Important Contact Information

Tips For Preventing Identity Theft

El Paso County Sheriff's Office

Non-Emergency Dispatch: 719-390-5555 *For emergencies, dial 911*

To File a Complaint with the FTC or For More Information on Identity Theft:

Call: 1-877-IDTHEFT (1-877-438-4338) TDD Line: 1-202-326-2502

Or visit: ftc.gov/idtheft

Or write to: Identity Theft Clearinghouse Federal Trade Commission 600 Pennsylvania Avenue, NW Washington, DC 20580

Reporting Fraud to Credit Bureaus:

- Equifax: 1-800-525-6285, PO Box 740250, Atlanta, GA 30374-0250
- Experian: 1-888-EXPERIAN (397-3742), PO Box 9532, Allen, TX 75013
- TransUnion: 1-800-680-7289, Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790

Reporting Stolen or Forged Checks to Verification Companies:

- TeleCheck: 1-800-710-9898 or 1-800-927-0188
- Certegy, Inc.: 1-800-437-5120
- International Check Services: 1-800-631-9565

Protect personal information that could be used illegally to steal your identity: this includes your name, Social Security Number, date and place of birth, bank or credit card account numbers, driver's license number, passwords, etc.

- Don't give out personal information over the phone, internet or through the mail unless you
 initiated the contact. Be sure that the person or company you're giving it to is trustworthy.
- Don't mail bills, credit card applications or any other potentially sensitive information from an unsecured mailbox. Only use secure US Postal Service mail receptacles or take your mail directly to the Post Office.
- Don't throw away mail or other documents containing personal information. Shred these items first.
- If someone contacts you to update or "verify" your personal or banking records, don't
 provide any information. Instead, call the customer service number from your statement or
 bill and verify the employee's identity and purpose.
- Keep track of your driver's license, credit cards, checks and any other personal information.
 Don't leave these items easily accessible to others, even in your home.
- Occasionally change passwords and PIN numbers on your accounts. Avoid using easy to
 guess passwords, such as your mother's maiden name, your date of birth, a pet's name or
 consecutive numbers.
- Visit: <u>www.annualcreditreport.com</u> to request a free copy of your credit report from each of the three major credit reporting agencies.



What to Do If You Become a Victim of I DENTITY THEFT

1. File a report with the law enforcement agency in the community where the identity theft took place.

Try to obtain a copy of the case report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number.

2. Place a fraud alert on your credit reports and review them carefully.

Call the toll-free fraud number of any one of the three major credit bureaus (see reverse) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as one credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and a copy of all three reports will be sent to you free of charge.

Once you receive your reports, review them carefully for inquiries you didn't initiate, accounts you didn't open, and unexplained debts on your true accounts. Where "inquiries" appear from the companies that opened the fraudulent account(s), request that these "inquiries" be removed from your report. Check that information such as your SSN, address(es), name or initial, and employers are correct. Inaccuracies in this information may be due to typographical errors, however, whether the inaccuracies are due to fraud or error, notify the credit bureau as soon as possible by telephone and in writing. Continue to check your reports periodically, especially in the first year after you've discovered the theft, to make sure no new fraudulent activity has occurred.

3. Close any accounts that have been tampered with or opened fraudulently.

Credit accounts include all accounts with banks, credit card companies and other lenders, and phone companies, utilities, ISPs, and other service providers. If the company doesn't accept the FTC's ID Theft Affidavit (available online at www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf), ask the representative to send you the company's fraud dispute forms. If any of your ATM/Credit/Debit cards have been lost, stolen or otherwise compromised, cancel the cards as soon as you can and get new cards. If you're closing existing accounts and opening new ones, use new Personal Identification Numbers (PINs) and passwords. If your checks have been stolen or misused, close the account as soon as possible and ask your bank to notify the appropriate check verification service.

Note: No federal law limits your losses if someone steals your checks and forges your signature, but state laws may protect you. While most states hold the bank responsible for losses from a forged check, they also require you to take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely way that a check was lost or stolen. Contact your state banking or consumer protection agency for more information. Contact the three major check verification companies (see reverse) to request that retailers who use their databases not accept your checks. Also call SCAN (1-800-262-7771) to find out if the identity thief has been passing bad checks in your name.

4. File a complaint with the Federal Trade Commission.

The FTC enters the information you provide into a secure database. This will provide important information that can help law enforcement officials track down identity thieves and stop them. The FTC also can refer victim complaints to other appropriate government agencies and companies for further action. Visit the website: www.consumer.gov/idtheft to file a complaint or for information on the FTC's Privacy policy.