Identity Theft: What to Do if It Happens to You

You apply for a credit card and are turned down because of a low credit score, yet you know that you've always paid your accounts on time.

A debt collector calls to demand payment on a six-month overdue account for a credit card you have never had.

You receive a credit card in the mail that you've never applied for.

What's happening? You could be the victim of identity theft, where an imposter is using your personal information to obtain credit. Then when the thief does not pay the bills, the company itself or a debt collection company contacts you to demand payment. As a result, your credit report is likely to contain negative information about your bill-payment history, and your credit score has probably been lowered considerably, making it difficult or impossible to obtain new credit yourself.

This guide provides victims of identity theft with instructions on how to regain your financial health and who to contact for more help. You must act quickly and assertively to minimize the damage.

State-Specific Resources, www.privacyrights.org/fs/fs17a-ldTheft-US.htm.
Canadian victims, www.privacvrights.org/fs/fs17a-ldTheft-Canada.htm.

1. 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 that creditors are required to call you before extending credit. Consider using a cell phone number if you have one.

Equifax: P.O. Box 740250 Atlanta, GA 30374-0241 (888) 766-0008 www.equifax.com

Eperian: P.O. Box 9532 Allen, TX 75013 (888-397-3742

TransUnion: P.O. Box 6790 Fullerton, CA 92834-6790 (800) 680-7289
fvad@transunion.com

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 then 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, §6056) 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).

1a. 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.

1b. Security freeze. 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 web page: www.consumersunion.org/campaigns//learn more/003484indiv.html

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.

2. 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.htmffIdentity

3. 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

4. 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.htmffResolving (scroll down).

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. Federal law give you the right to obtain these documents. (FCRA § 609(e).

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.

5. 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.

6. 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.Drivacyrights.org/fs/fs27-debtcoll.htmtf8

7. Check and banking fraud. *If you have had checks stolen* or bank accounts set up fraudulently, ask your bank to report it to ChexSystems, a consumer reporting agency that compiles reports on checking accounts. Also, place a security alert on your file (see web address below).

Your bank should be able to provide you with a fraud affidavit. Put "stop payments" on any outstanding checks that you are unsure about. Close your checking account and other affected accounts and obtain new account numbers. Give the bank a password for your account (not mother's maiden name, Social Security number, date of birth, pet's name, sequential numbers, or any other easily guessed words).

- Phone: (800) 428-9623. Fax: (602) 659-2197
- Web: https://www.consumerdebit.com/consumerinfo/us/en/index.htm

- To place a security alert on your ChexSystems report: https://www.consumerdebit.com/consumerinfo/us/en/chexsystems/theftaffidavit/index.htm Write: ChexSystems Inc., Attn: Consumer Relations, 7805 Hudson Rd., Suite 100, Woodbury, MN 55125.

If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses. The major ones are listed here.

Fidelity National Information Services (was Certegy)	(800)437-5120	www.fidelityinfoservices.com
SCAN…	(800) 262-7771	www.consumerdebit.com
TeleCheck For annual file disclosure Fraud, id theft department		
International Check Services	(800) 526-5380	
Crosscheck	(800) 843-0760	www.cross-check.com

Under a new federal law, you now have a right to obtain any reports that these companies compile about you. For ChexSystems and any of the check verification companies listed here that you have had to contact as a result of your identity theft situation, we recommend that you request a copy of your file once a year. Make sure your file has been corrected. If not, you will find it difficult to open new bank accounts and/or write checks. Visit the web sites listed above to learn how to order your free annual reports. And read the PRC's guide on these "specialty reports." www.privacyrights.org/fs/fs6b-SpecReports.htm

8. ATM cards. *If your ATM or debit card has been stolen or compromised* , report it immediately. Contact your bank and fill out a fraud affidavit. Get a new card, account number, and password. Do not use your old password. Closely monitor your account statements. *You may be liable if the fraud is not reported quickly.* Start with a phone call and immediately follow up in writing. Be sure to read the debit card contract for information about liability. Some cards are better protected in cases of fraud than others.

ATM and debit card transactions are subject to the Electronic Fund Transfer Act. (15 USC §1693) Even if you are a victim of identity theft, your liability for charges can increase the longer the crime goes unreported. For more on EFTA, see the Federal Reserve Board's guide, www.federalreserve.gov/pubs/consumerhdbk/electronic.htm. Also read the FTC's guide on electronic banking, www.ftc.gov/bcp/conline/pubs/credit/elbank.htm

9. Brokerage accounts. You do not have the same protections against loss with brokerage accounts as you do with credit and debit card or bank accounts. The Securities Investor Protection Corporation (www.sipc.org) restores customer funds only when a brokerage firm fails. If an identity thief or other fraudster targets your brokerage account, refer to your account agreement for information on what to do. Immediately report the incident to the brokerage company and notify the Securities and Exchange Commission, www.sec.gov Also notify the National Association of Securities Dealers, www.nasd.org. To protect against fraud, put a password on each of your investment accounts. For more on identity theft involving brokerage accounts, how it can happen, and what to do, see the PRC alert, www.privacyrights.org/ar/BrokerageAlert.htm

10. Fraud involving U.S. mail. Notify the local Postal Inspector if you suspect an unauthorized change of your address with the post office or if the U.S mail has been used to commit fraud. Find out where fraudulent credit cards were sent. Notify the local Postmaster to forward all mail in your name to your own address. You may also need to talk with the mail carrier.

