CBI Identity Theft Unit

If Your Cards Are Lost or Stolen

- If your credit or charge cards are lost or stolen, call the issuer(s) immediately. Most card companies have a toll-free number for reporting missing cards. Some companies provide 24-hour service. By law, once you report the loss or theft, you have no further liability for unauthorized charges. In any event, your maximum liability under federal law is $50.

- Notify credit bureaus and establish fraud alerts. Immediately report the situation to the fraud department of the three credit reporting companies -- Experian, Equifax, and TransUnion. When you notify one bureau that you are at risk of being a victim of identity theft, it will notify the other two for you. Placing the fraud alert means that your file will be flagged and creditors are required to call you before extending credit. Consider using a cell phone number if you have one.

- If you choose to call Experian you will be subject to a marketing pitch for their "free" credit management tools. If you fail to cancel the service within 30 days, your credit card will automatically be charged for the service.
- Under new provisions of the Fair Credit Reporting Act (FCRA, §605A) you can place an initial fraud alert for only 90 days. The credit bureaus will each mail you a notice of your rights as an identity theft victim. Once you receive them, contact each of the three bureaus immediately to request two things:

    - a free copy of your credit report
    - an extension of the fraud alert to seven years

- You may request that only the last four digits of your Social Security number (SSN) appear on the credit report.

- You must have evidence of attempts to open fraudulent accounts and an identity theft report (police report) to establish the seven-year alert. You may cancel the fraud alerts at any time.
- In all communications with the credit bureaus, you will want to refer to the unique number assigned to your credit report and use certified, return receipt mail. Be sure to save all credit reports as part of your fraud documentation file.

- Once you have received your three credit reports, examine each one carefully. Report fraudulent accounts and erroneous information in writing to both the credit bureaus and the credit issuers following the instructions provided with the credit reports. The FTC's identity theft guide provides a sample letter to send to the credit bureaus requesting that fraudulent accounts be blocked.
  www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#Resolving (scroll down to find letter)

- Once you notify the credit bureaus about the fraudulent accounts, the bureau is required to block that information from future reports. The bureau must also notify the credit grantor of the fraudulent account. (FCRA, §605B) Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened if this information is not included on the credit report.

- In addition, instruct the credit bureaus in writing to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months to alert them to the disputed and erroneous information (two years for employers).

- Monitor your credit reports. Be aware that these measures may not entirely prevent new fraudulent accounts from being opened by the imposter. Credit issuers do not always pay attention to fraud alerts, even though the law now requires it. That is why we recommend that you check your credit reports again in a few months.

- The federal FACTA law enables you to receive a free credit report per year from each of the three credit bureaus. (FCRA §612) This is over and above the free reports you can order when you place fraud alerts on your three credit reports. Once you have received your free credit reports as a part of the fraud-alert process, follow up in a few months by taking advantage of your free FACTA copy. We recommend that you order your free credit reports by phone rather than using the online system. Call (877) 322-8228. For more on free credit reports, see www.ftc.gov/bcp/conline/pubs/credit/freereports.htm and www.annualcreditreport.com.

- Laws in several states give individuals additional opportunities to obtain free credit reports. For confirmed identity theft victims who live in California, you can get one free report each month for the first 12 months upon request. (California Civil Code 1785.15.3) And in seven states, whether a victim or not, you can receive one free credit report each year under state law, over and above the free FACTA report you can receive yearly under federal law. These states are: Colorado, Georgia (2 per year), Maine, Maryland, Massachusetts, New Jersey, and Vermont.

- As of November 2007, individuals nationwide are able to "freeze" their credit reports with Equifax, Experian, and TransUnion. By freezing your credit reports, you can prevent credit issuers from accessing your credit files except when you give permission. This effectively prevents thieves from opening up new credit card and loan accounts. In most states, security freezes are available at no charge to identity theft victims and for a relatively small fee for non-victims.
    - For state-by-state information on security freezes, visit this Consumers Union
- webpage: www.consumersunion.org/campaigns//learn_more/003484indiv.html
    - The California Office of Privacy Protection provides a guide on security freezes for
- Californians, www.privacy.ca.gov/sheets/cis10securityfreeze.pdf.

- If your identity thief is aggressive and gives no indication of ceasing to use your identity to obtain credit, consider using the security freeze to reduce access to your credit file. The security freeze is free to victims of identity theft in most states. Non-victims who wish to activate the security freeze for prevention must pay a fee in most states. Some states make the security freeze available only to identity theft victims.

