

ID THEFT PACKET & INFORMATION

You are a victim of identity theft; there are a number of important steps for you to follow. Be prepared to document all unauthorized transactions and to be patient—the process can take a number of months.

In most cases, the uniform officer that filled out a report is not the investigating officer. Your report number is:_____.

The following information in this packet will assist you in contacting various agencies. Complete the necessary forms and document everything you do. This case will be assigned to an investigator. In a short time he or she will be contacting you for an interview. It is important that you following the instructions in this packet and make every effort to complete each form.

Step 1 – Contact your bank and other credit card issuers. If the theft involved existing bank accounts (checking and or savings accounts as well as credit or debit cards) you should take the following steps.

- Put stop payment orders on all outstanding checks that might have been written without your knowledge or permission.
- Close all existing credit card accounts and any account accessible by debit card.
- Open up new accounts protected with a secret password or personnel identification number (PIN). **Do not use the same passwords or PINs as on the original accounts.**

Do not use common numbers (like birth dates, part of your social security number), or commonly chosen words (such as a child's, spouse's, or pet's name) as passwords or PINs.

Step 2 – File a report with the Federal Trade Commission. You can go on-line to file an identity theft complaint with the FTC www.consumer.gov/idtheft. There is an ID theft Affidavit enclosed in this packet. Many creditors and major credit reporting bureaus will accept the “ID theft Affidavit” available on this FTC web site. Go to –

<http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>. If you file on line be sure to make a copy for the investigator that will be contacting you.

Step 3 – Contact all three major credit reporting bureaus. First request the credit bureaus to place a “fraud alert” on your file. You must then be contacted directly before any new credit is taken out in your name. Second, file your police report or the report number given to you by the police. File it immediately with the credit reporting bureaus. A fraud report will be shared with the other bureaus. Place a security freeze on your credit reports. By contacting the three credit bureaus by letter or Internet you will be assigned a “PIN” number that can only be unlocked by you.

You can contact the fraud units at each of the bureaus as follows:

Scamsafe.com – will give you instructions on how to do a security freeze.

Equifax

P.O. Box 740256 Consumer Fraud Division

Atlanta, GA 30374 (800) 525-6285

Experian

P.O. Box 9530 National Consumer Assistance

Allen, TX 75013 (888) 397-3742

TransUnion

Fraud Victim Assistance Dept.

P.O. Box 6790 (800) 680-7289

Step 4 – Contact all of your creditors by phone and in writing. File a law enforcement report, or the FTC's ID Theft Affidavit, with each creditor (Some may require that you use their own form of affidavit).

Keep copies of all correspondence and documents exchanged with each creditor. An identity theft checklist and journal is enclosed in this packet to assist you.

Cancel all existing credit card accounts and open replacement accounts. Ask that those cancelled accounts be processed as “account closed at customer's request” to avoid any negative reporting to credit bureaus.

Step 5 – Notify the phone company. If the identity theft involves the misuse of a long-distance telephone account, cellular telephone, or other telephone service, contact your telephone or wireless company and immediately close all existing accounts.

Step 6 – Notify the post office. If you suspect that your mail has been stolen or diverted with a false change-of-address request, contact your local post inspector. You can obtain the address and telephone number of your local postal inspector by visiting the United States Postal Service web site at: <http://www.usps.com/ncsc/locators/findis.html> .

Step 7 – Notify the Social Security Administration. If you suspect that someone is using your social security number to obtain credit or employment, contact the Social Security Administration's fraud hotline at 1-800-269-0271. To check the accuracy of your work history, order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) and check it for accuracy. You can obtain a PEBES application at your local Social Security office or you can download one from the Social Security Administration web site: <http://www.ssa.gov/online/ssa-7004.pdf> .

Step 8 – Notify the State Department. If your passport has been stolen, notify the passport office in writing to be on guard for anyone ordering a new passport in your name. You can obtain additional information from their web site: <http://travel.state.gov/reportppt.html>.

