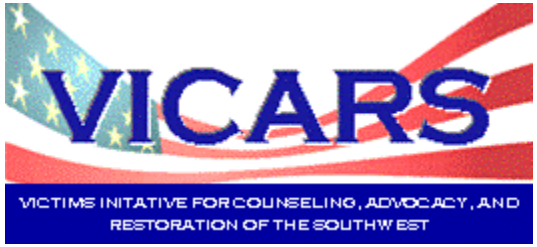

ACTION PLAN FOR VICTIMS OF IDENTITY THEFT

A program of the Texas Legal Services Center supported by Grant No. 2007-VF-GX-K032 awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice. ©2007

STEP 1 – PREPARE

- Get two folders, large envelopes, or other containers in which to keep documents.
- Label one folder "ORIGINALS." In it keep the originals of all materials you compile. Do not send your original documents to anyone. Keep them safe.
- Label the second folder "COPIES." In it keep copies of everything relevant to your identity theft/financial fraud case.
- Use the forms in this packet to document your progress.
- Begin by making several copies of pages 10, 11, 12, and 13 of this Action Plan. You may make as many copies of each form as you need.
- Prepare yourself mentally and emotionally. Know at the outset that clearing your credit history may take many months and will take many hours of your time. You may also incur out-of-pocket expenses such as postage and copying. It is worth the effort, though.
- Send all mail certified, return receipt requested. This is expensive, but worth it because it allows you to prove that the addressees received your letters. Our letter forms have a place below the recipient's address for you to record the certified mail number. This will help you match the postal service return cards (green cards) to your copies of the letters you send. When a green card is returned to you, paper clip it to your copy of the letter that matches the card and keep it in your folder.
- Do not take shortcuts. Follow up phone calls with letters confirming the contents of the calls. A document speaks for itself; whereas, you may not be able to prove what happened in a disputed telephone conversation.
- Keep track of your time. Each table in this Action Plan contains a column for you to record the time you spent working on your case. Record even a few minutes because they add up.
- Keep track of your expenses. Page 13 of this Action Plan is a table for recording your out-of-pocket expenses. Keep receipts in an envelope in case you need to copy them later.
- If you need additional help, call VICARS at 1-888-343-4414.

ACTION PLAN

The first thing you will be asked to do is prove that you are you. You will need copies of your drivers license or state issued ID card, your Social Security card, and most recent utility bills. You may be asked to prove your residence address for the last 5 years. Companies prefer to use utility bills as proof of address. Contact your utility provider and request a printout showing where you have had service for the past 5 years.

PROVING WHO I AM

My full name:

My date of birth:

Any other names that I have used:

My Social Security Number:

My Driver's License or ID Number:

My addresses for the past 5 years:

Time Spent

ACTION PLAN

The second thing you will be asked is, "Why do you think you are a victim of identity theft?" Make your answer as concise yet as complete as possible. Answer the questions below as accurately as possible. Use this chart as an outline when you speak to anyone about your identity theft. This will help you keep your communications consistent. You will use this information repeatedly in making reports and collecting evidence of your identity theft.

Question	Answer
How did you find out your identity was stolen? Examples: I was turned down for a car loan, or I got calls from a bill collector.	
When did you find out?	
What existing accounts, information, or property were taken and in what amount? Include as much information as you have. You will add to this later.	
What accounts were opened fraudulently using your identity? Include as much information as you have.	
Do you have written proof of the identity theft yet? Example: A letter from a collection agency.	

Time Spent

STEP 2 – REPORT

There are several steps to take to report your identity theft, and it may feel like you are duplicating your efforts. Each step is important, so do not be tempted to take shortcuts or omit a step. First, get a copy of your credit report and report your identity theft to local law enforcement and the FTC. You may encounter resistance. If so, be polite but firm. Advise each entity that you will provide additional information as it becomes available.

Credit Reporting Companies – Notify **one** that you are a victim. That company should notify the others within a few days. Request that a fraud alert be placed in your file. Request a free copy of your credit report. Request that the first 5 numbers of your Social Security Number be blocked from your credit report. After you have compiled more information (*see* p. 9), send a letter confirming your conversation and disputing all fraudulent activity on your credit report. At this point, you will be able to request an extended fraud alert. A form letter is provided in this toolkit. If you have internet access, get an instant credit report at www.annualcreditreport.com. Otherwise, it will take up to two weeks to receive your report. Because you can get one free report per company per year, it is a good idea to stagger your report requests. Ask for a free credit report from a different company every three to four months so that you can continuously monitor your credit. When you make telephone calls, you will not speak to a live person. All of the credit reporting companies and many other companies you contact use automated telephone systems.

