

שמתחילת המעשה וכל המעשה הזה
הוא כפי שראינו בפרק הקודם
שהוא כפי שראינו בפרק הקודם
שהוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

והוא כפי שראינו בפרק הקודם

TABLE OF CONTENTS

Identity Theft	1-3
Medical ID Theft	4
Privacy & Security Tips	5
Smartphones/Portable Devices	5-6
Vacation & Travel	7
Concerning Medical ID Theft	8-9
Sample Forms & Letters	10
Certified Letter to Merchants	10
Certified Letter to Credit Bureaus	10
Certified Letter to Bank Manager	11
Certified Letter to Check Guarantee Services	11
Certified Letter to County CourtHouse	12
Certified Letter to U.S. Department Of State	12
Complaint to the Federal Trade Commission about a Credit Bureaus Failure to Remove Fraudulent Accounts	13

Identity Theft

The following guidelines and forms are intended to assist you in the event that you have, (or suspect that you have) become a victim of identity theft. Note - quick reaction is key. The sooner you take steps to mitigate any possible damage, the less likely you will suffer losses.

1. If you suspect a crime may have been committed, immediately file a police report.

- Insist that you be given a report number and a copy of the report. (You may need these later as proof.)
- If you are married and are unsure which spouse was victimized, insist that the police report include both spouse's names and information. Note - If the police only take reports about identity theft on-line or by telephone, the FTC Identity Theft
- Complaint Form (see below) has a special section for automated police reports. Complete the "Automated Report Information" section. Attach a copy of any filing confirmation received from the police. If you have a choice, however, file your police report in person and be sure to obtain the report number.
- It is also recommended that keep a copy of your police report with you at all times - until all issues have been resolved.

2. Contact the fraud departments of each of the three major credit bureaus:

- Ask that they immediately place a 90-day Fraud Alert in your credit file and a statement that all creditors need to call you to authorize any new accounts.

Equifax (www.equifax.com)	800 525-6285
Experian (www.experian.com)	888 397-3742
Transunion (www.tuc.com)	800 680-7289

- For extra precaution, after you receive your police report, follow the procedures to place an extended 7 year fraud alert on your credit file.
- For even further protection, follow the procedures to place a security freeze on your credit file.

3. Immediately obtain a copy of your credit file from all 3 credit bureaus to check it for accuracy.

- When you receive your credit report, carefully and thoroughly review it.
- Demand that all fraudulent information be removed.
- Obtain the name, address, and direct phone number of each credit bureau representative that you work with, and follow up in writing (see sample in this guide).

Identity Theft

4. Access the FTC Identity Theft website at: www.ftc.gov/idtheft

- Complete and submit online the Identity Theft Complaint Form
- Download the Identity Theft Affidavit. Complete form as soon as possible. This form can be used when notifying and corresponding with creditors and companies that an account was fraudulently opened or used in your name. (This form is for your records - do not send to the FTC)

5. Immediately close any accounts that you know, or believe, have been tampered with or opened fraudulently.

- The Fair Credit Billing Act requires that you follow-up in writing, so be sure to ask for the name of the person you speak with.

6. If you are contacted by a company demanding payment for a purchase that you know nothing about, gather as much information as you can, such as:

Date of transaction	Dollar amount
Type of payment	Address on file
Account number	Was a credit application submitted? (request a copy)

7. Explain to the company what has happened. Be sure to use the phrase “Identity Theft”.

- Ask that your name be removed from their list of delinquent debtors and from the report filed with the credit bureaus.
- Follow up with a letter (see sample in this guide).
- Copies of all creditor/merchant letters should be sent to the three major credit bureaus.

