

**OFFICE OF THE STAFF JUDGE ADVOCATE
48TH FIGHTER WING, RAF LAKENHEATH, UK**



Identity Theft:

When Bad Things Happen To Your Good Name

TABLE OF CONTENTS

Introduction	3
Minimize Your Risk	3
Choosing to Share Personal Information – Or Not	5
Credit Bureaus	5
Departments of Motor Vehicles	5
Direct Marketers	5
If You're a Victim	7
Your First Three Steps	7
Your Next Steps	8
Where There's Help	9
Resolving Credit Problems	11
Credit Reports	11
Credit Cards	12
Debt Collectors	13
ATM Cards, Debit Cards and Electronic Fund Transfers	13
Sample Dispute Letters	14
Resources	15
Federal Government	15
State and Local Governments	19
Credit Bureaus	19

INTRODUCTION

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, call home on your cell phone, order new checks or apply for a credit card. Chances are you don't give these everyday transactions a second thought. But someone else may.

The 1990's spawned a new variety of crooks called identity thieves. Their stock in trade are your everyday transactions. Each transaction requires you to share personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); and your name, address and phone numbers. An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name.

Can you completely prevent identity theft from occurring? Probably not, especially if someone is determined to commit the crime. But you can minimize your risk by managing your personal information wisely, cautiously and with heightened sensitivity.

The Congress of the United States asked the Federal Trade Commission to provide information to consumers about identity theft and to take complaints from those whose identities have been stolen. The FTC has developed the ID Theft Affidavit – a form you can use to alert companies where a new account was opened in your name. To access the form, visit:
www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf

MINIMIZE YOUR RISK

While you probably can't prevent identity theft entirely, you can minimize your risk. By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft:

- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover his tracks.
- Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask if you have a choice about the use of your information: can you choose to have it kept confidential?
- Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up.
- Put passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- Minimize the identification information and the number of cards you carry to what you'll actually need.

- Do not give out personal information on the phone, through the mail or over the Internet unless you have initiated the contact or know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with whom you do business have the information they need and will not ask you for it.
- Keep items with personal information in a safe place. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements that you are discarding, expired charge cards and credit offers you get in the mail.
- Be cautious about where you leave personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.
- Find out who has access to your personal information at work and verify that the records are kept in a secure location.
- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible.
- Don't carry your SSN card; leave it in a secure place.
- Order a copy of your credit report from each of the three major credit-reporting agencies every year. Make sure it is accurate and includes only those activities you've authorized. The law allows credit bureaus to charge you up to \$9.00 for a copy of your credit report.

Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you've been sued, arrested or filed for bankruptcy. Checking your report on a regular basis can help you catch mistakes and fraud before they wreak havoc on your personal finances.

A SPECIAL WORD ABOUT SOCIAL SECURITY NUMBERS

Your employer and financial institution will likely need your SSN for wage and tax reporting purposes. Other private businesses may ask you for your SSN to do a credit check, such as when you apply for a car loan. Sometimes, however, they simply want your SSN for general record keeping. You don't have to give a business your SSN just because they ask for it. If someone asks for your SSN, ask the following questions:

- Why do you need my SSN?
- How will my SSN be used?
- What law requires me to give you my SSN?
- What will happen if I don't give you my SSN?

Sometimes a business may not provide you with the service or benefit you're seeking if you don't provide your SSN. Getting answers to these questions will help you decide whether you want to share your SSN with the business. Remember, though, that the decision is yours.

CREDIT BUREAUS

Equifax – www.equifax.com

To order your report, call: 1-877-322-8228 or write:

Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283 (free annual credit report)

To report fraud or place a fraud alert, call: 1-888-766-0008 or write: Equifax Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374

Experian – www.experian.com

To order your report, call: 1-888-EXPERIAN (397-3742) or write: Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283 (free annual credit report)

To report fraud, call: 1-888-EXPERIAN (397-3742)

TransUnion – www.transunion.com

To order your report, call: 1-800-888-4213 or write:

Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283 (free annual credit report), or TransUnion LLC, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19022 (to purchase a TransUnion credit report)

To report fraud, call: 1-800-680-7289/ TDD:

and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834.