Step 9 – If you are contacted by a collection agency about a dept for which you are not responsible, immediately notify them that you did not create the dept and that you are a victim of identity theft. Follow up with the collection agency and creditor in writing and include a copy of you police report or ID Theft Affidavit.

Send all letters and copy of the report affidavits, “return receipt requested” or with some other process that gives you proof that the collection agency received your letter.

Step 10 – This is one of your most important steps. Record everything. Make copies of everything. Leave nothing out. Get names and numbers of people you have contacted. Use the forms enclosed in this packet to assist you.

- The assigned detective wants to put the criminal in jail.
- The person that knows the details and facts of the case is you.
- By not filling out the victim packet, the result is the assigned detective may determine that the case is not workable.
- Detectives have heavy caseloads.
- Your case is not the only case he or she is working.
- When you come in for the interview, bring everything.
- Listen to the questions asked and direct your answers to those questions.
- Remember, the detective is in charge of the case.
- Respect their time and be brief during phone calls you make to them.
- Rudeness never works.
- Identity theft cases are slow and may take months to complete. It's not like what you see on TV.
- Leads may not pan out and evidence that you think might be perfect doesn't always prove a case.

Following are a list of contacts you may need to make. Remember, usually you can get this information faster than the detective because you don't need a subpoena. The detective would.

(Organizing Your Case) – www.idtheftcenter.org

(Copy of the ID Theft Affidavit) www.consumer.gov/idtheft.

(Opt out) 1-888-567-8688

(DMV) www.ftc.gov/privacy/protect.htm#Motor

(Direct Mail Marketing) www.thedma.org/consumers/offmailinglist.html

(Telemarketing) www.thedma.org/consumers/offtelephonest.html

(E-mail) www.dmaconsumers.org/offemaillist.html

(Stolen checks) TeleCheck 1-800-710-9898

Certegy, Inc. 1-800-437-5120

International Check Services 1-800-631-9656

(To find out if the identity thief has been passing bad checks in your name, call: 1-800-262-7771

(Mail theft) www.usps.gov/websites/depart/inspect

(Passport fraud) www.travel.state.gov/passport-services.html

(Cell phones and long distance) www.ftc.gov

(SSN misuse) www.ssa.gov

(Tax fraud) www.treas.gov/irs/ci

(Department of Justice) www.usdoj.gov

(FBI) www.fbi.gov

(Secret Service) www.treas.gov/usss

(Protecting yourself) www.treas.gov/usss/faq.shtm

(Security freeze) Scamsafe.com

It is very important that you fill out in detail the Identity Crime Incident Detail Form.

***Bring everything in with you for the interview with the detective.

IDENTITY CRIME INCIDENT DETAIL FORM

Please fill out this form and return it to the Police Department as soon as possible, or bring it to the meeting with the detective assigned to your case. The information you provide will be used to understand what occurred, organize the investigative case, determine where evidence might be found, develop a theory of how the identity crime occurred, and determine what financial institutions should be contacted in the course of the investigation.

Date this form was filled out: _____

First Name: _____

Middle Name: _____

Last Name: _____

Social Security Number: _____

Driver's License Number: _____

Date of Birth: _____

Home Address: _____

Home Telephone Number: _____

**Cell Phone
Number:** _____

**Pager
Number:** _____

**E-Mail
Address:** _____

Employer: _____

**Work
Address:** _____

**Work Telephone
Number:** _____

1. What is the best time to reach you at

home? _____

2. How did you become aware of the identity crime?

_____ found fraudulent charges on my credit card bill

Which one? _____

_____ found fraudulent charges on my cellular phone bill

Which one? _____

_____ received bill for an account(s) I did not open

Which one(s)? _____

_____ found irregularities on my credit report

_____ was contacted by a creditor(s) demanding payment

Which one(s)? _____

_____ was contacted by a bank's fraud department regarding charges

Which one(s)? _____

_____ was denied a loan

_____ was denied credit

_____ was arrested, had a warrant issued, or a complaint filed in my name for a crime I did not commit. Details _____

_____ was sued for a debt I did not incur

Which one? _____

_____ was not receiving bills regularly for a legitimate account

Which one? _____

_____ was denied employment

_____ had my driver's license suspended for actions I did not commit

_____ received a legal filing I did not file, such as a bankruptcy

_____ other; please explain _____

3. What date did you first become aware of the identity crime? _____

4. When did the fraudulent activity begin? _____

5. What is the full name, address, birth date, and other identifying information that the fraudulent activity was made under? _____