8. Keep a file of all of your correspondence and enclosures.

9. If you open a new account:

- Use new (PIN numbers) and passwords
- DO NOT use easily available information, such as the last four digits of your SSN, or your birth date, or your mother’s maiden name.
- Some of the worst passwords are: (password; 12345678; qwerty; abc123)

10. If necessary, contact the major Check-Guarantee Agencies.

- Inform them that you are a victim of Identity Theft and that no checks in your name should be guaranteed. Insist that any negative information due to fraudulent checks be purged.
- Follow up with both a letter (see sample in this guide) and a copy of your police report. Contact information:

Chexsystems	800 428-9623	N.P.C.	800 526-5380
Telecheck	800 710-9898	Equifax	800 909-7304
Scan	800 262-7771		

Identity Theft

- If you discover that any fraudulent checks have been passed, contact the banks in question, speak with the manager and explain that you are a victim of identity theft.
- Again, ask that they refrain from using your name on reports to the credit bureaus and check-guarantee agencies. Follow up with both a letter (see sample in this guide) and a copy of the police report.

11. If necessary, contact your local Department of Motor Vehicles.

- Explain that you are a victim of identity theft and that you will need a new driver's license.
- Verify that your old license has been voided in their records.

12. If necessary, contact your local Social Security Office.

- Explain that you are a victim of Identity Theft and that you may need a new Social Security Number issued.
- Be sure to have a copy of the police report with you.
- When opening a new credit account, do not allow old accounts to be transferred to your new SSN. This may result in negative information creeping into your new credit bureau file.

13. To determine if there are any civil and/or criminal actions pending against you, utilize background search services, such as "BackgroundCheckGateway.com".

14. If necessary, call all applicable courthouses, explain the situation, and have them search for any court records under your name.

- If you find judgments against you, ask that they be vacated.
- You will need to send a letter (see sample below) and copies of your police report and credit bureau documents.

15. For Passports, contact the U.S. Department of State regarding your Passport (see sample below)

- Explain your situation (be sure to include a copy of the police report).
- You will be requesting that any fraudulently obtained Passport in your name be canceled immediately. The address is:

U. S. State Department
Attn. Passport Services
1111 19th Street, NW, Ste. 500
Washington DC 20522

16. Order copies of your credit report periodically to ensure that negative information has not been allowed back into your record.

- If this happens, send a letter (see sample in this guide) to the credit bureau.
- Also included is a sample letter to the Federal Trade Commission. They are the agency responsible for regulating credit bureaus.

Medical Identity Theft

- 1. Exercise your rights under HIPAA - The Health Insurance Portability and Accountability Act - to correct errors in your medical and billing records.**
- 2. HIPAA gives you the right to receive copies of your records usually within 30 days after you ask for them.**
 - You will likely have to complete a form and pay a fee to get your copies.
 - Remember that you have the right to know what's in your file. If your request is denied, you can appeal by contacting the person identified in the provider's Notice of Privacy Practices or the patient representative or ombudsman.
 - If you are still denied, file a complaint with the U.S. Department of Health and Human Services' Office for Civil Rights, at www.hhs.gov/ocr.
- 3. Write to your health plan or provider detailing any information that seems inaccurate.**
- 4. Include copies (keep the originals) of any document that supports your position.**
- 5. Identify each item in your record that you dispute.**
- 6. State the facts and your reasons for disputing the information.**
- 7. Request that each error be corrected or deleted. (You may want to enclose a copy of your medical record with the items in question circled.)**
- 8. Send your letter by certified mail, and ask for a "return receipt,".**
- 9. Generally, your health plan or medical provider must respond:**
 - The creator of the information is obligated to amend the inaccurate or incomplete information.
 - It also should notify other parties, like labs or other health care providers, that may have received incorrect information.
- 10. If an investigation does not resolve your dispute with your plan or provider, you can ask that a statement of the dispute be included in your record.**

Privacy & Security Tips

Smartphones/ Portable Devices

1. Use a screen-lock

- Set up a screen lock so your device cannot be accessed or used without a password of some sort.
- Alphanumeric passwords are more effective.
- Make sure the screen locks automatically after 1 - 5 minutes of non-use.

2. Regularly install manufacturer's updates

- Most device system updates include enhancements to data security.

3. Treat your mobile device like a PC

- As with a PC, be sure to have the proper firewalls, anti-virus, anti-malware and anti-spyware protections in place.
- Spyware can intercept email and text messages that go in and out of the device, and can remotely turn it on and listen in on conversations.

