Peoria Police Criminal Investigations
Financial Crimes Division

Financial Crimes Questionnaire

In order for Peoria Police to investigate any case of fraud, **supportive documentation is essential**. Please fill out the form as it applies to your particular incident. This information will then be used to investigate your case further. 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. Please be advised that often in financial crimes, time is an important factor for investigators to be able to obtain any necessary information to proceed with your case. It should also be noted that subpoena requests and the request of certain documentation from financial institutions takes significant time for investigators to obtain. **Please read this packet carefully as it will explain to you what documentation you must provide in order for this agency to continue an investigation. Documentation of a financial crime is necessary in order to commence a proper investigation.**

Peoria Police Case # _____ Date this form was filled out: _____

First and Last Name: _____

Middle Name: _____

Date of Birth: _____

Driver's License Number: _____

Home Address: _____

Home Phone Number: _____

Cell Phone Number: _____

Email Address: _____

1. What is the best time to reach you at home? _____

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

- ☐ Found fraudulent charges on credit card bill
- ☐ Received bills for accounts I did not open
- ☐ Contacted by creditor demanding payment
- ☐ Denied a loan or credit
- ☐ Was sued for a debt you did not incur
- ☐ Denied employment
- ☐ Found fraudulent on my cell phone bill
- ☐ Found irregularities on credit report
- ☐ Contacted by bank
- ☐ Accused of crime that you did not commit
- ☐ Not receiving bills regularly for a legitimate account
- ☐ Other

3. Please explain your response for question 2.

4. What date did you first become aware of the financial crime? _____
5. When did the fraudulent activity begin? _____
6. What are full name, address, birth date, and other identifying information that the fraudulent activity was made under?

7. Please list all fraudulent activity that you are aware of to date. Include the locations and addresses of where fraudulent applications or purchases were made (retailers, banks, etc.).

   List in chronological order, if possible. For example: "on 9-18-06, I received a letter from MM Collections stating that I had accumulated $5,000.00 worth of charges on American Express Account #123456789. On 9-18-06, I called American Express and spoke with Jennifer Martin. She informed me the account was opened on 5-12-06 by telephone. I did not open this account, even though it was in my name. The account address was 1234 Maple Street, Anytown, IL. 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.

8. What documents and identifying information was stolen and/or compromised?

☐ Credit card(s). List bank issuing card, **provide copy of transaction record with fraudulent transactions noted**:

_____

☐ ATM card(s) List bank issuing card, **provide copy of transaction record with fraudulent transactions noted**:

_____

☐ Check(s) and /or checking account number. List bank issuing checks, **provide copies of checks (front and back) that were affected**:

_____

☐ Savings account. List bank, **provide copy of transaction record with fraudulent transactions noted**:

_____

☐ Brokerage/stock account. List bank/broker, **provide copy of transaction record with fraudulent transactions noted**:

_____

☐ Passport. List country issuing passport:

_____

☐ Driver's license or license number. List state issuing card, and card number:

_____

☐ State ID card or ID number. List state issuing card, and card number:

_____

☐ Birth certificate. List city/state issuing certificate:

_____

☐ Resident alien card, green card, or other immigration documents:

_____

☐ Bank account passwords or "secret words" such as mother's maiden name:

_____

☐ Unknown

☐ Other. Describe:

9. To assist law enforcement is 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 (including activities done by you and on your behalf by a member of your family or a friend)?

☐ I carried my Social Security Card in my wallet.

☐ I carried my bank account passwords, PINs or codes in my wallet

☐ I gave out my Social Security number. To whom?

_____

☐ My mail was stolen. When?

_____

☐ 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. Business or Pleasure?

- Where did you go and when? _____

☐ Mail was diverted from my home (either by forwarding order or in a way unknown to you)

☐ I did not receive a bill as usual. 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. When? What company?

_____

☐ 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. Who?

_____

☐ My home was burglarized. When?

_____

☐ My car was stolen or burglarized. When/where?

_____

☐ My purse/wallet was stolen. When /where?

_____

☐ My checkbook was stolen. When/where? _____

☐ My personal information was provided to a service business or non-profit (donated money, took out insurance, saw financial planner, gave blood, etc.) Give details:

☐ 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 (shopped for new car, applied for credit card, refinanced a home, etc.)

☐ My personal information is available on the Internet (in an open directory, white pages, genealogy website, high school/college reunion web site, etc.)

☐ A legitimate purchase was made where my credit card was out of my sight.

☐ My personal information was given to a telemarketer or telephone solicitor.

☐ My personal information was given to a door-to-door salesperson or charity fundraiser.

☐ A charitable donation was made using my personal information.

☐ My personal was given to enter a contest or claim a prize I had won.

☐ A new bank account or new credit card account was legitimately opened in my name.

☐ I re-financed my house or property.

☐ A legitimate loan was applied for or closed in my name.

☐ A legitimate lease was applied for or signed in my name.

☐ A legitimate license or permit was applied for in my name. Legitimate utility accounts were applied for or opened in my name.

☐ Legitimate government benefits were applied for in my name.

☐ My name and personal information were mentioned in a newspaper, magazine or on a website.

☐ Online purchases were made using my credit card.

☐ Personal information was included in an email.

☐ I released personal information to a friend or family member.