Agency	Phone Number/ Address	Date of Contact	Contact Person Name/Title	Notes of Conversation	Date Dispute Letter Mailed	Time
www.annualcreditreport.com	not applicable					
Equifax	800-525-6285 P.O. Box 740241 Atlanta, GA 30374					
Experian	888-397-3742 P.O. Box 9532 Allen, TX 75013					
Transunion	800-680-7289 P.O. Box 6790 Fullerton, CA 92834					

ACTION PLAN

Federal Trade Commission (FTC) – It is important to file a complaint with the FTC so that your information is part of the Identity Theft Data Clearinghouse, a data bank that documents instances of identity theft in the U.S. and that is used by law enforcement nationwide to assist in the investigation and prosecution of identity thieves. The FTC prefers that complaints be filed online; however, if you do not have computer access, you may file the complaint by telephone or mail. If you file an FTC complaint using their online form, you will be given a printed report that you can send to local law enforcement agencies.

FTC Complaint	Method of Contact	Date Contacted	Contact Person Name/Title	Notes of Contact	Report Taken	Copy Requested	Copy Received	Time
Federal Trade Commission online form: www.ftc.gov/idtheft phone: 877-438-4338 TYY: 866-653-4261 Identity Theft Clearinghouse Federal Trade Commission 600 Pennsylvania Ave. NW Washington, DC 20580	☐online ☐phone ☐mail				☐yes ☐no	☐yes ☐no	☐yes ☐no	

ACTION PLAN

Local Law Enforcement – Notify the local police, sheriff's department, or other local law enforcement agency that you are a victim of identity theft/financial fraud. Ask to make a complaint. Request that an official written incident report be made, and ask for an official copy suitable for sending to creditors. If you have a complaint report from the FTC (*see* p. 6), offer to provide a copy.

Agency	Phone Number	Date Called	Contact Person Name/Title	Notes of Conversation	Report Taken	Copy Requested	Copy Received	Time
Local Police Department					☐yes ☐no	☐yes ☐no	☐yes ☐no	
County Sheriff's Dept.					☐yes ☐no	☐yes ☐no	☐yes ☐no	
Other					☐yes ☐no	☐yes ☐no	☐yes ☐no	

You may also want to report your identity theft to other law enforcement agencies or check verification companies depending on your situation. A few of these options are more fully explained below.

U.S. Postal Inspector – Make a report to the U.S. Postal Inspector if you believe that the identity thief used the United States mail in stealing your identity. Like the FTC, the federal Postal Inspection Service prefers that reports of identity theft be made online. However, if you do not have access to a computer, you may make a complaint by telephone or mail.

Postal Inspector	Method of Contact	Date Contacted	Notes of Contact	Report Taken	Copy Requested	Copy Received	Time
online complaint form: http://postalinspectors.uspis.gov/forms/idtheft.aspx phone: 877-876-2455 mail: Criminal Investigations Service Center ATTN: MAIL FRAUD 222 S. Riverside Plaza, # 1250 Chicago, IL 60606-6100	☐online ☐phone ☐mail			☐yes ☐no	☐yes ☐no	☐yes ☐no	

Your State's Department of Motor Vehicles - If it appears that an identity thief has used your drivers license or has obtained a drivers license using your personal information, you should notify your state's Department of Motor Vehicles.

Department of Motor Vehicles	Date Contacted	Notes of Contact	Report Taken	Copy Requested	Copy Received	Time
Texas, New Mexico, Oklahoma – Go in person to your nearest drivers license office Colorado – Call 303-205-8383			☐yes ☐no	☐yes ☐no	☐yes ☐no	

ACTION PLAN

Check Verification Companies – If an identity thief has passed checks in your name or using your bank accounts, notify the major check verification companies. Make a report of identity theft, and request that they notify retailers not to accept your checks. You may also be able to get a free annual credit report from these companies.

Company	Address/Phone Number	Date Called	Contact Person Name/Title	Notes of Conversation	Date Letter Sent	Time
Telecheck	800-710-9898 P.O. Box 4451 Houston, TX 77210					
Certegy, Inc.	800-437-5120 11601 N. Roosevelt Blvd. St. Petersburg, FL 33716					
Check Rite	800-766-2748 P.O Box 66178 Chicago, IL 60666					
Chex Systems	800-428-9623 12005 Ford Rd. Dallas, TX 75234					

Federal Bureau of Investigation - The FBI investigates cases involving the internet or criminal enterprises with many victims.