- Law enforcement. Report the crime to your local police or sheriff's department right away. You might also need to report it to police department(s) where the crime occurred if it's somewhere other than where you live. Give them as much documented evidence as possible. Make sure the police report lists the fraudulent accounts. Get a copy of the report, which is called an "identity theft report" under the FCRA. Keep the phone number of your investigator handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime.

- FTC regulations define an "identity theft report" to include a report made to a local, state, or federal law enforcement agency. If your local police department refuses to file a report and your situation involves fraudulent use of the U.S. mail, you can obtain an identity theft report from the U.S. Postal Inspector. If your case involves fraudulent use of a driver's license in your name, you might be able to obtain a report from your state's Department of Motor Vehicles. The FTC has more information on identity theft reports at www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#Identity

- Federal Trade Commission. Report the crime to the FTC. Include your police report number. Although the FTC does not itself investigate identity theft cases, they share such information with investigators nationwide who are fighting identity theft.
    - Call the FTC's Identity Theft Hotline: (877) IDTHEFT (877-438-4338)
    - Or use its online identity theft complaint form: www.consumer.gov/idtheft
    - Or write: FTC Identity Theft Clearinghouse, 600 Pennsylvania Ave. N.W.,
- Washington, DC 20580.
    - The FTC's uniform fraud affidavit form is available at
- www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf

- What to do with new credit accounts opened by the imposter. If your credit report shows that the imposter has opened new accounts in your name, contact those creditors immediately by telephone and in writing. Recent amendments to the FCRA (§623(6)(B)) allow you to prevent businesses from reporting fraudulent accounts to the credit bureaus.
- The FTC provides a sample dispute letter at www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#Resolving.

- Creditors will likely ask you to fill out fraud affidavits. The FTC provides a uniform affidavit form that most creditors accept, www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf. No law requires affidavits to be notarized at your own expense. You may choose to substitute witness signatures for notarization if creditors require verification of your signature.
- Ask the credit grantors in writing to furnish you and your investigating law enforcement agency with copies of the documentation, such as the fraudulent application and transaction records. Both federal and California law give you the right to obtain these documents. (FCRA § 609(e), and California Penal Code 530.8). The California Office of Privacy Protection provides instructions and sample letters on how to obtain documentation from credit grantors, www.privacy.ca.gov/sheets/cis3aenglish.pdf

- A victim of identity theft must provide a copy of the FTC affidavit or another affidavit acceptable to the business, plus government-issued identification, and a copy of an "identity theft report" (police report) in order to obtain the documents created by the imposter. The business must provide copies of these records to the victim within 30 days of the victim's request at no charge. The law also allows the victim to authorize a law enforcement investigator to get access to these records.

- When you have resolved the fraudulent account with the creditor, ask for a letter stating that the company has closed the disputed account and has discharged the debts. Keep this letter in your files. You may need it if the account reappears on your credit report.
- You must also notify the credit bureaus about the fraudulent accounts. Instructions are provided in Section 1 above.

- Handling problems with your existing credit or debit accounts. If your existing credit or debit accounts have been used fraudulently, report it in writing immediately to the credit card company.

- Request replacement cards with new account numbers. In addition to phoning the credit card company regarding the fraud, you will need to follow up in writing and will likely be asked to provide a fraud affidavit or a dispute form. Send the letter to the address given for "billing inquiries," not the address for sending payments. Carefully monitor your mail and bills for evidence of new fraudulent activity. Report it immediately. Add

secure passwords to all accounts. These should not be your mother's maiden name or any word that is easily guessed.

- Debt collectors. If debt collectors try to get you to pay the unpaid bills on fraudulent accounts, ask for the name of the collection company, the name of the person contacting you, phone number, and address. Tell the collector that you are a victim of fraud and are not responsible for the account. Ask for the name and contact information for the referring credit issuer, the amount of the debt, account number, and dates of the charges. Ask if they need you to complete their fraud affidavit form or whether you can use the FTC affidavit. Follow up by writing to the debt collector explaining your situation. Ask that they confirm in writing that you do not owe the debt and that the account has been closed.

- Under new provisions in the FCRA, a debt collector must notify the creditor that the debt may be a result of identity theft. (§615(g)) The FCRA also prohibits the sale or transfer of a debt caused by identity theft. (§615(f)) For additional information on dealing with debt collectors, read our Fact Sheet 27, which has a section for victims of identity theft at www.privacyrights.org/fs/fs27-debtcoll.htm#8