IDENTITY THEFT AND FRAUD

PRESENTED BY: NANCY HARVEY

THRIVENT CAMPUS RELATIONS

What Is Identity Theft?

- Fraudulent access and use of a person's private identifying information for financial gain

- Steal a persons name, credit card number, social security number or drivers license number
  - It can cost you time and money
  - It can destroy your credit and ruin your good name

- One of the fastest growing crimes in America according to the FBI, Department of Justice and Federal Trade Commission

Identity Theft in the Spotlight

- 60 million Americans have been affected by identity theft according to a 2018 survey - Javelin Strategy & Research since 2012

- Most Notable Data Breaches to date:
  - Yahoo – 3 Billion consumers affected (2013)
  - Marriott (Starwood Hotels) – 500 Million consumers affected (2018)
  - Equifax – 143 million consumers affected (2017)
  - Target – 110 million consumers affected (2013)
  - Anthem – 78.8. millon consumers affected (2015)

- People between the ages of 18-24 have the highest rates of ID theft

- Up to 18% of victims take 4 years or longer to discover they are a victim of Identity Theft
- It takes the average victim an estimated $500 and 30 hours to resolve each identity theft crime

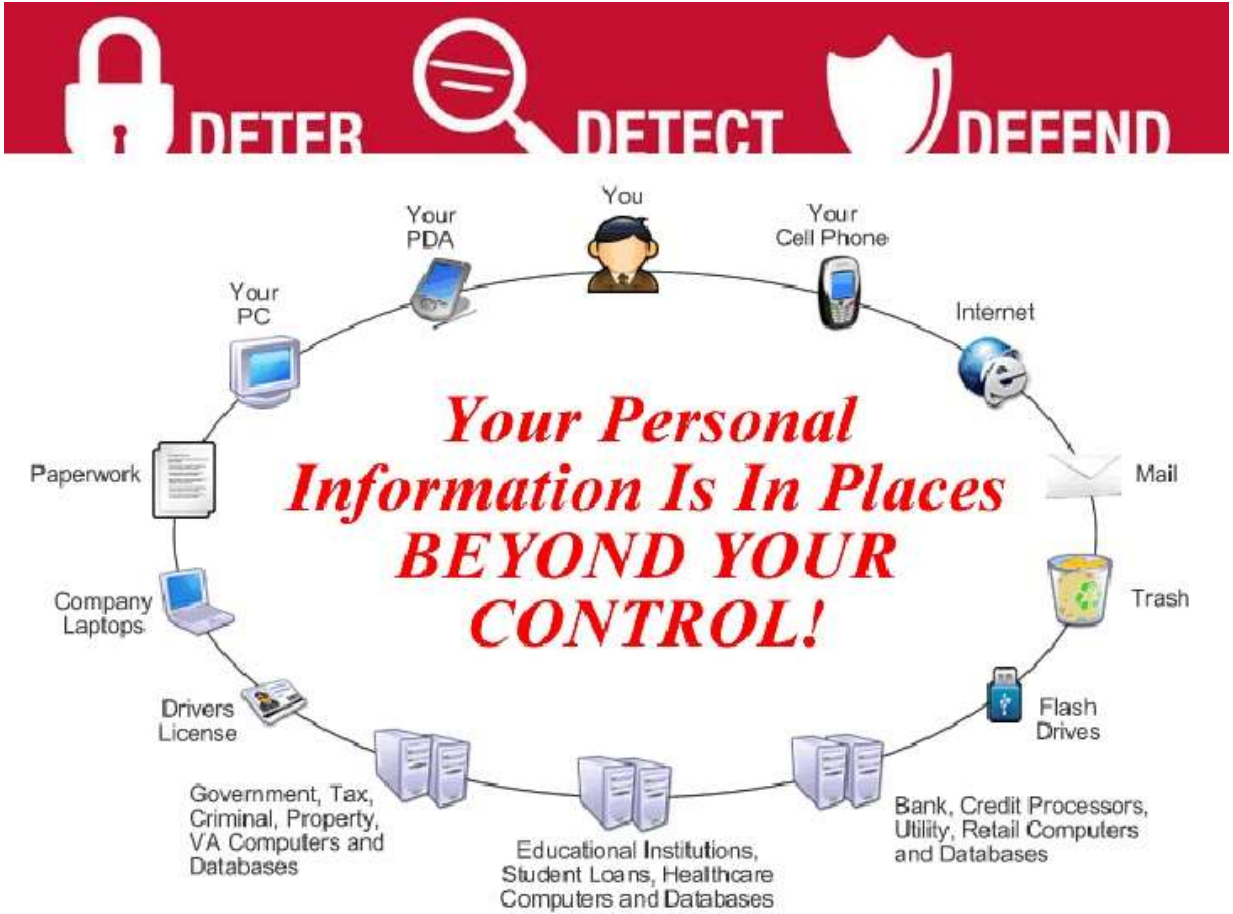
- Studies have shown that the ones stealing your identity are often the ones closest to you – friends, family, neighbors, co-workers, etc.