FBI	Method of Contact	Date Contacted	Notes of Contact	Report Taken	Copy Requested	Copy Received	Time
online complaint form: www.ic3.gov phone or mail: 202-324-3000 ask for the telephone number and address for the nearest FBI field office	☐online ☐phone ☐mail			☐yes ☐no	☐yes ☐no	☐yes ☐no	

STEP 3 – INVESTIGATE

Next, you need to discover and document how extensively the thief has used your identity. Start by reviewing your last few bank or financial account statements, your credit card bills, and your credit reports. Mark any activity or accounts that do not belong to you. Call SCAN 1-800-262-7771 to find out if a thief has been passing bad checks in your name. Record information about any fraudulent activity or accounts in the following table. Contact law enforcement agencies and credit reporting companies to update your reports with this information.

Company/ Bank/Other Institution Name	Address and Phone Number	Fraudulent Account Number	Amount Involved	Notes	Time

STEP 4 – DISPUTE

Call the fraud investigation or security department of each creditor, company, debt collector, or financial institution associated with each account fraudulently used in your name. Report the identity theft. Request that each fraudulently used account be closed and that the fraudulent accounts be removed from your credit report. File a formal dispute for every account or transaction that is not yours. Request a copy of all applications or business transaction records relating to your identity theft. A form letter is provided in this toolkit. Follow-up each telephone contact in writing, and include a copy of your FTC complaint, police report, and other relevant documents. Send your letters by certified mail, return receipt requested and keep a copy.

Company/ Bank/Other Institution Name	Address and Phone Number	Fraudulent Account Number	Date Called	Contact Person Name/Title	Date of Follow-up Letter	Time

STEP 5 – MONITOR

Keep an accurate record of all people and businesses that contact you regarding your identity theft and any follow-up contacts that you make. Keep a copy of all letters that you send and all information that you receive.

Name/ Title	Company/ Institution/Agency Name	Address and Phone Number	Date of Contact	Notes	Time

STEP 6 – DOCUMENT

Document your out-of-pocket expenses using the form below. Log every penny you spend including cost of telephone calls, copies, postage, and any other expenses you incur. Keep copies of receipts, telephone bills, and other written evidence of your expenses.

Date	Payee	Description	Amount

STEP 7 – PREVENT

Take the following actions to prevent future identity thefts.

Watch your trash. Shred any documents with account or identity information before you throw them away or recycle them. This includes bills, account statements, bank statements, tax returns, and credit card offers.

Watch your mail. If possible, install a mail box that locks so that thieves cannot steal your mail. When you go out of town, contact your local post office and ask that your mail be held until you return.

Consider a credit freeze. A credit freeze makes your credit report unavailable for viewing by many potential creditors unless you take steps to thaw it. It takes about three business days to thaw a credit freeze. When a potential creditor makes a request to see your credit report, the reporting agency notifies the potential creditor that your report cannot be viewed unless you take steps to release your credit report. If you are a victim of identity theft, there should be no charge for placing a freeze on your credit; however, if you are not a victim or if you are requesting a thaw, you may be charged a nominal fee. You must request a credit freeze in writing. Send your request by certified mail. A form letter is included in this toolkit.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790

Opt out of credit card offers. Call 1-888-5-OPT-OUT (1-888-567-8688). Ask to opt out of credit card offers. You will be sent a form. You must fill out and return the form in order for your opt out to take effect.

Get on the federal "no call" list. Visit https://www.donotcall.gov/. You may register both your home and cell phone numbers. After your telephone numbers have been placed in the registry for 31 days, most telemarketers should not call you. Charities, political organizations, and businesses with whom you currently do business are exempt and are allowed to contact you in some cases unless you specifically ask them not to.

Surf Safely. Protect email and other online accounts with passwords. Do not use passwords that are easily guessed, *e.g.*, your name, your birthdate, or your telephone number. Do not keep a list of your passwords on your computer or near your computer. Do not open or respond to emails unless you know the sender. Do not respond to emails asking for passwords or personal information. Find out more at www.OnGuardOnline.gov.

IF YOU NEED ADDITIONAL HELP:

No publication can cover every conceivable situation that may arise for a victim of identity theft or financial fraud. Thieves are very creative, and their victims include both the individuals whose personal information was used fraudulently and the businesses that sold goods, performed services, or issued credit based on a stolen identity. The volume of identity theft cases is huge, and you may encounter resistance from law enforcement agencies that are not equipped to handle the large number of cases being reported to them, from creditors or other businesses that are losing tremendous sums of money to identity thieves and scammers, from credit reporting companies that are committed to serving the businesses that pay them and not the consumer whose identity has been fraudulently used, and from bill collectors whose payment depends on the number of dollars collected on delinquent accounts. You may have questions that are not answered in this publication, or you may need the services of an attorney. Help is available.

If you need additional help resolving issues related to your identity theft or financial fraud, contact the Victims Initiative for Counseling, Advocacy, and Restoration of the Southwest toll free at 1-888-343-4414.