

## Question 1. What do I do if I notice any suspicious activity on my credit file?

- Contact the following entities:
  1. **Legal Services for Students**
    - If you are a KU student and qualify for our services, schedule an appointment to meet with a Legal Services for Students staff member regarding identity theft.
    - If you are not a student, request referral information.
  2. **The credit bureau** maintaining your credit file with the suspicious activity and report the activity to them
    - CONTACT the credit bureau **IMMEDIATELY**. The contact information is listed under Question 9
      - Inform them of the fraudulent information
      - Inform them that you dispute the fraudulent data
        - This will then be noted on your credit file
  3. **The creditor** reporting the fraudulent data on the credit report
    - By telephone or in writing
    - Inform them that you are a fraud victim and would like to **file a fraud claim**
    - Each creditor has a process for investigating your claim
    - **Cooperate fully** with the request of the credit grantor, so you can be assured you are not held responsible for payment of the unauthorized transactions on the account
  4. Notify **local law enforcement**
    - Call their **non-emergency line**
    - Explain what has happened
    - They will then direct you to the appropriate department and explain what information you need to provide to file a police report
    - Insist on filing a **written report** and be sure to **get a copy**
  5. Notify the **Federal Trade Commission**
    - Contact the **Federal Trade Commission** (FTC) to report the identity theft, if you have not already done so.
    - 1-877-ID-THEFT [1-877-438-4338]
  6. Notify the other two **credit bureaus**
    - Notify the other two credit bureaus
    - The contact information is listed under Question 2 in Handout #1
    - Experian offers an additional safety measure you can place on your credit file

## HANDOUT 2: ACTION TO TAKE IF YOUR INFORMATION HAS BEEN USED FRAUDULENTLY

- **Experian Victim Statement**

- a. What is a Victim Statement?**

- A special type of statement that asks a credit grantor to call you by phone before granting credit
    - A Victim Statement remains on your credit file for **7 years**
    - These are generally added once you have **confirmed** that **someone is using your identification** information in a fraudulent manner
      - Do not place a victim impact statement on your credit file until you believe your information has been used fraudulently
    - If you did not apply for credit, you can instruct the creditor not to process the application
      - This should prevent new accounts from being established using your identification information.

- b. How do I do this?**

- i. By Writing (the only way to add a victim statement)**

- **Include:**
    - 1. A **letter** containing the following information:
        - Your full name
        - current mailing address
        - Social Security Number
        - Any previous addresses used in the last 5 years
        - Phone numbers you would like added to the victim statement (so creditors can contact you before issuing credit)
      - 2. A copy of a **bill or statement**
        - You must show your name at the address used to obtain the credit report
        - Examples: Utility bill, insurance statement, driver's license, government benefit statement, or military identification
      - 3. A copy of a **phone bill**
        - The bill must clearly display one of the two phone numbers that will appear in the victim statement

## HANDOUT 2: ACTION TO TAKE IF YOUR INFORMATION HAS BEEN USED FRAUDULENTLY

### c. What if I want to change my phone number later?

- You must request that your phone number be changed in a letter sent to:
  - Experian National Consumer Assistance
  - P.O. Box 1017
  - Allen, TX 75013
  
- 1. Send a **letter** containing the following information:
  - Your full name
  - Address
  - Social security number
  - Date of birth
  - Any previous addresses used in the last 5 years
  - Specifically state the new phone number you would like added AND the number to be deleted
  
- 2. Include a copy of a **bill or statement** showing the **new phone number** that you would like to be displayed
  - Include a copy of bill or statement showing your name at the address you are requesting to have a credit report mailed to
  - Once you send in the written request, a credit report will be mailed to your address reflecting the change in the victim statement

## Question 2: How do I contact the 3 Credit Bureaus?

1. Equifax Credit Information Services  
Consumer Fraud Division  
P.O. Box 105069  
Atlanta, GA 30348  
Phone: (888) 766-0008 or (800) 525-6285
  
2. TransUnion Fraud Victim Assistance Dept.  
P.O. Box 6790  
Fullerton, CA 92834  
Phone: (800) 680-7289
  
3. Experian National Consumer Assistance  
P.O. Box 1017  
Allen, TX 75013  
Phone: (888) 397-3742

### Question 3. What should I do if I suspect there has been an unauthorized transaction on my account?

#### 1. Contact Legal Services for Students

- If you are a KU student and qualify for our services, schedule an appointment to meet with a Legal Services for Students staff member regarding identity theft.
- If you are not a student, request referral information

#### 2. Contact your account provider

- a. **File a claim** and request that an **investigation** take place
- b. **Cooperate fully** with the investigation. It is a lengthy but necessary process.
- c. Request that your **accounts** with that financial account provider be **closed** and **new accounts opened** with new account numbers
- d. **Request documentation** showing the fraudulent transaction be provided to you
- e. **Refuse to pay the bill** or portion of the bill that is the result of fraud or identity theft while **the investigation** takes place
- f. If checks have been stolen, place a **stop payment** on those checks with your bank.
- g. **How long do I have to file a report with my account provider?**
  - There is generally a grace period for reporting any unauthorized transactions after the transaction has been made
  - If you do not report any suspicious activity within this grace period, the account provider may rightfully **deny** your claim and is **not required to investigate** the potential fraud
    - Therefore, it will be your loss if you fail to report this within the specified period of time after the transaction
  - Although most account providers provide a grace period, **contact the account provider IMMEDIATELY** once you are aware of any unauthorized activity with your bank account
  - This will ensure that you have filed your claim with the account provider before the grace period has ended