CHOOSING TO SHARE YOUR PERSONAL INFORMATION

What happens to the personal information you provide to companies, marketers and government agencies? They may use your information just to process your order. They may use it to create a profile about you and then let you know about products, services or promotions. Or they may share your information with others. More organizations are offering consumers choices about how their personal information is used. For example, many let you "opt out" of having your information shared with others or used for promotional purposes.

You can learn more about the choices you have to protect your personal information from credit bureaus, state Departments of Motor Vehicles and direct marketers.

CREDIT BUREAUS

Pre-Screened Credit Offers

If you receive pre-screened credit card offers in the mail (namely, those based upon your credit data), but don't tear them up after you decide you don't want to accept the offer, identity thieves may retrieve the offers for their own use without your knowledge.

To opt out of receiving pre-screened credit card offers for five years, call: 1-888-5-OPTOUT (1-888-567- 8688). The three major credit bureaus use the same toll-free number to let consumers choose not to receive pre-screened credit offers. To opt out permanently, you may begin the permanent Opt-Out process online at www.optoutprescreen.com. To complete your request, you must return the signed Permanent Opt-Out Election form, which will be provided after you initiate your online request.

When you call or visit the website, you'll be asked to provide certain personal information, including your home telephone number, name, Social Security number, and date of birth. The information you provide is confidential and will be used only to process your request to opt out. If you don't have access to the Internet, you may send a written request to permanently opt out to each of the major consumer reporting companies. Make sure your request includes your home telephone number, name, Social Security number, and date of birth.

Experian

Opt Out
P.O. Box 919
Allen, TX 75013

TransUnion

Name Removal Option
P.O. Box 505
Woodlyn, PA 19094

Equifax, Inc.

Options
P.O. Box 740123
Atlanta, GA 30374

Innovis Consumer Assistance

P.O. Box 495
Pittsburgh, PA 15230

Marketing Lists

Of the three major credit bureaus, only Experian offers consumers the opportunity to have their names removed from lists that are used for marketing and promotional purposes. To have your name removed from Experian's marketing lists, call 1-800-407-1088.

DEPARTMENTS OF MOTOR VEHICLES

Take a look at your driver's license. All the personal information on it-and more-is on file with your state Department of Motor Vehicles (DMV). A state DMV may distribute your personal information for law enforcement, court proceedings and insurance underwriting purposes, but may not distribute it for direct marketing without your express consent.

Contact your state DMV for more information.

DIRECT MARKETERS

The Direct Marketing Association's (DMA) Mail, E-mail and Telephone Preference Services allow consumers to opt out of direct mail marketing, e-mail marketing and/or telemarketing solicitations from many national companies. Because your name will not be on their lists, it also means that these companies can't rent or sell your name to other companies.

To obtain more information about getting off telephone call lists and the Telephone Preference Service, visit: <https://www.the-dma.org/cgi/offtelephonedave>.

IF YOU'RE A VICTIM

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information to yourself. If you suspect that your personal information has been hijacked and misappropriated to commit fraud or theft, take action immediately, and keep a record of your conversations and correspondence. Exactly which steps you should take to protect yourself depends on your circumstances and how your identity has been misused. However, three basic actions are appropriate in almost every case.

YOUR FIRST THREE STEPS

First, contact the fraud departments of each of the three major credit bureaus.

Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, as well as a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts. This can help prevent an identity thief from opening additional accounts in your name.

At the same time, order copies of your credit reports from the credit bureaus. Credit bureaus must give you a free copy of your report if your report is inaccurate because of fraud, and you request it in writing. Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. Also, check the section of your report that lists "inquiries." Where "inquiries" appear from the company(ies) that opened the fraudulent account(s), request that these "inquiries" be removed from your report. (See "Credit Reports" for more information.) In a few months, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.

Second, contact the creditors for any accounts that have been tampered with or opened fraudulently.

Creditors can include credit card companies, phone companies and other utilities, and banks and other lenders. Ask to speak with someone in the security or fraud department of each creditor, and follow up with a letter. It's particularly important to notify credit card companies in writing because that's the consumer protection procedure the law spells out for resolving errors on credit card billing statements. Immediately close accounts that have been tampered with and open new ones with new Personal Identification Numbers (PINs) and passwords. Here again, avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

Third, file a report with your local police or the police in the community where the identity theft took place.