Major Areas of Identity Theft

- Social Security
  - Most Valuable Piece of Information a Thief can Steal
  - Kids/Teenagers are often targeted
  - Crimes can easily be committed in your name if your SSN is stolen
- Financial
  - When someone gains access to your credit cards, bank accounts, financial holdings, etc
  - Crime typically committed online after access has been gained
- Medical
  - Utilize victim's insurance to make false claims
  - Most difficult to fix

Major Areas of Identity Theft

- Driver's License
  - Stolen Driver's License contains name, address, DOB as well as state ID number
  - Information used to apply for credit cards, loans and even open bank accounts to obtain checking accounts
  - Arguably easiest form to commit
- Character/Criminal
  - ID Thieves commit crimes posing as you!
  - Difficult to convince local police and court you are really the victim and innocent of the crimes committed in your name
- Social
  - Someone uses your name/phots to create fake social media account


DETER
DETECT
DEFEND
You
Your PDA
Your Cell Phone
Your PC
Internet
Your Personal Information Is In Places BEYOND YOUR CONTROL!
Paperwork
Mail
Company Laptops
Trash
Drivers License
Flash Drives
Government, Tax, Criminal, Property, VA Computers and Databases
Educational Institutions, Student Loans, Healthcare Computers and Databases
Bank, Credit Processors, Utility, Retail Computers and Databases

Common Ways of Stealing your Identity/Information

Low-Tech Methods

- Identity Theft in your Mailbox
  - Contains your address, possibly SSN, account numbers and other personal identifying information
  - Highest risk away from the internet
  - File change of address in your name and divert mail to gather info/data
  - Drop off your mail at the post office NOT your mailbox
- Dumpster Diving
  - Digging through garbage cans or communal dumpsters in search of cancelled checks, credit card pre-approval offers, bank statements, medicine bottles, etc
- Phone/Email Scams
  - Do not give out personal information over the phone
  - Don't let someone repeat your credit card number over the phone
  - Reputable financial organizations will NOT contact you by eMail to discuss financial matters
  - Phishing emails that look like reputable companies

Common Ways of Stealing your Identity/Information

Low-Tech Methods

- Skimming Devices
  - Found on ATMs, Cash Registers, Gas Station Credit Card Readers, etc
  - Readily available to purchase via the Internet
- Shoulder Surfing
  - Thieves take video of you punching in your information (PIN) at registers, ATMs – commonly done via cell phone
- Job Recruitment Scams
  - Receive emails/solicitation calls for possible jobs
  - Especially prey on the unemployed

Common Ways of Stealing your Identity/Information

High Tech Methods

- Unsecured Websites/Wireless Hacking
  - HTTPS vs. HTTP
  - Security Logos
  - Do not conduct financial or other personal transactions over public WiFi
  - UPDATE HOME NETWORK PASSWORD!
- Internet Cookies
  - Never leave information (cookies) in your browser at work or public computers
- Key Logging Malware
  - Software secretly records every keystroke you make – usernames, passwords, or SSNs
  - Typically a virus or worm from a website or download
- Database Security Breaches
  - Examples: Target, Yahoo, Equifax

How Profitable is Identity Theft?

