Identity Theft

Identity theft and ***fraud*** 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. It occurs when someone gains access to a person's basic information, including name, address, credit card or social security number, and uses that information. Identity theft and fraud affects millions of new victims each year.

How does ID theft happen?

- ✓ Stolen wallets, purses, computers, cell phones
- ✓ Stolen or diverted mail
- ✓ "Dumpster Diving"
- ✓ Stealing records from an employer
- ✓ From the internet
- ✓ Skimming credit cards
- ✓ Scams

Common Scams

- **Phishing:** Someone claiming to be from a company or government agency with a problem that you need to take card of right now. Creates a sense of urgency, hoping to get you will give them your information.
- **Grandparent**: Someone claiming to be a relative with an emergency, needing money RIGHT NOW! You can help by wiring them money. But don't tell mom and dad….
- **Overpayment**: Someone is interested in buying what you are selling. They issue you a check. Oops! The check was made out for too much. You keep the check and simply send a portion back to them with the item they bought.
- **Nigerian Letter:** Someone claiming to have millions of dollars and they just happen to need your help getting money out of another country.
- **Lottery:** You won a lottery or sweepstakes and you just need to pay some fees to claim your prize.
- **Charity**: False charities are often created after large tragedies.

Preventing Scams

- **NEVER** provide personal information (social security number, credit card or bank account numbers, date of birth, etc.) unless *you initiate the contact and are familiar or acquainted with the business!*
  - Don't click on links or open attachments in these emails.
  - Use only official contact channels.
- Make all efforts to verify a story before sending money.
  - Check with relatives, research charities, ask for second opinions.
  - A good rule of thumb is *if someone asks you to wire money, it is a scam.*
- You cannot win a lottery, sweepstakes, or drawing you never entered.
  - It is illegal to enter foreign lotteries.
  - You do not have to pay for a prize upfront.
- Never accept a check and agree to return the difference.
- No one would ask you to help them move millions of dollars…especially a total stranger.
- ***IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS!***

Preventing ID theft by Reducing Access to Your Personal Data

- Minimize the number of credit cards you carry in your wallet or purse.
- Don't carry PINs or social security cards in your wallet or purse.
- Shred pre-approved credit offers and personal information before you throw away.
- When creating passwords and PINs, do **not** use digits of your social security number, birth dates, names, or anything that can be easily guessed.
- Review your bills and bank statements to ensure that no fraudulent activity has taken place.
- Store your checks in a safe place.
- Obtain a copy of your credit report at least once a year to check for errors.
- Beware of "Shoulder Surfers", who can obtain your PIN and access your bank accounts.
- Do not mail bills from your home mailbox. Use a U.S. Post Office mailbox instead.
- Remove your name from credit bureau marketing lists. **Opt Out** by calling **1-888-567-8688.**
- Remove yourself from national **telemarketing** lists. Call the **National "Do Not Call List" (1-888-382-1222)** from the phone number you want removed. In addition, you can tell telemarketers who call you to put you on *their* "Do Not Call" list.

Protection on the Computer

- Maintain current virus protection software and use a firewall.
- Verify browsers are secure for financial transactions.
- Avoid automatic log-in features.
- Delete any personal info before disposing of your computer.
- Don't respond to unsolicited emails or requests for personal or financial information. Most legitimate companies will *not* initiate contact for this information via email.

If You are a Victim of ID Theft…

- Contact one of the 3 major credit bureaus to place a fraud alert in your file:

Experian	**Equifax**	**TransUnion**
888-397-3742	Fraud:888-766-0008	Fraud:800-680-7289
www.experian.com	www.equifax.com	www.transunion.com

- Contact all financial institutions with whom your name has been used fraudulently–by phone and in writing. Close affected accounts. Obtain **new** account numbers.
- Keep detailed information and copies of all correspondence related to identity theft.
- Carefully monitor accounts for evidence of new fraudulent activity. Report immediately.
- File a report with your local police department.
- File a complaint with FTC, if needed. (1-877-IDTHEFT or www.consumer.gov/idtheft)

***Information you need to know…*Fair and Accurate Credit Transactions Act (FACTA) states:**

- **Consumers can get free credit reports from EACH of the credit bureaus once a year.**
- **ID theft victims need only notify one of the 3 credit bureaus. A 90-day fraud alert must then accompany all credit reports issued by any of them. Victims can extend alerts for 7 years by providing a police report.**
- **Businesses where fraudulent accounts were opened have to give the victim account information to help clear their name. They must accept reports by the victim or the credit bureau.**

Resources

Federal Trade Commission (ID Theft): www.consumer.gov/idtheft or 1-877-IDTHEFT (1-877-438-4338)
US Postal Inspections (Mail Theft): www.usps.gov/websites/depart/inspect
US State Department (Passport Fraud): www.travel.state.gov/passport.passport_1738.html
Social Security Administration (To report misuse): www.socialsecurity.gov/oig
Social Security Administration (To verify earnings): 1-800-772-1213
IRS (Tax Fraud): www.treas.gov/irs/ci