Get a copy of the police report in case the bank, credit card company or others need proof of the crime. Even if the police can't catch the identity thief in your case, having a copy of the police report can help you when dealing with creditors.

YOUR NEXT STEPS

Although there's no question that identity thieves can wreak havoc on your personal finances, there are some things you can do to take control of the situation. For example:

- **Stolen mail.** If an identity thief has stolen your mail to get new credit cards, bank and credit card statements, pre-screened credit offers or tax information, or if an identity thief has falsified change-of-address forms, that's a crime. Report it to your local postal inspector. Contact your local post office for the phone number for the nearest postal inspection service office or check the Postal Service web site at www.usps.gov/websites/depart/inspect.
- **Change of address on credit card accounts.** If you discover that an identity thief has changed the billing address on an existing credit card account, close the account. When you open a new account, ask that a password be used before any inquiries or changes can be made on the account. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. Avoid using the same information and numbers when you create a PIN.
- **Bank accounts.** If you have reason to believe that an identity thief has tampered with your bank accounts, checks or ATM card, close the accounts immediately. When you open new accounts, insist on password-only access to minimize the chance that an identity thief can violate the accounts.

In addition, if your checks have been stolen or misused, stop payment. You can contact the following major check verification companies to learn more about the services they provide in helping you track your stolen or misused checks.

SCAN: 1-800-262-7771

TeleCheck: 1-800-710-9898

CrossCheck: 1-800-843-0760

Equifax Check Systems: 1-800-437-5120

International Check Services: 1-800-526-5380

National Processing Co.: 1-800-526-5380

ChexSystems: 1-800-428-9623

If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can and get another with a new PIN.

Investments. If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the Securities and Exchange Commission.

You can file a complaint with the SEC by visiting the Complaint Center at <http://www.sec.gov/complaint/select.shtml>

- Be sure to include as much detail as possible.
- **Phone service.** If an identity thief has established new phone service in your name; is making unauthorized calls that seem to come from - and are billed to - your cellular

phone; or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs.

If you are having trouble getting fraudulent phone charges removed from your account, contact your state Public Utility Commission for local service providers or the Federal Communications Commission for long-distance service providers and cellular providers at <http://www.fcc.gov/complaints> or 1-888-CALL-FCC.

- **Employment.** If you believe someone is using your SSN to apply for a job or to work, that's a crime. Report it to the SSA's Fraud Hotline at 1-800-269-0271. Also call SSA at 1-800-772-1213 to verify the accuracy of the earnings reported on your SSN, and to request a copy of your *Social Security Statement*. Follow up your calls in writing.
- **Driver's license.** If you suspect that your name or SSN is being used by an identity thief to get a driver's license or a non-driver's ID card, contact your Department of Motor Vehicles. If your state uses your SSN as your driver's license number, ask to substitute another number.
- **Bankruptcy.** If you believe someone has filed for bankruptcy using your name, write to the U.S. Trustee in the Region where the bankruptcy was filed. A listing of the U.S. Trustee Program's Regions can be found at www.usdoj.gov/ust, or look in the Blue Pages of your phone book under U.S. Government - Bankruptcy Administration.

Your letter should describe the situation and provide proof of your identity. The U.S. Trustee, if appropriate, will make a referral to criminal law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed.

- **Criminal records/arrests.** In rare instances, an identity thief may create a criminal record under your name. For example, your imposter may give your name when being arrested. If this happens to you, you may need to hire an attorney to help resolve the problem. The procedures for clearing your name vary by jurisdiction.

SHOULD I APPLY FOR A NEW SOCIAL SECURITY NUMBER?

Under certain circumstances, SSA may issue you a new SSN - at your request - if, after trying to resolve the problems brought on by identity theft, you continue to experience problems. Consider this option carefully. A new SSN may not resolve your identity theft problems, and may actually create new problems. For example, a new SSN does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old SSN with those from your new SSN. Even when the old credit information is not associated with your new SSN, the absence of any credit history under your new SSN may make it more difficult for you to get credit. And finally, there's no guarantee that a new SSN wouldn't also be misused by an identity thief.

