



- Place a fraud alert on your credit report at all three major credit reporting agencies (CRAs). You are entitled to get a credit report at no charge whenever you place a fraud alert. Technically, reporting to one of the three CRAs should be enough, because the first one contacted is required to notify the other two. However, if you have not received a written response from all three within 7 - 10 business days, you should contact any that have failed to contact you.
- Check the credit report that you get for free when you place the fraud alert. Look for new accounts that you did not open, renewed activity on dormant accounts, as well as any variations to your name, address, place of employment and Social Security number. In addition, look in the credit inquiry section for recent checks on credit. This can give law enforcement vital clues as to the current acts of the identity thief.
- Contact your existing creditors' fraud departments alerting them to the crime and misuse of your accounts and, for credit cards, ask them to change your account numbers. Closing accounts can damage credit ratings - and the better avenue may be to change credit card account numbers. However, when the thief is able to continue to pretext the institution and obtain your new account numbers, it may be better to close the account and open a new account at a different institution.
- Contact companies where the thief opened new accounts in your name and ask them to close the accounts and absolve you of the debts.
- Maintain log of contacts with creditors and financial institutions. A sample log template can be found at <http://www.ftc.gov/bcp/edu/resources/forms/chart-course-action.pdf>.
- Place a security freeze on your accounts (if you do not think that fraud alerts provide enough protection).
- File an online complaint at the FTC and print out an Identity Theft Victims' Universal Complaint to help you develop an Identity Theft Report and to assist law enforcement in determining if your case is part of a larger conspiracy. Visit <https://www.ftccomplaintassistant.gov/> or <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html>.
- In your FTC complaint, list all inaccurate information on your credit report that was caused by your identity crime, such as unauthorized accounts, and the institution and billing address associated with the account. Also list what you know about how and where the thief used your information, anything you know about the thief, and any events or incidents where/when your personal information might have been compromised.
- Bring your printed FTC Universal ID Theft Complaint to your local law enforcement agency, sign it in the presence of an officer, and ask the officer to sign it and put your report number on it.
- Send a written dispute letter and a copy of your Universal ID Theft Complaint with your police report attached to the companies where your identity has been used or impacted, such as the credit reporting agencies, the companies where accounts were opened in your name or the thief misused your accounts, and debt collectors who have contacted you. Sample letters can be found at <http://www.ftc.gov/bcp/edu/microsites/idtheft/tools.html> and www.privacyrights.org.