Fact Sheet 100: Financial Identity Theft- The Beginning Steps

Fact Sheet 100A will take you through the more complex step

Written by: Linda and Jay Foley, Identity Theft Resource Center Executive Directors
Resource Material of: www.idtheftcenter.org
Email: itrc@idtheftcenter.org

I'VE BECOME A VICTIM OF IDENTITY THEFT- WHAT SHOULD I DO NOW?

There are three types of identity theft: financial, criminal and cloning. This guide deals with the preliminary steps of financial identity theft.

Other guides on the ITRC website will address other aspects of this crime including *Lost and Stolen Wallets*, *Dealing with Collection Agencies, Check Fraud/Theft, Family Identity Theft, The Evidence Trail and Enhancing Communications with Law Enforcement*.

Partner guide 100A deal with more complex cases of financial identity theft.

GENERAL INFORMATION:

Your rights under the law:

1. To have a police report taken. Many states do not have an express law about this but if you are persistent you should be able to get a report in the jurisdiction where you live.

   With a Police Report you are entitled to:
   - A 7-year Fraud Alert
   - A Credit Freeze in states that have passed that legislation
   - Have inaccurate or fraudulent information blocked from your credit report
   - Receive a copy of all application and transaction records on accounts opened fraudulently in your name (FCRA 609e)

2. Have the account removed from your credit report once you have provided evidence the account is fraudulent. This includes any collection actions or inquiries.

Organizing Your Case:

1. Keep a detailed log in a spiral or composition notebook of all phone calls you receive or make including name of person you spoke with, that person's title, phone number, company name, and what was said during the conversation. Keep loose papers in a notebook or an accordion folder.

2. Send all correspondence to collection agencies, credit issuers and other entities via certified mail , return receipt requested to confirm the letter has been delivered. Keep the postcards that you receive for evidence if necessary.

3. Confirm all conversations and agreements in writing. The person who made an oral agreement with you may not be at that company two months later.

4. Keep all receipts of expenses and copies of correspondence.

The Players:
The biggest waste of time is talking with the wrong people. Keep in mind whenever possible you want to speak with someone on the investigative or fraud side of a company or governmental agency.

- Collection agencies and credit issuers: Customer service helps with billing. You need to speak with a fraud investigator or the legal department if a small company.
- The Social Security Administration does not work on financial identity theft cases. SSA only gets involved through the Office of Inspector General if there is benefit fraud or theft of benefit checks.
- Instead of talking with customer service representatives (credit issuers or collection agencies) request the fraud department of that company.
- Law enforcement: Talk with your local police department or the department where the crime is occurring. The Secret Service and FBI only get involved upon the request of local law enforcement or the U.S. Attorney General's office. Typically these are large money or multiple victim cases or cases involving a cybercrime.
- When mail theft or fraud is an issue, speak only with the Postal Inspector's Office, not a post office manager.
- When speaking to a Department of Motor Vehicles, ask for a fraud investigator.

TERMS you should know:

- FCRA- Fair Credit Reporting Act

- FDCPA- Fair Debt Collection Practices Act- you can get a copy of this at www.ftc.gov

- SSN- Social Security Number

- CRAs- These are the 3 major Credit Reporting Agencies- Equifax, Experian, and TransUnion

- Fraud Alert - This is a statement that instructs credit issuers to contact you prior to approving an application. It is a federal law that they should do so (and you can provide a phone number for someone to call you on) but it is not widely enforced. ITRC has found a fraud alert to be about 65-70% effective. It doesn't affect your credit score but could slow down the credit issuing process (for you and the thief!)

- Security or Credit Freezes- With a freeze, a company may not look at your credit report for the purposes of establishing new lines of credit. Companies you already have an existing relationship with (example: a credit card, loan or utility service) may look at the reports but only to review your credit-worthiness. This is a strong step to take and will affect your ability to get instant credit because it can take up to 3 days to thaw a report. However, it also locks out thieves and that is the purpose. In those states with freezes, there typically is no charge for an identity theft victim with a police report. Some states also allow consumers to buy a freeze. You may thaw your freeze any time you wish to apply for credit but you will need to plan ahead.

