ITRC Fact Sheet 100
Financial Identity Theft: The Beginning Steps

This guide includes:

- What you need to know before you start
- Assessing the Damage and Beginning Steps
- Continuing the Recovery Process
- Collection Agencies
- Terms You Should Know

WHAT YOU NEED TO KNOW BEFORE YOU START:

Your rights under the law:

- To have a police report taken. Many states do not have a specific 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 the states that have adopted this procedure into law
  - 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 Section 609e (http://www.ftc.gov/os/statutes/031224fcra.pdf)) Refer to LF 100-1 (/Letter-Forms/lf100-1.html)
- To 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: (See ITRC Fact Sheet FS 106 (/Fact-Sheets/fs106.html) for more detailed information)

- Keep a detailed log in a spiral or composition book of all phone calls you receive or make, including the names or people, their title, phone numbers, company name, and notes about the conversation. Keep loose papers in an accordion folder (or something similar).
- Mail all correspondence "certified, return receipt requested" to confirm it has been delivered. Keep the postcard you receive for evidence, if necessary.
- 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.
- Keep all receipts of expenses and copies of correspondence.

Working with the Right People:

The biggest waste of time is talking with the wrong people. Keep in mind that whenever possible you want to speak with someone on the investigative or fraud side of a company or governmental agency. Customer service is seldom the correct department. They only deal with billing and service issues.

- The Social Security Administration does not work on financial identity theft cases. SSA only gets involved through their Office of Inspector General if there is benefit fraud or theft of benefit checks ITRC Solution SN 27 (/Solutions/sn-27.html) - Someone Working as You.
- Talk with your local law enforcement agency and file an identity theft report with them.
- The Secret Service and FBI only get involved upon the request of local law enforcement or the U.S. Attorney General's Office.
- 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.

ASSESSING THE DAMAGE AND BEGINNING STEPS

- 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 the card, you should be able to find a 24/7 phone number on the back of a billing or bank account statement.
- 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 statements), 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 ITRC Fact Sheet FS 126 (/Fact-Sheets/fs-126.html) - Checking Account Takeover and Check Fraud for details. A password on the account may help to deter a thief from changing the billing address or adding a name to the account.
- Stolen-Lost Wallets - If your wallet (or PDA) has been lost or stolen, follow the steps in ITRC Fact Sheet FS 104 (/Fact-Sheets/fs-104.html)
- If your Social Security Number (SSN) has been taken, order your credit reports from all three CRAs. The primary contact numbers are:

1. Equifax: Call (800) 525-6285. TDD: (800) 255-0056
2. TransUnion: Call (800) 680-7289. TDD: (877) 553-7803. Fraud victims can also email fvad@transunion.com (mailto:fvad@transunion.com)
3. Experian: Call (888) 397-3742

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 being used.

- When ordering your credit reports, you will have an opportunity to place a FRAUD ALERT. The initial fraud alert will only last for 90 days. It is renewable, using the same phone number and procedure you used to place your first fraud alert. 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.
- Please understand 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 have access to a fraud assistance advisor once you receive your reports in the mail.
- While the first credit reporting 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.

- When placing the fraud alert, 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 requested documents) to the address given, which may vary from state to state.
- 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.

Don't rush into taking a short-cut and buying a "tri-report" (three-in-one report). It could cut you off from fraud investigators at the CRAs. The reports generated by placing a fraud alert will have additional information that is not on a "tri-report", such as contact information for companies with open accounts in your name.

- Review Your Credit Report Carefully: See ITRC Fact Sheet FS 128 (/Fact-Sheets/fs-128.html) - How to Read Your Credit Report. (Credit reports are divided into five major sections. These sections may not be in the same order as listed below.)
- The header: This is where you will find your information such as name, date of birth, address, Social Security Number and spousal information. There may be information about your employer and/or previous addresses.
- Section 1: These are the accounts that you have open or have had opened during the last seven years. Make sure all accounts belong to you. There may be cases where the name of the company will not be familiar; they may be a part of a parent company.
- 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 card solicitation.
- Section 4: Will display a list of previous addresses where you have lived (if not in the header section).
- Section 5: Consumer alert information. This is where information about fraud alerts and other information from the consumer are placed.

