, pretending to be YOU!
- -This can place improper information in your medical files, leading to wrong treatment
- -False Medical Bills / Claims
- -Denial of Claims and Insurance
- -Creating false patient records
- -More “out of pocket” expenses that YOU will be held responsible for
- Always check your “Explanation of Benefits” (EOB) whenever received
- Any discrepancies, immediately follow up with physician and insurance company

# Social Security Theft



- With a stolen Social Security number, an identity thief can:
  - Assume your identity
  - Use YOUR number and create a different name and biological information in a combination, thus creating a completely new identity
- Social Security Cards have little to no modern security features, making false duplication easy!

# IRS / False Tax Return

- Tax Return
  - -Very active and prevalent activity today
  - -The thief utilizes your identity to file a tax return
  - -You will then be unable to file a return
  - -The thief has obtained your identity and USES IT!



# How do they get our information?

- Intercepting mail and documents
- Data Breaches
- Recording computer activity (Taking over PC)
- ATM Skimming Device / Keypad Camera
- Fraudulent forms and phone calls
- Tax Forms
- Medical Bills / Claims
- Bank Records
- Thieves obtaining your info when paying for items
- Shared contact lists, suspects trade information
- FROM YOU!



# ID Theft Protection

- Pay close attention and check you Credit Report
- -Always sign credit / debit cards
- -Make Safe Passwords (no birthdates, pet's name, spouse name)
- -Always report lost or stolen credit cards....Immediately
- -Shred any and all documents that have personal info
- Pay attention to mail delivery and sending mail
  - -Thieves will steal both incoming and outgoing mail
  - -Use post office boxes and suspend mail when away
  - -Some accounts can be paid online, when secure and trusted
- Keep personal documents locked in your home or use safety deposit boxes
  - -Always be aware of whose in your home (visitors)



# If you're a victim....

- **Notify any bank, credit card etc. that was compromised**
  - -Close these accounts immediately
  - -Have new cards issued
  - -Begin Fraud Process with company
- **Make a police report!**
  - -NCIC ID Theft Victim Entry (optional)
  - -Most financial institutions will want a report
  - -Keep records of everyone you speak to with time and dates
- **Notify the major credit bureaus:**
  - -Experian
  - -Equifax
  - -Transunion

# Reporting

- Equifax: 1-800-525-6285
- Experian: 1-888-397-3742
- TransUnion: 1-800-680-7289
- Internet based scams report to IC3.gov (FBI)



# Questions / Comments

Credit to:

- [FBI.gov](https://www.fbi.gov)
- [BBB.gov](https://www.bbb.org)
- [FTC.gov](https://www.ftc.gov)
- [IRS.gov](https://www.irs.gov)