4. Be prepared

- Install software so in case of loss, you can lock, track or remotely wipe the data.
- Regularly back up the stored information for retrieval in case of loss.

5. Be responsible when down-loading apps

- Research online to see if the app you are about to download has been reviewed by reputable sources.
- Don't download apps from untrusted sources
- Apps that haven't been approved by an official app store are more likely to be invasive.
- Read the "Permissions" screen when you download and install any apps.
- Many apps will advise you that they are accessing your contacts, call history, location, etc.
- Be sure to note if that your data is going to be stored by the app, delivered by the app to the app vendor, or sent to third-party companies for other uses.
- If you download an app but stop using it, get rid of it. Do not leave it on your device.

6. Be careful of attachments

- Be careful about opening e-mail attachments sent to you by people you do not know.
- Take the same precautions on your device that you would on your home computer.
- This also applies to downloads from web sites, social networks, shortened URLs, etc.

7. Manage your location settings

- Most portable devices come with either GPS or carrier-aided location tracking features.
- There are thousands of apps that want to access your location data.
- You can control your location settings in these apps individually in most cases.
- If you want to make your location as secret as possible, turn off all forms of location.

Privacy & Security Tips

Smartphones/ Portable Devices

8. Be aware of your surroundings

- Take care to conduct sensitive business on your device in a way that prying eyes or ears can't see or hear.
- Be discrete. Keep private conversations in front of people to a minimum.

9. Do not leave your device unattended

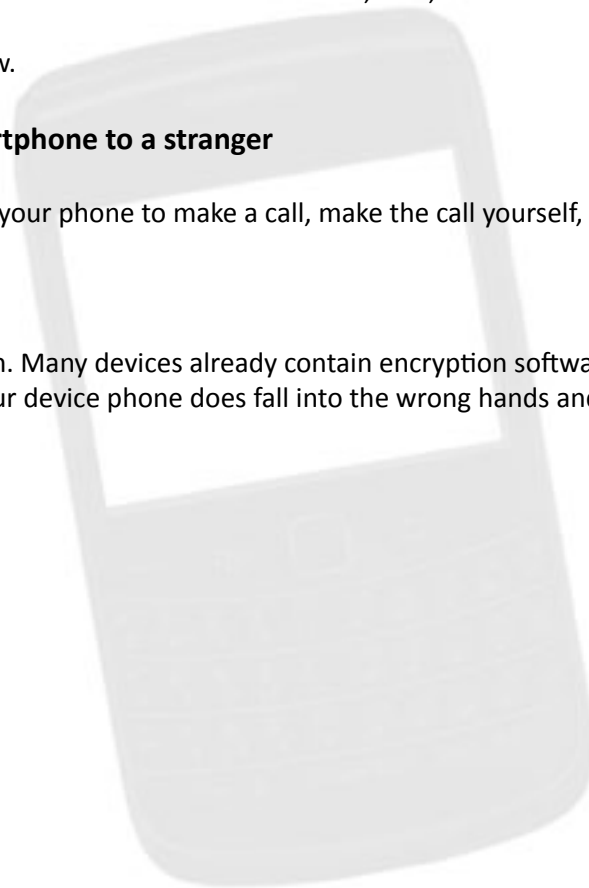
- Don't leave your device where it can be grabbed by a stranger.
- Popular places to lose portable devices include restaurants, bars, health clubs - any place where it might be left on a table
- Keep your device out of view.

10. Do not ever hand your smartphone to a stranger

- If a stranger asks to borrow your phone to make a call, make the call yourself, and put it on speakerphone.

11. Encrypt Device's Data

- Consider utilizing encryption. Many devices already contain encryption software - it just needs to be activated.
- This ensures that even if your device phone does fall into the wrong hands and is accessed, some level of protection remains.



Privacy & Security Tips

Vacation and Travel

1. Do not advertise that you are going on vacation.

- Be cautious of what you share on social networking and check-in sites.
- Do not broadcast your schedule or your travel plans.

2. Hold your mail and newspaper.

- Suspend delivery of your newspaper or ask a trusted neighbor to hold it as well as your mail for you.
- Mail left in an unlocked mailbox is a serious identity theft risk.

