ABOUT IDENTITY THEFT

WHAT IS IDENTITY THEFT?

Identity Theft is a term used to 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.

WHAT ARE TYPICAL WAYS THAT IDENTITY THEFT CAN HAPPEN TO YOU?

- In public places, for example, criminals may engage in ***shoulder surfing*** (watching you from a nearby location as you punch in your telephone calling card number or credit card number) or listen in on your conversation if you give your credit card number over the telephone.

- If you receive applications for ***pre-approved*** credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.

- Many people respond to ***spam*** (unsolicited email) that promises them some benefit but requests identifying data, without realizing that in many cases the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to steal large amounts of personal data.

- With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes. For example:

  - False applications for loans and credit cards.
  - Fraudulent withdrawals from bank accounts.
  - Fraudulent use of telephone calling cards or online accounts, or
  - Obtaining other goods or privileges which the criminal might be denied if he were to use his real name.

WHAT CAN YOU DO IF YOU'VE BECOME A VICTIM OFIDENTITY THEFT?

- If someone is using your personal or financial information to make purchases, receive benefits, file taxes, or commit fraud, that's ***Identity Theft***. This book will guide you through the recovery process.

- If you're dealing with ***Tax Identity Theft***, ***Medical Identity Theft***, or ***Child Identity Theft***, read the chapter entitled **SPECIAL FORMS OF IDENTITY THEFT**. If you

have had personal or financial information lost or stolen, refer to the chapter entitled **DATA BREACHES AND LOST OR STOLEN INFORMATION**.

WHAT TO DO RIGHT AWAY

STEP 1: CALL THE COMPANIES WHERE YOU KNOW FRAUD OCCURRED

- Call the fraud department. Explain that someone stole your identity.
- Ask them to close or freeze your accounts. After your account is frozen, nobody can add new charges unless you agree.
- Change logins, passwords, and PINs for your accounts.
- You might have to contact these companies again after you have an ***Identity Theft Report***.

STEP 2: PLACE AFRAUD ALERT AND OBTAIN YOUR CREDIT REPORTS

- To place a ***Fraud Alert***, contact one of the three credit bureaus. The credit bureau you select must inform the other two credit bureaus.

  Experian.com/fraudalert
  1-888-397-3742

  TransUnion.com/fraud
  1-800-680-7289

  Equifax.com/CreditReportAssistance
  1-888-766-0008

- A ***Fraud Alert*** is free. It will make it difficult for another entity to open new accounts in your name.
- You'll receive a letter from each credit bureau confirming that they have placed a ***Fraud Alert*** on your file.
- Get your free ***Credit Report*** from **Equifax**, **Experian**, and **TransUnion**. Go to ***annualcreditreport.com*** or call 1-877-322-8228.

Have you already ordered your free annual ***Credit Reports*** this year? If so, you can pay to receive your reports immediately or you can follow the instructions in the