6. Please list all fraudulent activity that you are aware of to date, with the locations and addresses of where fraudulent applications or purchases were made (retailers, banks, etc.). List in chronological order, if possible. For example, "On 9-18-02, I received a letter from MM Collections, stating that I had accumulated \$5,000 worth of charges on American Express Account 123456789. On 9-18-02, I called American Express and spoke with Jane Doe. She informed me that the account was opened on 5-12-02 by telephone. I did not open this account, even though it is in my name. The account address was 123 Main St. Anytown, NE. Ms. Martin said she would send me an Affidavit of Forgery to complete and return to her." You may attach a separate piece of paper if you need the space. Please be concise and state the facts.

_____ credit card(s) List bank(s) issuing credit card(s): _____

_____ ATM card(s) List bank(s) issuing ATM card(s): _____

_____ checks and/or checking account number

List bank(s) issuing checks: _____

_____ savings account passbook or number

List bank(s) holding savings account(s): _____

_____ brokerage or stock accounts

List banks and/or brokers: _____

_____ passport List country issuing passport: _____

_____ driver's license or license number List state issuing license: _____

_____ state identity card or identity number List state issuing card: _____

_____ social security card or number

_____ birth certificate List state and municipality issuing birth certificate: _____

_____ resident alien card, green card, or other immigration documents

_____ bank account passwords or "secret words", such as mother's maiden name

_____ other Describe: _____

_____ Unknown

8. to the best of your knowledge at this point, what identity crimes have been committed?

_____ making purchase(s) using my credit card(s) or credit card number(s) without authorization

_____ opening new credit card accounts in my name

_____ opening utility and/or telephone accounts in my name

_____ unauthorized withdrawals from my bank accounts

_____ opening new bank accounts in my name

_____ taking out unauthorized loans in my name

_____ unauthorized access to my securities or investment accounts

_____ obtaining government benefits in my name

_____ obtaining medical services or insurance in my name

_____ evading prosecution for crimes committed by using my name or committing new crimes under my name

_____ check fraud

_____ passport/visa fraud

_____ other _____

9. To assist law enforcement in pinpointing when and by whom your information was compromised, it is of value to retrace your actions in recent months with regard to your personal information. This information is not solicited to “blame the victim” for the crime, but to further the investigation toward who might have stolen your personal or financial

identifiers. What circumstances and activities have occurred in the last six months (include activities done by you and on your behalf by a member of your family or a friend)?

_____ carried Social Security Card in my wallet

_____ carried my bank account passwords, PINs, or codes in my wallet

_____ gave out my Social Security Number To whom? _____

_____ my mail was stolen When? (appx.) _____

_____ I went away and my mail was held at the post office or collected by someone else

_____ I traveled to another location outside my home area

Where did you go and when? _____

_____ mail was diverted from my home (either by forwarding order or in a way unknown)

_____ I did not receive a bill as usual (i.e., a credit card bill failed to come in the mail)

Which one? _____

_____ a new credit card I was supposed to receive did not arrive in the mail as expected.

Which one? _____

_____ bills I was paying were left in an unlocked mailbox for pickup by the postal service.

_____ service people were in my home. From what company?

When? _____

_____documentation with my personal information was thrown in the trash without being shredded

_____credit card bills, pre-approved credit card offers, or credit card “convenience” checks in my name were thrown out without being shredded.

_____my garbage was stolen or gone through

_____my ATM receipts and/or credit card receipts were thrown away without being shredded

_____my password or PIN was given to someone else

_____my home was burglarized

_____my car was stolen or burglarized

_____my purse or wallet was stolen

_____my personal information was provide to a service business or non-profit (i.e., I gave blood, donated money, took out insurance, or saw a financial planner)

Please list: _____

_____my credit report was queried by someone claiming to be a legitimate business interest Who? _____

_____I applied for credit and/or authorized a business to obtain my credit report (i.e., shopped for a new car, applied for a credit card, or refinanced a home).