Example “Pay Days” for ID Theft Criminals

$7: Pay Pal Account Log-On and Password

$12: Hotmail addresses with password

$25: Credit Card Number with Security Code and Exp Date

$100: Social Security Card

$150: Birth Certificate

$150: Driver’s License

$200: 1,000 Gmail addresses with password

$500: Credit Card with Pin

$600 - $1,300: Health Insurance Card/Information

Preventing Identity Theft

Protecting Your Personal Information

- Never Give out Information Unsolicited
- Leave your Social Security Card at Home
- Store Documents in a Safe Place
- Shred Documents and Mail with Cross-Cut Shredder
- Don’t Use Obvious Passwords
- Order Your Credit Report and Monitor Often
- Remove your name from 3 Credit Bureaus to reduce pre-approved credit offers
- Do Not leave mail with personal information in your mailbox
- Keep your SSN off Medical Questionnaires
- Cancel unused credit card accounts

Preventing Identity Theft

Secure Your Computer

- Make Sure Operating System Security Patches are Up To Date
- Use Anti-Virus Software and Firewall
  - Update your virus definitions
- Make Sure Your Network is Secured
  - Wireless security settings

Preventing Identity Theft

Stop the Junk Mail!!!

- Opt out of Junk Mail
  - www.optoutprescreen.com or 1-888-567-8688

- Reduce Telemarketing Calls
  - https://www.donotcall.gov
    - Register Phone Number(s) – up to 3
    - Verify the information
    - File Complaint

Preventing Identity Theft

Detect suspicious activity by routinely monitoring your personal and financial information

- Be Alert
  - Mail or bills that do not arrive
  - Denials of credit for no reason
- Inspect Your Credit Report
  - Allowed one free report from each Credit Bureau a year
    - www.AnnualCreditReport.com or 1-877-322-8228
- Inspect Your Financial Statements
  - Look for charges you did not make

Preventing Against Identity Theft in College

"Universities are, by nature, open trusting environments……"

\- Alan Woodward (Cyper Security Specialist)

- Social Media Dangers
  - Students Often over-share personal details on Social Media
    - Example: Date of Birth on Social Media
- Students are very trusting/inexperienced
  - Easy "prey" for scam artists
  - Avoid saving passwords/PIN on cell phones, computers
    - Laptops, IPADS and phones stolen all the time
- Ensure college/university follows FERPA guidelines and protects databases
- Computer Security Protection
  - Too caught up in activities/studying
  - Need to learn to vary passwords

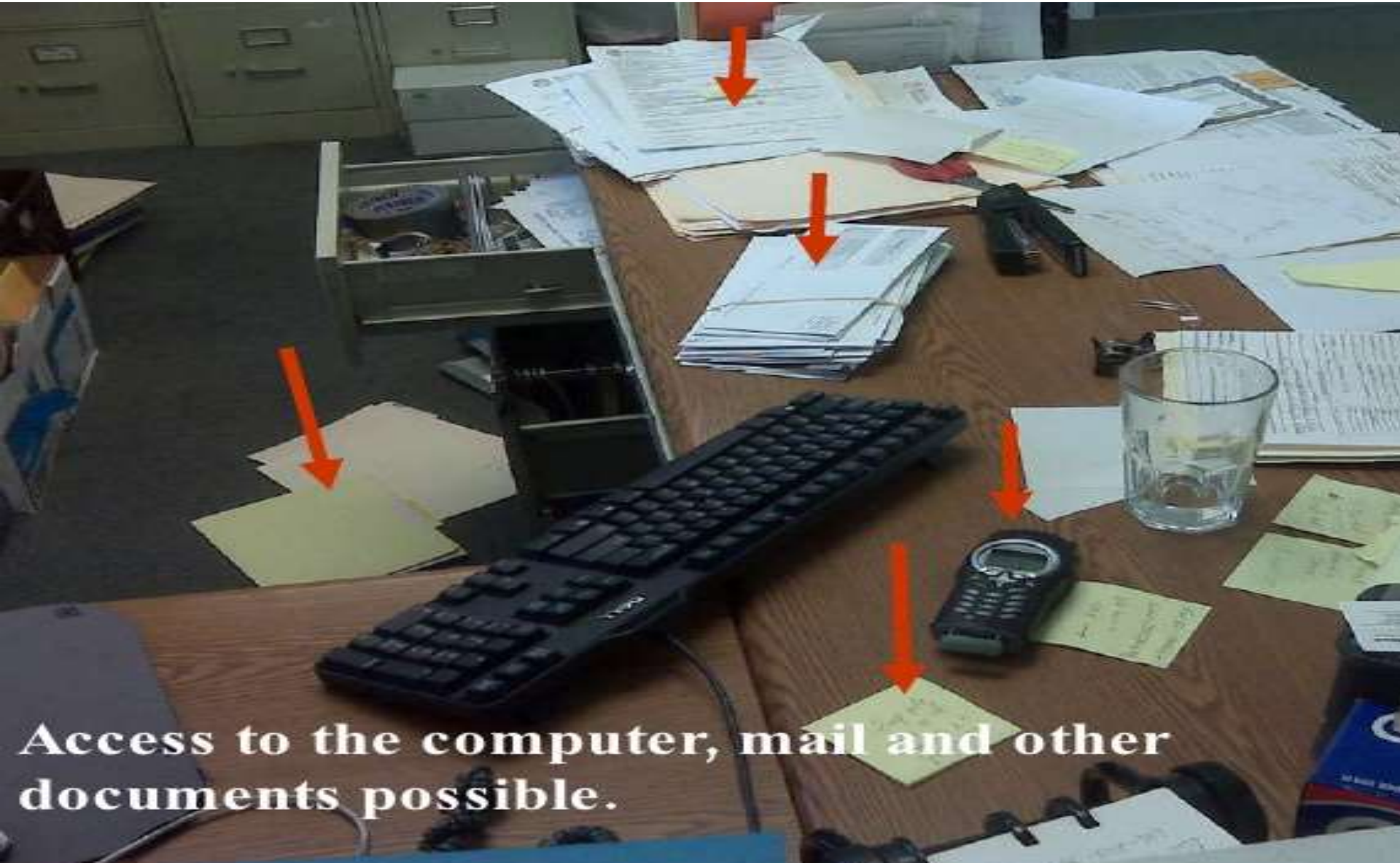
Preventing Against Identity Theft in College