3. Thoroughly clean-up your purse or wallet.

- Inventory and retain only what is absolutely necessary for your trip.
- Remove any unnecessary credit cards, and other unneeded documents that could compromise your identity if lost or stolen.
- NEVER carry your Social Security Card with you. Memorize it immediately.
- Do not take your checkbook or debit cards while on vacation.
- Use credit cards or traveler's checks instead.
- If possible, make a list or photocopy what remains in your purse or wallet, and keep it in a secure location at home.

4. If using an ATM:

- Use ATM machines found at banks, trusted hotels, in well-lit areas.
- Check to see if someone has tampered with the machine - or any point-of-sale terminal.

5. Be wary when going on-line.

- Many Wi-Fi hotspots are unsecured and unencrypted.
- Avoid accessing any sensitive information from a public computer.

6. Physically secure your belongings.

- Use the hotel room safe.
- Never leave your purse or wallet anywhere unattended.

Privacy & Security Tips Concerning Medical Identity Theft

1. You may be a victim of Medical Identity Theft if:

- You order a copy of your credit report and see medical collection notices you do not recognize;
- You try to make a legitimate insurance claim and your health plan says you have reached your limit on benefits
- You are denied insurance because your medical records reflect a condition you do not have.
- You get a bill for medical services you did not receive;
- A debt collector contacts you about a medical bill you do not owe.

2. Medical identity theft may change your medical and health insurance records: Every time an identity thief uses your medical identity to get care, a health record is created with the imposter's medical information that could be mistaken for your medical information – For example:

- A diagnosis of an illness, allergy or condition you do not have
- Test results that are not yours
- An inaccurate history of drug or alcohol abuse
- A different blood type

Any of these could lead to improper diagnosis and/or treatment, which in turn, could lead to injury, illness or worse.

Prevention Tips for Medical ID Theft

1. Safeguard your medical and health insurance information.

- If you are asked on-line to share personal or health information like your SSN, insurance account information, or any details of your health or medical conditions, ask:
 - Why is it needed?
 - How it will be kept secure?
 - Will it be shared?

****Remember - e-mail is usually not secure.****

2. Verify the source before sharing information.

- Do not share personal or medical information (by phone, by mail, on-line, in-person) unless you have initiated the contact and you are sure you know who you're dealing with.

3. Look for indicators that a site is secure, like a 'lock' icon on the browser's status bar or a URL that begins "https:" (the "s" is for secure).

Privacy & Security Tips Concerning Medical Identity Theft

4. Look for and carefully read health/medical website privacy policies

- How will the site operator maintain the accuracy of your personal and health information?
- How will they secure it?
- Who has access to it?
- How are they going to use your information?
- Are they going to share it with third parties?
- Who are those third parties?

5. When disposing of any personal and health records

- Shred your health insurance forms and prescription and physician statements.
- Destroy the labels on your prescription bottles and packages before you throw them out.

6. Carefully read all of the Explanation of Benefits (EOB) statements that you receive. Look for:

- The name of the provider
- The date of service
- A description of the service provided

If there is a discrepancy, immediately contact your health plan to report the problem.

7. Review your medical and health insurance records regularly.

8. You can also obtain a copy of the accounting of disclosures of your medical records from your health plan and providers.

- It will help you follow the trail of your information and identify who has incorrect information about you.
- By law, you can order one free copy of the accounting from each of your providers every 12 months.
- The accounting is a record of:
 - » The date of the disclosure;
 - » The name of the person or entity who received the information;
 - » A brief description of the information disclosed;
 - » A brief statement of the purpose of the disclosure or a copy of the request for it.

SAMPLE FORMS AND LETTERS

SAMPLE LETTER 1

CERTIFIED LETTER TO MERCHANTS

Date
Your Name, Address & Phone Number
Re: Identity Theft

Dear Sir/Madam:

Pursuant to our recent conversation on (date), this is to confirm that, as I indicated, a fraudulent account was opened / (fraudulent charges were incurred) in my name with your firm.

Please close this account immediately and discontinue reporting it to the credit bureau.