WHERE THERE'S HELP...

The FTC collects complaints about identity theft from consumers who have been victimized. Although the FTC does not have the authority to bring criminal cases, the Commission can help victims of identity theft by providing information to assist them in resolving the financial and other problems that can result from this crime. The FTC also refers victim complaints to other appropriate government agencies and private organizations for further action.

Other agencies and organizations also are working to combat identity theft. If specific institutions and companies are not being responsive to your questions and complaints, you also may want to contact the government agencies with jurisdiction over those companies.

Identity Theft and Assumption Deterrence Act of 1998

The Identity Theft and Assumption Deterrence Act makes it a federal crime when someone:

"knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Note that under the Act, a name or SSN is considered a "means of identification." So is a credit card number, cellular telephone electronic serial number or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

In most instances, a conviction for identity theft carries a maximum penalty of **15 years imprisonment, a fine and forfeiture of any personal property used or intended to be used to commit the crime.** The Act also directs the U.S. Sentencing Commission to review and amend the federal sentencing guidelines to provide appropriate penalties for those persons convicted of identity theft.

Schemes to commit identity theft or fraud also may involve violations of other statutes, such as credit card fraud; computer fraud; mail fraud; wire fraud; financial institution fraud; or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties - in some cases, as high as 30 years in prison, fines and criminal forfeiture.

State Laws Many states have passed laws related to identity theft; others may be considering such legislation. Where specific identity theft laws do not exist, the practices may be prohibited under other laws. Contact your State Attorney General's office or local consumer protection agency to find out whether your state has laws related to identity theft, or visit www.consumer.gov/idtheft.

RESOLVING CREDIT PROBLEMS

Resolving credit problems resulting from identity theft can be time-consuming and frustrating. The good news is that there are federal laws that establish procedures for correcting credit report errors and billing errors, and for stopping debt collectors from contacting you about debts you don't owe.

Here is a brief summary of your rights, and what to do to clear up credit problems that result from identity theft.

CREDIT REPORTS

The Fair Credit Reporting Act (FCRA) establishes procedures for correcting mistakes on your credit record and requires that your record be made available only for certain legitimate business needs.

Under the FCRA, both the credit bureau and the organization that provided the information to the credit bureau (the "information provider"), such as a bank or credit card company, are responsible for correcting inaccurate or incomplete information in your report. To protect your rights under the law, contact both the credit bureau and the information provider.

First, call the credit bureau and follow up in writing. Tell them what information you believe is inaccurate. Include copies (NOT originals) of documents that support your position. In addition to providing your complete name and address, your letter should clearly identify each item in your report that you dispute, give the facts and explain why you dispute the information, and request deletion or correction. You may want to enclose a copy of your report with circles around the items in question. Send your letter by certified mail, and request a return receipt so you can document what the credit bureau received and when. Keep copies of your dispute letter and enclosures.

Credit bureaus must investigate the items in question - usually within 30 days - unless they consider your dispute frivolous. They also must forward all relevant data you provide about the dispute to the information provider. After the information provider receives notice of a dispute from the credit bureau, it must investigate, review all relevant information provided by the credit bureau and report the results to the credit bureau. If the information provider finds the disputed information to be inaccurate, it must notify any nationwide credit bureau that it reports to so that the credit bureaus can correct this information in your file. Note that:

- Disputed information that cannot be verified must be deleted from your file.
- If your report contains erroneous information, the credit bureau must correct it.
- If an item is incomplete, the credit bureau must complete it. For example, if your file shows that you have been late making payments, but fails to show that you are no longer delinquent, the credit bureau must show that you're current.
- If your file shows an account that belongs to someone else, the credit bureau must delete it.

When the investigation is complete, the credit bureau must give you the written results and a free copy of your report if the dispute results in a change. If an item is changed or removed, the credit

bureau cannot put the disputed information back in your file unless the information provider verifies its accuracy and completeness, and the credit bureau gives you a written notice that includes the name, address and phone number of the information provider.