Call the U.S. Postal Service to find the nearest Postal Inspector at (800) 275-8777 or visit its web site at www.usps.com/postalinspectors. The online complaint form is available at www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm. Or you can mail your complaint to: U.S. Postal Service, Criminal Investigations Service Center, Attn: Mail Fraud, 222 S. Riverside Plaza Suite 1250, Chicago, IL 60606-6100.

11. Secret Service. The U.S. Secret Service has jurisdiction over financial fraud. But, based on U.S. Attorney guidelines, it usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies and/or banks, as well as the police investigator, to notify the Secret Service agent they work with.
www.treas.gov/usss/financial crimes.shtml

12. Social Security number (SSN) misuse. The Social Security Administration (SSA) does nof in most cases provide assistance to identity theft victims. But be sure to contact the SSA Inspector General to report Social Security benefit fraud, employment fraud, or welfare fraud.

- Social Security Administration online complaint form: www.socialsecuritv.gov/oig
- SSA fraud hotline: (800) 269-0271
- By mail: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235

As a last resort, you might try to change your number, although we *don't recommend it except for very serious cases .* The SSA will only change the number if you fit their fraud victim criteria. See the Identity Theft Resource Center's Fact Sheet 113 for more information, www.idtheftcenter.org/vg113.shtml

If your SSN card has been stolen or lost, order a replacement. Complete the SSA's application available at www.socialsecurity.gov/online/ss-5.html or by calling the SSA at (800) 772-1213, or by visiting your local SSA office. You will need to provide the required documentation such as birth certificate and government ID at your local SSA office to get a replacement card.

13. Passports. Whether you have a passport or not, write to the passport office to alert them to anyone ordering a passport fraudulently.

- U.S. Dept. of State, Passport Services, Consular Lost/Stolen Passport Section, 1111 19th St., NW, Suite 500, Washington, DC 20036.
- Website: www.traveLstate.gov/passport/lost/lost 849.html

14. Phone service. Identity thieves often establish fraudulent cell phone accounts, with monthly bills going unpaid. The imposter might also have opened local and long distance telephone accounts. If the imposter has obtained phone account(s) in your name, contact the phone company for information on how to report the situation. The steps that you take to clear your name with both the Phone Company and credit bureaus are much the same as with credit card accounts described above in steps one and three.

If your calling card has been stolen or there are fraudulent charges, cancel it and open a new account. For your own phone accounts, add a password that must be used any time your local, cell phone, and long distance accounts are changed.

15. Student loans. If an identity thief has obtained a student loan in your name, report it in writing to the school that opened the loan. Request that the account be closed. Also report it to the U.S. Dept. of Education:

- Call: U.S. Dept. of Education Inspector General's Hotline: (800) MISUSED (800-647-8733)

- Write: Office of Inspector General, U.S. Dept. of Education, 400 Maryland Ave., SW, Washington, DC 20202-1510.
- Web: www.ed.gov/about/offices/list/oig/hotiine.html?src=rt

16. Driver's license number misuse. You may need to change your driver's license number if someone is using yours as ID on bad checks or for other types of fraud. Call the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license if your state's DMV provides a fraud alert process. Go to your local DMV to request a new number. Fill out the DMV's complaint form to begin the investigation process. Send supporting documents with the completed form to the nearest DMV investigation office.

17. Identity theft involving family members and others you know. If a deceased relative's information is being used to perpetrate identity theft, or if you personally know the identity thief, additional information about how to address these situations is available in other fact sheets. Visit the Identity Theft Resource Center web site:

- When you know the perpetrator (family member, acquaintance), www.idtheftcenter.org/vg11 S.shtml
- ID theft of the deceased, www.idtheftcenter.org/vg117.shtml
- Children and ID theft, www.idtheftcenter.org/vg120b.shtml

18. Victim statements. If the imposter is apprehended by law enforcement and stands trial and/or is sentenced, write a victim impact letter to the judge handling the case. Contact the victim-witness assistance program in your area for further information on how to make your voice heard in the legal proceedings. Read the Identity Theft Resource Center's Fact Sheet 111, www.idtheftcenter.org/vg111 .shtml.

19. False civil and criminal judgments. Sometimes victims of identity theft are wrongfully accused of crimes that were committed by the imposter. If you are wrongfully arrested or prosecuted for criminal charges, contact the police department and the court in the jurisdiction of the arrest. Also contact your state's Department of Justice and the FBI to ask how to clear your name. If a civil judgment is entered in your name for your imposter's actions, contact the court where the judgment was entered and report that you are a victim of identity theft. For more on what to do if you become the victim of criminal identity theft, see PRC Fact Sheet 17g, www.privacyrights.org/fs/fs17g-CrimldTheft.htm

20. Legal help. You may want to consult an attorney to determine legal action to take against creditors, credit bureaus, and/or debt collectors if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor. Call the local Bar Association (www.abanet.org/premartindale.html), a Legal Aid office in your area (for low-income households), or the National Association of Consumer Advocates (www.naca.net) to find an attorney who specializes in consumer law, the Fair Credit Reporting Act, and the Fair Credit Billing Act.

