Medicaid/Medicare, insurance, or State benefits

Steps to Take Immediately - Follow each step below to help recover from the damage caused by identity theft.

If you have been notified by a medical service provider, insurance company, a state or federal government agency, or if you have received calls from a collection agency about services or benefits that you are not aware of, then a thief may be using your identity to obtain benefits. If you identify benefits identity theft, you should order copies of your records to check for mistakes. You have the right to see your records and have them corrected.

Step 1: Organize Your Case

In order to help law enforcement investigate your case, and to help recover from the damage caused by an identity theft, you should:

- Keep a detailed list of all phone calls you receive or make related to your identity theft incident including name of the person you spoke with, that person's title, phone number, organization name, and what was said during the conversation.
- Make sure you keep a copy of all medical, government documents, financial statements, police reports, affidavits, credit reports, collection letters, and all other documents related to your incident.
- Keep all loose documents in a notebook or accordion folder.
- Send all correspondence using certified mail with return receipt requested.
- Keep track of your time and any expenses you incur in the event you are given the opportunity to be reimbursed for your costs through court ordered restitution.
- Use ID Theft Central's Contact Tracking Sheet to keep track of the people you speak with regarding your identity theft incident.

Step 2: Contact the benefits provider

Contact the benefits provider and inform them of the situation. Request, in writing, copies of all documentation associated with the fraud, including the fraudulent application. Submit any documentation received to the investigating law enforcement agency. Contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and location where a thief may have used your information. If a medical provider refuses to provide you with copies of your records because it thinks that would violate the identity thief's privacy rights, you have a right to appeal their decision. Contact the person the provider lists in its Notice of Privacy Practices, the patient representative, or the ombudsman.

Explain your situation and ask for your records. If after 30 days, your provider has not provided you with your written request for your records, you may file a complaint with the U.S. Department of Health and Human Services' Office for Civil Rights.

Step 3: Get an Accounting of Disclosure

Request from each of your health plans and medical providers a copy of the "Accounting of Disclosure" for your medical records. The accounting is a record of who got copies from your provider. The law allows you to order one free copy of the accounting from each of your medical providers every 12 months. The accounting shows a listing of all disclosures of an individual's protected health information (PHI) made by the medical provider or its business associates for up to six years preceding the request. Note that the accounting may exclude disclosures made by the medical provider to carry out treatment, payment and health care operations, which constitute the overwhelming majority of communications. Covered entities have 60 days to meet your request. An additional 30-day extension beyond that is allowed if the requester is provided with a written explanation for the delay.

Individuals are entitled to a single accounting every 12 months without charge. Additional requests within a 12-month period may be subject to a "reasonable, cost-based fee." As with other HIPAA rights, institutions must designate a privacy office/officer to handle disclosure accounting requests, and must document the processing of any requests that are received.

Step 4: Ask for corrections

Write to your health plan and medical providers and explain which information is not accurate. Send copies of the documents that support your position. You can include a copy of your medical records and circle the disputed items. Ask the provider to correct or delete each error. Be sure to keep the original documents. All correspondence should be sent by certified mail, and ask for "return receipt," so you have records of what the plan or provider received. Mistaken information in your medical records must be changed by the health plan or medical provider that made the mistake. You should ask the medical or benefit provider that made the mistake to contacts labs, other health care providers, and anyone else that might have gotten the wrong information. If your health care or benefits provider refuses to make the changes you request, ask it to include a statement of your dispute in your record.

Step 5: File an identity theft report at ID Theft Central or with your local police department

Once you have confirmed unauthorized use of your information to obtain benefits in your name, file a report at ID Theft Central or with your local police department.

- Report the crime at ID Theft Central.
- Contact your local police department and report the crime by calling their non-emergency number and explain to them what happened.
- Make sure your police department issues you a police report with a case number.
- You can use their police report to obtain a Consumer Credit Freeze from the credit reporting companies at no cost. You can also use the report to help clear the damage caused by the theft.

Step 6: Send a copy of your police report to your health insurer's or benefits provider's fraud department.

Step 7: Initiate a 90 Day Fraud Alert

To help protect your personal identifying information from being used to obtain new benefits by a thief, initiate a 90 Day Fraud Alert. A 90 Day Fraud Alert notifies potential credit grantors to verify your identification before extending new credit in your name.

You only need to contact one of the three credit reporting companies to set up a Fraud Alert for all three.

- You will receive a free copy of your credit report from all three credit reporting companies.
- You will receive a notice of your rights as an identity theft victim.
- A 90 Day Fraud Alert stays on your file for at least 90 days and can be renewed.
- A Fraud Alert may slow down your approval process for new credit.

To place a Fraud Alert, you may be required to provide appropriate proof of your identity, which may include copies of your Social Security card, driver's license, and/or utility bills. You may cancel the fraud alerts at any time.

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
P.O. Box 740250
Atlanta, GA 30374-0241
1-800-525-6285
www.equifax.com

Transunion
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289
www.transunion.com

You Might Also Like

Consumer Credit Freeze

How to use a Police Report to help recover from identity theft

How to use an identity theft affidavit to help recover from identity theft