If you request, the credit bureau must send notices of corrections to anyone who received your report in the past six months. Job applicants can have a corrected copy of their report sent to anyone who received a copy during the past two years for employment purposes. If an investigation does not resolve your dispute, ask the credit bureau to include your statement of the dispute in your file and in future reports.

Second, in addition to writing to the credit bureau, tell the creditor or other information provider ***in writing*** that you dispute an item. Again, include copies (NOT originals) of documents that support your position. Many information providers specify an address for disputes. If the information provider then reports the item to any credit bureau, it must include a notice of your dispute. In addition, if you are correct - that is, if the disputed information is not accurate - the information provider may not use it again.

CREDIT CARDS

The Truth in Lending Act limits your liability for unauthorized credit card charges in most cases to \$50 per card. The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts.

The Act's settlement procedures apply to disputes about "billing errors." This includes fraudulent charges on your accounts.

To take advantage of the law's consumer protections, you ***must***:

- write to the creditor at the address given for "billing inquiries," not the address for sending your payments. Include your name, address, account number and a description of the billing error, including the amount and date of the error.
- send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. If the address on your account was changed by an identity thief and you never received the bill, your dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill. This is why it's so important to keep track of your billing statements and immediately follow up when your bills don't arrive on time.

Send your letter by certified mail, and request a return receipt. This will be your proof of the date the creditor received the letter. Include copies (NOT originals) of sales slips or other documents that support your position. Keep a copy of your dispute letter.

The creditor must acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

DEBT COLLECTORS

The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection.

You can stop a debt collector from contacting you by writing a letter to the collection agency telling them to stop. Once the debt collector receives your letter, the company may not contact you again - with two exceptions: they can tell you there will be no further contact and they can tell you that the debt collector or the creditor intends to take some specific action.

A collector also may not contact you if, within 30 days after you receive the written notice, you send the collection agency a letter stating you do not owe the money. Although such a letter should stop the debt collector's calls, it will not necessarily get rid of the debt itself, which may still turn up on your credit report. In addition, a collector can renew collection activities if you are sent proof of the debt. So, along with your letter stating you don't owe the money, include copies of documents that support your position. If you're a victim of identity theft, including a copy (NOT original) of the police report you filed may be particularly useful.

ATM CARDS, DEBIT CARDS AND ELECTRONIC FUND TRANSFERS

The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card or other electronic way to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

It's important to report lost or stolen ATM and debit cards immediately because the amount you can be held responsible for depends on **how quickly** you report the loss.

- If you report your ATM card lost or stolen within two business days of discovering the loss or theft, your losses are limited to \$50.
- If you report your ATM card lost or stolen after the two business days, but within 60 days after a statement showing an unauthorized electronic fund transfer, you can be liable for up to \$500 of what a thief withdraws.
- If you wait more than 60 days, you could lose **all** the money that was taken from your account after the end of the 60 days and before you report your card missing.

The best way to protect yourself in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing - by certified letter, return receipt requested - so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After notification about an error on your statement, the institution generally has 10 business days to investigate. The financial institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that the error has occurred. If the institution needs more time, it may take up to 45 days to complete the investigation - but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

Note: VISA and MasterCard voluntarily have agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to \$50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.

Sample Dispute Letter — Credit Bureau

Date

Your Name

Your Address

Your City, State, Zip Code

Complaint Department

Name of Credit Bureau

Address

City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute also are circled on the attached copy of the report I received. (Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

This item is (inaccurate or incomplete) because (describe what is inaccurate or incomplete and why). I am requesting that the item be deleted (or request another specific change) to correct the information.

Enclosed are copies of (use this sentence if applicable and describe any enclosed documentation, such as payment records, court documents) supporting my position. Please investigate this (these) matter(s) and (delete or correct) the disputed item(s) as soon as possible.

Sincerely, Your name

Enclosures: (List what you are enclosing.)