- Passwords- Your mother's maiden name should never be used as a password or a word that is easily known to you such as a pet's name. Use an unusual or made-up word such as "banapple." Place

passwords on all bank accounts and credit cards as a proactive prevention action against account takeover.

- FTC- Federal Trade Commission: the governmental agency that oversees identity theft issues. All victims should report their case when they have time to 877-IDTHEFT or to the website: www.consumer.gov/idtheft. The information the FTC collects is vital statistical information and they have a booklet that will also help you.

- EFTA- Electronic Transfer Act - provides consumer protection for all transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers.

STEP ONE: ASSESS THE DAMAGE

1. Stolen credit cards, checks, ATM or debit cards- Contact the financial institution immediately and close the affected accounts. Put passwords on the new accounts. If you never made a copy of your card, you should be able to find a 24/7 phone number on the back of a billing or bank account statement.

2. Account Takeover- If a bank, credit card or debit account has been taken over by another person (charges you didn't make appear on your monthly statement), close the account and open a new one. In most cases you need to notify the company (bank or credit card issuer) within 30 days so act quickly. It is vital to check statements monthly as few financial institutions allow a "grace" period longer than the contractual agreement (on the back of your monthly statement.) Add a password for protection. If checks are involved see Guide 125 for details. A password on the account will also prevent a thief from changing the account billing address or adding a name to the account.

3. Stolen-Lost Wallets- If your wallet has been taken follow the steps in Guide 104

4. If your SSN has been taken, order your credit reports from all three CRAs.
   - The best way to evaluate how bad your case might be is to examine your credit reports. You may call the CRAs 24 hours a day, 7 days a week. At this time, English is the only language that is being used.

   - When ordering your reports, you will have an opportunity to place a FRAUD ALERT on your report. This is an advisory statement and has been found to be only partially effective. The initial fraud alert will only last for 90 days. It is renewable using the same number and procedure you used to place one the first time. It may be extended to 7 years when you write the agency and send a copy of your police report verifying you as an identity theft victim. A fraud alert will not affect your credit score.

   - While the first agency you call will state that they will contact the other two agencies for you, ITRC recommends you empower yourself and make sure the job is done by calling all three agencies. These are separate companies and they may have different information about you causing one of them to not send a report to you. You may also ask that your entire SSN is not on the report mailed to you, a good safety measure. Be sure that you have a locked mailbox in which you receive mail - a good tip for everyone.

   - Finally, you will NOT be speaking with a person. These are automated systems and it is safe to give them your Social Security number. You will be asked a number of questions to try to

confirm if you are you. This is for your security and to ensure they don't send out a credit report to the wrong person. You will have access to a fraud assistance advisor once you receive your reports in the mail.

- Don't give in to the urge to rush into taking a short-cut and buying a tri-report. It cuts you off from the assistance from the CRAs you will need. The reports generated by placing a fraud alert will have different information on them that is not found on reports from commercial reports.

- Should you hear that the information you have provided does not match the information on file, this is a clear indication that there is a problem. This may mean that a thief has used an address with such frequency that it appears to be your primary address. In that case, follow the directions given and mail your request (with the required documents) to the address given, which may vary from state to state.

- During the time the alert is in place, should there be an inquiry into your credit, you should be notified by a phone call from the company making an inquiry confirming with you that you really requested the credit.

The primary contact numbers for the CRAs are:
Equifax: Call (800) 525-6285. TDD: (800) 255-0056
TransUnion: Call (800) 680-7289. TDD: (877) 553-7803. Fraud victims can also email fvad@transunion.com but we recommend that you do not send Social Security numbers via email if avoidable.
Experian: Call (888) 397-3742

5. Review Your Credit Reports Carefully:

The credit reports are divided into five major sections.

The header: This is where you will find your information such as name, date of birth, address and SSN. There may be information about your yearly income.

Section 1: These are the accounts that you have open or have had opened during the last seven years. You will need to verify that it is an account that belongs to you. There are cases where the name of the company will not appear to be familiar. You may need to verify the account by comparing the account number to the number on your credit cards or billing statements.