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

10. How many purchases over the Internet have you made in the last six months?

_____

11. What Internet sites have you bought from? List all:

12. In the last six months, to whom has your Social Security number been given? List all:

13. Do your checks have your Social Security or driver's license numbers imprinted on them? ☐Yes ☐No
    If yes, list the retailer names where checks have been used:

14. Do you own a business that may be affected by this financial crime? ☐ Yes ☐ No
    If yes, list the business name: _____

15. Do you have any information on a suspect in this identity crime case? How do you believe the theft occurred? Please provide specific information as to why you believe said person *may* be a suspect.

16. Have you or a retailer written your Social Security or driver's license numbers on any checks in the last six months? If yes, list retailer name/details

17. Are the financial institution(s), credit card company(s), utility company(s) holding you responsible for funds/charges taken or made unlawfully? ☐ Yes ☐ No

18. Has the financial institution(s), credit card company(s), utility company(s) reimbursed you for the funds/charges taken or made unlawfully? ☐ Yes ☐ No

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

20. Check the following organizations you have contacted to request a Fraud Alert be placed on your account:

☐ Equifax	Date Contacted:_____
☐ Experian	Date Contacted:_____
☐ Trans Union	Date Contacted:_____
☐ Your Bank Name: _____	Date Contacted:_____
☐ Your Bank Name: _____	Date Contacted:_____
☐ Your Bank Name: _____	Date Contacted:_____
☐ Your Bank Name: _____	Date Contacted:_____
☐ Secretary of State: _____	Date Contacted:_____
☐ Social Security Administration	Date Contacted:_____
☐ Other: _____	Date Contacted:_____

21. Check the following credit bureaus you requested a credit report from, and if the form has been received:

☐	Equifax	Credit report received (attach copy to this form)
☐	Experian	Credit report received (attach copy to this form)
☐	Trans Union	Credit report received (attach copy to this form)

22. Please list any financial institutions you contacted regarding either legitimate or fraudulent accounts opened in your name. List details:

Financial Institution	Phone#	Person you spoke with

The following information is very important. Please read carefully and provide the requested information when returning this packet.

For cases involving Forgery, Credit Card Fraud (Unlawful Use of Credit Card—includes debit cards) and Financial Identity Theft please read below.

Forgery: (check, etc. taken, used, and signed without your consent/knowledge): Please provide any copies of checks/documents. Copies of the front and back of the check will be necessary, if they can be obtained.

Credit Card Fraud: (Unlawful Use of Credit Card—includes debit cards): Please provide credit and/or debit card number. Please include copies of statements, noting the fraudulent transactions.

Financial Identity Theft: Please provide any documentation you may have. If this was done via computer/online service, please provide any emails, correspondence, and any related documentation. Please provide any copies of collection notices, and account statements (credit card, bank account, etc.) noting on them any fraudulent transactions.

Deceptive Practices: Please provide any documentation you may have. If this was done via computer/online service, please provide any emails, correspondence, and any related documentation. Please provide any copies of collection notices, and account statements (credit card, bank account, etc.) noting on them any fraudulent transactions. Please provide any copies of checks/documents. Copies of the front and back of the check will be necessary, if they can be obtained.

All documentation can be mailed to the following address:

Peoria Police Department
Attn: Fraud Division
600 SW Adams St.
Peoria, IL 61602

An incident will not be assigned for follow up until the receipt of the above mentioned documentation. Proper documentation is necessary to substantiate the incident, as well as to provide information for follow up. Spreadsheets and handwritten notes will not be accepted. In cases of large dollar amounts, and/or incidents occurring over a long period of time, an accounting may be required. The Peoria Police Department has no means of conducting such an accounting.

The following pages are to be kept by the reporting citizen. They contain information on proper steps to further protect your credit and personal information.

Peoria Police Criminal Investigations
Financial Crimes Division

Financial Crimes Questionnaire

PLEASE KEEP THE REMAINING PAGES AS A GUIDE FOR THE VICTIM OF A FINANCIAL CRIME.

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. It is important that you follow 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 you 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 personel 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. 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/conline/pubs/credit/affidavit.pdf. If you file on line be sure to make a copy for your records.

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 Atlanta, GA 30374	Experian P.O. Box 9530 Allen, TX 75013	Trans Union P.O. Box 6790 Fullerton, CA 92834
Consumer Fraud Division 1-800-525-6285	National Consumer Assistance 1-888-397-3742	Fraud Victim Assistance Dept. 1-800-680-7289

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 exchanges with each creditor. Cancel all existing credit card accounts and open replacement accounts. Ask that thos e cancelled accounts be processed as "account closed at customer's request' to avoid any negative reporting to credit bureaus.

Step – 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 – 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

If a collection agency contacts you about a debt for which you are not responsible, immediately notify them that you did not create the debt and that you are a victim of identity theft. Follow up with the collection agency and creditor in writing and include a copy of your 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 you letter.

Following are a list of contacts you may need to make. Remember, usually you can get this information faster than an investigator because you as a victim do not need a subpoena.

- Organizing Your Case — www.idtheftcenter.org
- Direct Mail Marketing — www.thedma.org/consumers/offmailinglist.html
- Stolen Checks — Tele Check: 1-800-710-9898
Certegy: 1-800-437-5120
International Check Services: 1-800-631-9656
- E-mail Solicitation List — www.dmaconsumers.org.offemaillist.html
- Mail Theft — www.usps.gov/website/depart/inspect
- Telemarketing — www.thedma.org/consumers/offtelephonelist.html
- Passport Fraud — www.travel.state.gov/passport-services.html
- Cell phones and Long Distance — www.ftc.gov
- Social Security 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 — www.scamsafe.com