Sample Dispute Letter — Credit Card Issuers

Date

Your Name

Your Address

Your City, State, Zip Code

Your Account Number

Name of Creditor

Billing Inquiries

Address

City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a billing error in the amount of \$_____ on my account. The amount is inaccurate because (describe the problem). I am requesting that the error be corrected, that any finance and other charges related to the disputed amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as sales slips, payment records) supporting my position. Please investigate this matter and correct the billing error as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

A Special Word About Lost or Stolen Checks

While no federal law limits your losses if someone steals your checks and forges your signature, state laws protect you. Most states hold the bank responsible for losses from a forged check. At the same time, however, most states 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 manner that a check was lost or stolen. Contact your state banking or consumer protection agency for more information.

RESOURCES

FEDERAL GOVERNMENT

***Federal Trade Commission (FTC)* — www.ftc.gov**

The FTC is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not have the authority to bring criminal cases, the Commission helps victims of identity theft by providing them with information to help resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for action.

If you've been a victim of identity theft, file a complaint with the FTC by contacting the FTC's Identity Theft Hotline by telephone: toll-free 1-877-IDTHEFT (438-4338); TDD: 1-866-653-4261; by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or online: www.consumer.gov/idtheft.

Banking Agencies

If you're having trouble getting your financial institution to help you resolve your banking-related identity theft problems including problems with bank-issued credit cards contact the agency with the appropriate jurisdiction. If you're not sure which agency has jurisdiction over your institution, call your bank or visit <http://www.ffiec.gov/nicpubweb/nicweb/nichome.aspx>

***Federal Deposit Insurance Corporation (FDIC)* — www.fdic.gov**

The FDIC supervises state-chartered banks that are not members of the Federal Reserve System and insures deposits at banks and savings and loans.

Call the FDIC Consumer Call Center at 877-275-3342; or write: Federal Deposit Insurance Corporation, Division of Compliance and Consumer Affairs, 550 17th Street, NW, Washington, DC 20429.

***Federal Reserve System (Fed)* — www.federalreserve.gov**

The Fed supervises state-chartered banks that are members of the Federal Reserve System.

Call: 202-452-3693; or write: Division of Consumer and Community Affairs, Mail Stop 801, Federal Reserve Board, Washington, DC 20551; or contact the Federal Reserve Bank in your area. The 12 Reserve Banks are located in Boston, New York, Philadelphia, Cleveland, Richmond, Atlanta, Chicago, St. Louis, Minneapolis, Kansas City, Dallas and San Francisco.

National Credit Union Administration (NCUA) — www.ncua.gov

The NCUA charters and supervises federal credit unions and insures deposits at federal credit unions and many state credit unions.

Call: 703-518-6360; or write: Compliance Officer, National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314.

Office of the Comptroller of the Currency (OCC) — www.occ.treas.gov

The OCC charters and supervises national banks. If the word "national" appears in the name of a bank, or the initials "N.A." follow its name, the OCC oversees its operations.

Call: 1-800-613-6743 (business days 7:00 a.m. to 7:00 p.m. CST); fax: 713-336-4301; write: Customer Assistance Group, 1301 McKinney Street, Suite 3710, Houston, TX 77010.

Office of Thrift Supervision (OTS) — www.ots.treas.gov

The OTS is the primary regulator of all federal and many state-chartered thrift institutions, which include savings banks and savings and loan institutions.

Call: 202-906-6000; or write: Office of Thrift Supervision, 1700 G Street, NW, Washington, DC 20552.

Department of Justice (DOJ) — www.usdoj.gov

The DOJ and its U.S. Attorneys prosecute federal identity theft cases. Information on identity theft is available at <http://www.stopfraud.gov/protect-identity.html>

Federal Bureau of Investigation (FBI) — www.fbi.gov

The FBI is one of the federal criminal law enforcement agencies that investigates cases of identity theft. Local field offices are listed in the Blue Pages of your telephone directory.

Federal Communications Commission (FCC) — www.fcc.gov

The FCC regulates interstate and international communications by radio, television, wire, satellite and cable. The FCC's Consumer Information Bureau is the consumer's one-stop source for information, forms, applications and current issues before the FCC.

Call: 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554. You can file complaints via the online complaint form at www.fcc.gov, or e-mail questions to fccinfo@fcc.gov.