Please list: _____

_____my personal information is available on the Internet, such as in an open directory, white pages, genealogy web site, or college reunion web site.

_____a legitimate purchase was made where my credit card was out of my sight

_____my personal information was given to a telemarketer or a telephone solicitor

Please list: _____

_____my personal information was given to a door-to-door salesperson or charity fundraiser

Please list: _____

_____ a charitable donation was made using my personal information

Please list: _____

_____ my personal information was given to enter a contest or claim a prize I had won.

Please list: _____

_____ a new bank account or new credit card account was legitimately opened in my name

_____ a legitimate loan was applied for or closed in my name

_____ a legitimate lease was applied for or signed in my name

_____ legitimate utility accounts were applied for or opened in my name

_____ a license or permit was applied for legitimately in my name

_____ government benefits were applied for legitimately in my name

_____ my name and personal information were mentioned in the press, such as in a newspaper, magazine, or on a web site

_____ online purchases were made using my credit card Through what company?

_____ personal information was included in an e-mail

_____ I released personal information t a friend or family member

_____ my personal information was given to a medical care provider, such as a dentist, doctor, etc.

For any items checked above, please, in as much detail as possible, explain the circumstances of the situation:

10. How many purchases over the Internet (retailer or auction sites) have you made in the last six months? _____

11. What Internet sites have you bought from? _____

12. In the last six months, whom has your Social Security Number been given to? (List all)

13. Do your checks have your Social Security Number or Driver's License Number imprinted on them?

____ Yes. (Please list retailer names where checks have been tendered)

14. Have you written your Social Security Number or Driver's License number on any checks in the last six months, or has a retailer written those numbers on a check?

____ Yes. Please list instances and retailer names: _____

15. Do you own a business(es) that may be affected by the identity crime?

____ Yes. Please list the business(es): _____

16. Do you have any information on a suspect in this identity crime case? ___ Yes ___ No

How do you believe the theft occurred?

17. Please list all the banks that you have accounts with. Place an (*) by accounts that have fraudulent charges on them.

Bank Type of account and number Fraudulent?

18. Please list all the credit card companies and banks that you have credit cards with. Place a (*) next to accounts that have fraudulent charges on them.

19. Please list all the utility companies you have accounts with. Place a (*) next to the accounts that have fraudulent charges on them.

20. Please list all the financial institutions you have loans, leases, and mortgages from. Place a (*) next to accounts that have fraudulent charges on them.

Financial Institution Type of account and number Fraudulent?

21. Please list any merchants who you have credit accounts with, such as department stores, or retailer. Place a (*) next to accounts that have fraudulent charges on them.

22. Please list any other financial institutions where fraudulent accounts were opened in your name or using your personal identifiers.

23. Please list any documents fraudulently obtained in your name (driver's license, social security cards, etc.)

24. Have you contacted the following organizations and requested a Fraud Alert be put on your account?

_____ **Equifax** On what date: _____

_____ **TransUnion** On what date: _____

_____ **Experian** On what date: _____

_____ **Your Bank(s) Name of Bank(s):**

_____ **Department of Motor Vehicles**

_____ **Social Security Administration**

_____ **Other; Please list:**

25. Have you requested a credit report from each of the three credit bureaus?

(If you have them in your possession, please attach them to this form)

_____Equifax _____TransUnion _____Experian

26. Have you contacted any financial institution, concerning either legitimate or fraudulently opened accounts? If yes, please list:

Name of financial institution Phone number Person you spoke with

*****Please bring this document with you to the meeting with the detective: all account statements, letters, correspondence, phone records, credit reports, and other documents regarding this case.**

Also, please make a copy of this completed form for your records.

Remember to keep a detailed log of all your correspondence and contacts since realizing you were the victim of identity crime.