Section 2: This is the section where inquiries are logged. Inquiries come in several different versions. One is that the company making the inquiry has an application in their possession and wish to verify your worthiness for credit. The other inquiry is by companies that you currently have a financial relationship with and it serves as an account review.

Section 3: This section will display lists of companies that have acquired your information so that they can offer you a pre-approved credit solicitation.

Section 4: Will display a list of other addresses where you have lived.

STEP TWO: TAKE ACTION – RESOLVE THE CASE

1. Contact the Police in the jurisdiction where you live and file a Police Report.

1. Organize Your Case and Taking Notes – see Guide 106 for details (Organizing Your Case)

2. Contact all credit issuers, utility companies and collection agencies that show a fraudulent account. Close the accounts and ask for a FRAUD INVESTIGATOR. Send either our Letter Form 1 or the FTC affidavit (www.consumer.gov/idtheft) along with your police report. While talking with them, place passwords on affected accounts.

3. Get Application and Transaction Records- FCRA section 609e requires companies to send you any documents they have. You will need to send an affidavit and a police report to receive copies of transaction and application records. A copy may also be sent to a designated police department. These documents may contain valuable evidence to point to a thief or help you to clear your name. The credit issuers must send you this information within 30 days. This demand is already part of Letter Form 1. Highlight it if you wish.

4. Once you get the information from the credit issuers, contact the fraud department and point out any errors or fraudulent information. Provide evidence to prove your statements. For example, you could not have bought a shirt in El Paso on October 10th since you were at work in Miami that day and your timecard can prove it. Or- that isn't my handwriting.

5. Contact the 3 CRAs using the form they provide for "correction of errors" and place a "BLOCK" on the fraudulent account. The Fair Credit Reporting Act (FCRA) says they must remove the information unless the credit issuer proves it is a true account. They must also correct any errors including addresses, phone numbers, birthdates and other information provided by the thief.

6. Get Letters of Clearance- keep these for at least 10 years

7. Check your credit reports and make sure all corrections have been made

STEP THREE: COLLECTION AGENCIES

ITRC has written an entire guide for this activity. See Guide 116 for complete details.

STEP FOUR: STOP THE THIEF

1. When you first place your report, you will place a fraud alert. It lasts only 90 days and may be renewed. However, with a police report you can extend it to 7 years. It is advisory in nature only and is not completely reliable since some companies refuse to honor them.
2. If your state has a credit freeze law- look carefully at that option. A list of states (changing all the time) is under "What's New" and the steps to take are in Guide 124. This is a strong step to take and will affect your ability to get instant credit because it can take up to 3 days to thaw a report. In many ways this is the only truly proactive step you can take to stop a thief.

STEP FIVE: REDUCE STRESS

See info Guide 108
Please note that this process takes time. It will not be resolved overnight and you must mentally be prepared to take the necessary time to clear it up. Find a healthy stress reducer and build a support team to help you during this period of your life.

STEP SIX: CHECK ADDITIONAL RESOURCES

Federal Trade Commission- This publication is entitled Taking Charge. You can get a copy sent to you or download this document at http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm . You can also call them at 877-IDTHEFT and read about more information at www.consumer.gov/idtheft

www.identitytheft.org- This resource book and video was written by an attorney and id theft expert, Mari Frank. Please remember to indicate that the Identity Theft Resource Center referred you. It is full of letter forms, good advice and inspiration.

To report fraudulent use of your checks

- CheckRite: (800) 766-2748
- Chexsystems: (800) 428-9623
- CheckCenter/CrossCheck: (800) 843-0760
- Certigy/Equifax: (800) 437-5120
- International Check Services: (800) 526-5380
- SCAN: (800) 262-7771
- TeleCheck: (800) 710-9898

California Office of Privacy Protection, (Dept. of Consumer Affairs), (866) 785-9663. Web: www.privacy.ca.gov.

Florida AG ID Theft Hotline: www.myfloridalegal.com/identitytheft or 866-966-7226

FBI Internet Fraud Complaint Center, Web: www.ifccfbi.gov