Internal Revenue Service (IRS) — <http://www.irs.gov/>

The IRS is responsible for administering and enforcing the internal revenue laws. If you believe someone has assumed your identity to file federal Income Tax Returns, or to commit other tax fraud, call toll-free: 1-800-908-4490. For assistance to victims of identity theft schemes who are

having trouble filing their correct returns, call the IRS Taxpayer Advocates Office, toll-free: 1-877-777- 4778.

U.S. Secret Service (USSS) — <http://www.secretservice.gov/>

The U.S. Secret Service is one of the federal law enforcement agencies that investigates financial crimes, which may include identity theft. Although the Secret Service generally investigates cases where the dollar loss is substantial, your information may provide evidence of a larger pattern of fraud requiring their involvement. Local field offices are listed in the Blue Pages of your telephone directory.

Social Security Administration (SSA) — www.ssa.gov

SSA may assign you a new SSN - at your request - if you continue to experience problems even after trying to resolve the problems resulting from identity theft. SSA field office employees work closely with victims of identity theft and third parties to collect the evidence needed to assign a new SSN in these cases.

SSA Office of the Inspector General (SSA/OIG)

The SSA/OIG is one of the federal law enforcement agencies that investigates cases of identity theft.

Direct allegations that an SSN has been stolen or misused to the SSA Fraud Hotline. Call: 1-800-269-0271; fax: 410-597-0118; write: SSA Fraud Hotline, P.O. Box 17785, Baltimore, MD 21235; or e-mail: oig.hotline@ssa.gov

U.S. Postal Inspection Service (USPIS) — www.usps.gov/websites/depart/inspect

The USPIS is one of the federal law enforcement agencies that investigates cases of identity theft. USPIS is the law enforcement arm of the U.S. Postal Service. USPIS has primary jurisdiction in all matters infringing on the integrity of the U.S. mail. You can locate the USPIS district office nearest you by calling your local post office or checking the list at the web site above.

U.S. Securities and Exchange Commission (SEC) — www.sec.gov

The SEC's Office of Investor Education and Assistance serves investors who complain to the SEC about investment fraud or the mishandling of their investments by securities professionals. If you've experienced identity theft in connection with a securities transaction, you can file a complaint with the SEC by visiting the Complaint Center at www.sec.gov/complaint.shtml. Be sure to include as much detail as possible. If you do not have access to the Internet, write to the SEC at: SEC Office of Investor Education and Assistance, 100 Fifth Street, NW, Washington, DC 20549-0213, or call 202-942-8088.

U. S. Trustee (UST) — www.usdoj.gov/ust

If you believe someone has filed for bankruptcy using your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A list of the U.S. Trustee's Regional Offices is available on the UST web site, or check the Blue Pages of your phone book under U.S. Government

Bankruptcy Administration. Your letter should describe the situation and provide proof of your identity. The U.S. Trustee, if appropriate, will make a criminal referral to criminal law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed.

The U.S. Trustee does not provide legal representation, legal advice or referrals to lawyers. That means you may need to hire an attorney to help convince the bankruptcy court that the filing is fraudulent. The U.S. Trustee does not provide consumers with copies of court documents. Those documents are available from the bankruptcy clerk's office for a fee.

STATE AND LOCAL GOVERNMENTS

Many states and local governments have passed laws related to identity theft; others may be considering such legislation. Where specific identity theft laws do not exist, the practices may be prohibited under other laws. Contact your State Attorney General's office (for a list of state offices, visit www.naag.org) or local consumer protection agency to find out whether your state has laws related to identity theft, or visit www.consumer.gov/idtheft/.

CREDIT BUREAUS

Equifax – www.equifax.com

To order your report, call: 1-877-322-8228 or write:

Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283 (free annual credit report)

To report fraud or place a fraud alert, call: 1-888-766-0008 or write: Equifax Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374

Experian – www.experian.com

To order your report, call: 1-888-EXPERIAN (397-3742) or write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5283 (free annual credit report)

To report fraud, call: 1-888-EXPERIAN (397-3742)

TransUnion – www.transunion.com

To order your report, call: 1-800-888-4213 or write:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (free annual credit report), or TransUnion LLC, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19022 (to purchase a TransUnion credit report)

To report fraud, call: 1-800-680-7289/ TDD:

877-553-7803 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634-6790