I am enclosing a copy of the police report I filed in this matter. Please contact me at once if there you have any problems or questions.

I greatly appreciate your help.

Sincerely,

Your Name (Signature)
Fraudulent Account Number:

SAMPLE LETTER 2

CERTIFIED LETTER TO CREDIT BUREAUS

Date
Your Name, Address & Phone Number
Your birth date & social security number
RE: Identity Theft

Dear Sir/Madam:

Per my recent conversation with (name), I have been a victim of identity theft and accordingly have requested that my credit file be corrected by deleting the fraudulent accounts listed below. I have been assured that a fraud block will be placed on my account.

I would like to receive a copy of my corrected credit report as soon as possible.

Sincerely,

Your Name (Signature)
LIST OF FRAUDULENT ACCOUNTS:

SAMPLE FORMS AND LETTERS

SAMPLE LETTER 3

CERTIFIED LETTER TO BANK MANAGER

Date

Your Name, Address & Phone Number

Dear Sir/Madam:

This is a follow up to our recent conversation. As I indicated by phone, I am a victim of identity theft. It has come to my attention that the identity thief opened a checking account in my name at your bank, that is, Account Number [include account number, if available].

I have no responsibility for this account and request that it be closed immediately. I also request that you do not report any non sufficient funds checks to check guarantee services or credit bureaus.

For your information, I am enclosing a copy of the police report I filed in this matter.

I sincerely appreciate your help.

Name (Signature)

SAMPLE LETTER 4

CERTIFIED LETTER TO CHECK GUARANTEE SERVICES

Date

Your Name, Address & Phone Number

Re: Identity Theft

Dear Sir/Madam:

I have been a victim of identity theft and the following fraudulent checking account was opened in my name. [Provide bank name, address, and account number.]

Please remove my name and any other identifying information from your system immediately.

For your information, I am enclosing a copy of the police report I filed regarding this matter. Your cooperation is sincerely appreciated. Please contact me if you have any questions.

Sincerely,

Your name (Your Signature)

SAMPLE FORMS AND LETTERS

SAMPLE LETTER 5

CERTIFIED LETTER TO COUNTY COURTHOUSE

Date
Your Name, Address & Phone Number
Re: Identity Theft

Dear Sir/Madam:

Per our recent conversation, I have found that there are civil judgments in your files against me. However, as I indicated, I have been victimized by an identity thief and am in fact not the person named in these judgments.

Accordingly, I hereby request that the judgments listed below be vacated immediately and removed from your files.

For your information, enclosed is a copy of the police report I filed regarding this matter. I sincerely appreciate your help. Please contact me if there are any questions or problems whatsoever.

Sincerely,
Your Name
(Signature)
LIST OF JUDGMENTS:

SAMPLE LETTER 6

CERTIFIED LETTER TO U.S. DEPARTMENT OF STATE

Date
Your Name, Address & Phone Number
Re: Identity Theft

Dear Sir/Madam:

This is to notify your office that I have been victimized by an identity thief who may attempt to obtain a fraudulent passport in my name.

Please enter this information into your system and notify me if this individual is apprehended.
For your information I am enclosing a copy of the police report I filed regarding this matter.

Please cancel my current passport.

Sincerely,
Your Name
(Signature)

SAMPLE FORMS AND LETTERS

SAMPLE LETTER 7

LETTER OF COMPLAINT TO THE FEDERAL TRADE COMMISSION ABOUT A CREDIT BUREAU'S FAILURE TO REMOVE FRAUDULENT ACCOUNTS

Date

Your Name, Address & Phone Number

Re: Complaint

Dear Sir/Madam:

I have been a recent victim of identity theft.

On (date of contact) I contacted (name of credit bureau) and requested that fraudulent accounts be removed from my file. I spoke with (name of credit bureau representative).

However, I subsequently discovered that my request had not been complied with. I then recontacted the bureau and again requested compliance with my request. The bureau again failed to comply.

This non compliance is causing me serious personal and financial hardship. I am therefore requesting that your agency assist me in this matter.

Thank you in advance for any help you can provide me in resolving this.

Sincerely,
Name
(Signature)