Identity Theft

A recent national survey of college students found that: Almost half of all college students receive credit card applications on a daily or weekly basis Many of these students throw out card applications without destroying them

- Nearly a third of students rarely, if ever, reconcile their credit card and checking account balances
- Almost 50 percent of students have had grades posted by Social Security number

- **►18 to 24 year olds are at the greatest risk for identity theft** Although occurrence of identity theft are lower, the damage can be greater because they are less aware of what to look for and how to recognize that their identity has been stolen


Access to the computer, mail and other documents possible.

Preventing Against Identity Theft in College

- Majority of Identity Theft at a College/University Occurs the "old fashioned way" - Theft!
  - Lock-up Valuables when leave dorm rooms
  - Be careful/mindful when running up a Tab at the bar
  - Keep SSN cards and birth certificates at home with parents
- SCAMS
  - Scholarship Scams – providing personal information, fees
  - Student Loan Assistance Companies
  - Housing Scams
- Applying for Jobs
  - Only provide SSN to employer when hired
  - Deliver applications to hiring Mgr or HR
  - If submit application online, make sure its secure

What to Do if You're a Victim of Identity Theft?

- Contact your Financial Institution
- Close the Account
- Place a FRAUD ALERT on your credit reports
  - Equifax: 1-800-525-6285
  - Experian: 1-888-EXPERIAN
  - TransUnion: 1-800-680-7289
- File a Police Report
- File a complaint with Attorney General's Office
- Contact the Federal Trade Commission

Online Resources

- Federal Trade Commission:
  - www.ftc.gov
- Department of Justice:
  - https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
- Better Business Bureau:
  - www.bbb.org
- National Criminal Justice Reference Service:
  - www.ncjrs.gov

Non-Profit organizations committed to promoting prevention and recovery from Identity Theft

- https://www.idtheftcenter.org/knowledge-base/
- www.identitytheft.org
- www.privacyrights.org/identity.htm

Sources

- U.S. Dept of Justice – www.justice.gov
- Federal Trade Commission & ABC News Report
- ABC News Report & More From USA.Gov: Small Businesses: Prepare to Be Breached!
- ABC News May 24, 2015 Report & USA.Gov
- Randall Chesnutt - Institute of Fraud Risk Management
- Sources: USA Today, October 2006
- Yahoo Finance 2014 – The Exchange
- Credit Source
- Washington State Department of Financial Institutions
- *Student Monitor and ed.gov Statistics*
- "How to Protect against Identity Theft in College" – Menachem Wecker

QUESTIONS?