If you are a senior citizen or take care of a dependent adult, be sure to contact an elder law service or the nearest Aging and Independent Services program. Many district attorneys have an elder abuse unit with expertise in financial crimes against seniors.

21. Keep good records. In dealing with the authorities and financial companies, *keep a log* of all conversations, including dates, names, and phone numbers. Note the time you spent and any

expenses incurred in case you are able to seek restitution in a later judgment or conviction against the thief. You may be able to obtain tax deductio ns for theft-related expenses (26 U.S.C. §165(e) -consult your accountant). Confirm all conversations in writing. Send correspondence using certified mail with return receipt requested. Keep copies of all letters and documents.

Visit these web sites for tips on organizing your case:

- FTC's guide *Take Charge,* www.ftc.gov/bcp/conline/pubs/credit/idtheft.htmtfldentity
- Identity Theft Resource Center, www.idtheftcenter.org/vg106.shtml

22. Dealing with emotional stress. Psychological counseling may help you deal with the stress and anxiety commonly experienced by victims. Know that you are not alone. Contact the Identity Theft Resource Center for information on how to network with other victims and deal with the impact of this crime, www.idtheftcenter.org

23. Making change. Write to your state and federal legislators. Demand stronger privacy protection and prevention efforts by creditors and credit bureaus.

24. Don't give in. Do not pay any bill or portion of a bill that is a result of fraud. Do not cover any checks that were written or cashed fraudulently. Do not file for bankruptcy. Your credit rating should not be permanently affected. No legal action should be taken against you. If any merchant, financial company or collection agency suggests otherwise, restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills. Report such attempts to government regulators immediately.

25. Other Useful Tips

If you are in the military, place an active duty alert on your credit report
When you are away from your usual duty station, you can place an active duty alert on your three credit reports as an extra protection against identity theft. The alert remains on your credit reports for 12 months. Contact the fraud departments for the three credit bureaus. Those phone numbers are provided in Section 1 above.

Order your free credit report
Whether or not you are a victim of identity theft, take advantage of your free annual credit reports, now a requirement of federal law.

- Phone: (877) 322-8228
- Web: www.annualcreditreport.com
- FTC's guide: www.ftc.gov/bcp/conline/pubs/credit/freereports.htm

Opt out of pre-approved offers of credit for all three credit bureaus

- Call (888) 5OPTOUT (888-567-8688). You may choose a five-year opt-out period or permanent opt-out status.
- Or opt-out online, www.optoutprescreen.com

Remove your name from mail marketing lists (Direct Marketing Association)

- Write: Mail Preference Service, P.O. Box 282, Carmel, NY 10512. Include check or money order for $1.
- Web: www.dmaconsumers.org/cgi/offmailinglist. Online opt-out program costs $1 by credit card.

Remove your phone number(s) from telemarketing lists

- Phone the FTC's Do Not Call Registry: (888) 382-1222
- Online registration: www.donotcall.gov

Order your earnings report from the Social Security Administration

- Order your Personal Earnings and Benefits Estimate Statement if you suspect an identity thief has used your SSN for employment: (800) 772-1213. The SSA automatically mails it to individuals three months before the birthday each year, www.ssa.gov/online/ssa-7004.html

- For information on reporting fraud to the SSA, read tip 12 above.

26. Resources

Federal Trade Commission (FTC)

- Read its guide, *Take Charge: Fighting Back Against Identity Theft,* www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.
- Online information and complaint form: www.consumer.gov/idtheft
- FTC uniform fraud affidavit form: www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf
- Identity Theft Hotline: (877) IDTHEFT (877-438-4338)
- Write: FTC Identity Theft Clearinghouse, 600 Pennsylvania Ave. N.W., Washington, DC 20580

Federal Agencies and Technology Industry

- For tips on online safety, visit www.onguardonline.gov

Identity Theft Resource Center (ITRC)

- Guides for victims, www.idtheftcenter.org (Click on Victim Resources.)
- Phone: (858) 693-7935
- Web: www.idtheftcenter.org
- E-mail: itrc@idtheftcenter.org
- Write: P.O. Box 26833, San Diego, CA 92196

Identity Theft Survival Kit

- Mari Frank, Esq., author of *From Victim to Victor: A Step-by-Step Guide for Ending the Nightmare of Identity Theft* and *Safeguard Your Identity: Protect Yourself with a Personal Privacy Audit*
- Web: www.identitytheft.org
- Phone: (800) 725-0807

U.S. Dept. of Justice. The DOJ prosecutes federal identity theft cases.

- Web: www.usdoi.gov/criminal/fraud/idtheft.html

FBI Internet Fraud Complaint Center. The Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center, allows you to report suspected cases of Internet and e-commerce fraud, including phishing.

- Web: www.ic3.gov