CONTINUING THE RECOVERY PROCESS

- Contact the law enforcement agency in the jurisdiction where you live and file an Identity Theft Report. You will need to obtain a physical copy of this report, not just a case number. This is a critical document required to clear your name.
- Contact all credit issuers, utility companies and collection agencies that have opened a fraudulent account. Speak only to a FRAUD INVESTIGATOR. Then:
  - Request to close the account(s)
  - Request the company mail you their fraud packet or an address to send either our ITRC Letter Form LF 100-1 (/Letter-Forms/lf100-1.html) or the FTC Identity Theft Report: https://identitytheft.gov/ (https://identitytheft.gov/) along with your police report. Always mail out certified with return receipt. If the company does not request document information from you, then they are most likely not clearing the account.

- Inform then that they may not sell, share, exchange, give away, donate, and/or trade this account to any other entity for the purposes of collection while it is under investigation.
- Get Application and Transaction Records - FCRA section 609e (http://www.ftc.gov/os/statutes/031224fcra.pdf) requires companies to send you any documents they have. You will need to send an affidavit and/or a police report to receive copies of transaction and application records. A copy of the transaction information may also be sent to a designated police department. These documents may contain valuable evidence to point to the thief or help you to clear your name. The credit issuers must send you this information within 20 days (FCRA/FACTA). This demand is part of ITRC Letter Form LF 100-1 (/Letter-Forms/lf100-1.html) - Initial Victim Statement.
- Once you get the information from the credit issuers, contact the investigating law enforcement agency and provide the information to them.
- Contact the three CRAs using the form they provide for "correction of errors." FCRA (http://www.ftc.gov/os/statutes/031224fcra.pdf) states they must remove the information unless credit issuers prove it is a true account. Ultimately the credit issuer must be the one to remove fraudulent accounts from your credit report permanently. The credit issuers also must correct any erroneous information including addresses, phone numbers, birthdates and other information falsely provided by the thief.
- Get Letters of Clearance from the credit issuers. (Refer to ITRC Letter Form LF 100-2 (/Letter-Forms/lf-100-2.html).) Keep these for at least 10 years.
- Check your credit reports and make sure all corrections have been made.
- If your state has a credit freeze law (see State and Local Resources (/map.html)) - look carefully at that option. Refer to ITRC Fact Sheet FS 124 (/Fact-Sheets/fs-124.html) - Credit Freeze and Fraud Alerts.

COLLECTION AGENCIES:

ITRC has written an entire guide for this activity. See ITRC Fact Sheet FS 116 (/Fact-Sheets/fs-116.html) - Collection Agencies and Identity Theft for complete details.

TERMS you should know:

FCRA - Fair Credit Reporting Act

FDCPA - Fair Debt Collections Practices Act: you can get a copy of this at www.ftc.gov (http://www.ftc.gov/)

SSN - Social Security Number

Credit Reporting Agencies (CRAs) - The Credit Reporting Agencies (Equifax, Experian, Transunion) are for-profit companies that are a necessary component of the identity theft remediation process. The ITRC does not recommend consumers contact these entities as an endorsement of their goods, products or services, but rather as a necessary part of the mitigation process. There is no alternative for following this process. The ITRC is able to provide it's free services due to the financial support of our corporate sponsors. We currently have the following Credit Reporting Agencies providing financial support to the ITRC: none.

FTC - Federal Trade Commission is 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: https://identitytheft.gov/ (https://identitytheft.gov/).

EPTA - 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.

Fraud Alert - A fraud alert heightens credit issuer's awareness that they need to authenticate and verify the applicant before issuing credit. However, it is not 100% reliable and not always heeded. They don't affect your credit score but may slow down the application process. When you initially place a fraud alert as a potential victim of identity theft, you will be offered a free credit report as part of your federal rights. This is not the same as the free federal annualcreditreport.com (please refer to ITRC Fact Sheet FS 125 (/Fact-Sheets/fs-125.html)).

Security or Credit Freeze - 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 view your reports but only to review your credit-worthiness. Placing a freeze is a strong step to take and will affect your ability to get instant credit since it can take up to three days to lift the freeze from (unfreeze) your credit report. However, it also locks out thieves. In those states with freeze laws, most state that victims with a police report get this service for free. Most states also allow the consumer to buy a freeze. You may lift your freeze anytime you wish to apply for credit but you will need to plan ahead. See ITRC Fact Sheet FS 124 (/Fact-Sheets/fs-124.html) for more information or our State & Local Resources (/state-resource-map) to see if your state has a freeze program.

Passwords - a password should not be a mother's maiden name. If the bank insists on a mother's maiden name then make one up. A strong password should be more than 8 characters in length, and contain both capital letters and at least one numeric or other non-alphabetical character. Use of non-dictionary words is also advised. Place passwords on all bank accounts and credit cards as a proactive prevention action against account takeover.