## HANDOUT 2: ACTION TO TAKE IF YOUR INFORMATION HAS BEEN USED FRAUDULENTLY

- Also, this is in your best interest so future unauthorized transactions can be prevented

### h. **How long do I have to file a claim if the account is with a bank?**

- Unauthorized electronic withdrawals/transactions
  - 60 days from when the bank sends the statement showing the unauthorized withdrawal/transaction
  - UNLESS you can show extenuating circumstances (then you are given a “reasonable period of time”)
  - You can notify the bank by person, in writing, or over the telephone
- All other unauthorized transactions (checks, debits, etc.)
  - This is set by state law and varies from state to state
  - Contact your bank as soon as the fraud occurs

### 3. **Notify the local police department**

- Call their **non-emergency line**
- Explain what has happened
- They will then direct you to the appropriate department and explain what information you need to provide to file a police report
- Insist on filing a **written report** and be sure to **get a copy**

### 4. **Notify the Federal Trade Commission**

- Contact the **Federal Trade Commission** (FTC) to report the identity theft, if you have not already done so.
- 1-877-ID-THEFT [1-877-438-4338]

### 5. **Notify ALL three credit bureaus**

- Contact information is listed under Question 2
- Request a copy of your credit report
- Place fraud alerts on your credit files, if you have not already done so

## **Question 4: What does the account provider do once I have notified them of the unauthorized transaction?**

- The account provider will likely investigate the suspicious transaction so long as you have notified them within the grace period.
  - Before the account provider can begin investigating the unauthorized transaction, you will likely be required to provide them with information and complete several forms. They should provide all of this information to you.
  - If the account provider refuses to investigate and you are within the grace period, or have a good reason as to why you could not file within the grace period (illness or extended travel), please contact our office for assistance.
- If the account provider determines that the transaction was fraudulent, you will most likely be credited with any money that was lost in the fraudulent transaction

## Question 5: What if my Social Security Number has been used fraudulently for employment purposes?

1. Contact **Legal Services for Students**
  - If you are a KU student and qualify for our services, schedule an appointment to meet with a Legal Services for Students staff member regarding identity theft.
  - If you are not a student, request referral information
2. Contact the **Social Security Administration** immediately & notify them that your social security number may have been **stolen if it is being used for employment purposes by the thief**
  - [www.ssa.gov](http://www.ssa.gov)
  - (800) 269-0271
  - Order your Earnings and Benefits Statement from the Social Security Administration to verify its contents
    - (800) 772-1213
3. Notify **local law enforcement**
  - Use their non-emergency line
  - Explain what has happened
  - They will then direct you to the appropriate department and explain what information you need to provide to file a police report
  - Insist on filing a written report and be sure to get a copy
4. Notify the **Federal Trade Commission**
  - Contact the **Federal Trade Commission** (FTC) to report the identity theft, if you have not already done so.
  - 1-877-ID-THEFT [1-877-438-4338]

## Question 6: When should I contact local law enforcement officials?

- **ONLY** after your identity has been used fraudulently
- Once your identity has been used fraudulently:
  - Contact local law enforcement:
  - Call their **non-emergency line**
  - Explain what has happened
  - Tell them someone has fraudulently used your identity
  - You should then be directed to the appropriate department
    - Someone will then explain what information you need to provide to file a police report
    - Insist on filing a **written report** and be sure to **get a copy**

## **Question 7: What if my social security number is being used to fraudulently establish credit or new accounts?**

- IF your social security number is **ONLY being used to establish credit or new accounts**, it is **not recommended that you change your SSN**.
  - Changing your social security number will cause future complications
- **Do not contact** the Social Security Administration. They are unable to repair your credit if your social security number is used fraudulently.
- **HOWEVER**, you should do the following if your social security number is being used by someone else:
  1. **Contact Legal Services for Students**
    - If you are a KU student and qualify for our services, schedule an appointment to meet with a Legal Services for Students staff member regarding identity theft.
    - If you are not a student, request referral information
  2. **Contact the business where the social security number was used to obtain an account or services**
    - By telephone or in writing
    - Inform them that you are a fraud victim and would like to file a fraud claim
    - Each creditor has a process for investigating your claim
    - Cooperate completely with the request of the credit grantor, so you can be assured you are not held responsible for payment on the account
  3. **The local police department**
    - Use their non-emergency line
    - Explain what has happened
    - They will then direct you to the appropriate department and explain what information you need to provide to file a police report
    - Insist on filing a written report and be sure to get a copy
  4. **The Federal Trade Commission**
    - Contact the **Federal Trade Commission** (FTC) to report the identity theft, if you have not already done so.
    - 1-877-ID-THEFT [1-877-438-4338]
  5. **Notify ALL three credit bureaus**
    - Contact information is listed under Question 2
    - Request a copy of your credit report
    - Place fraud alerts on your credit files, if you have not already done so

### **Question 8: What if my address is stolen or someone fraudulently changed my address?**

- Contact the U.S. Postal Inspection Service
- Call the U.S. Post Office at (800) 275-8777
- [www.usps.com/postalinsepectors](http://www.usps.com/postalinsepectors)
- Notify the Postal Inspector that the mail system has been used to commit fraud
- If you know where the fraudulent credit cards or other materials have been sent, ask that all mail sent to the fraudulent address be forwarded to your own address

### **Question 9: What if my identity has been used fraudulently to make long distance phone calls?**

1. Contact **Legal Services for Students**
  - If you are a KU student and qualify for our services, schedule an appointment to meet with a Legal Services for Students staff member regarding identity theft.
  - If you are not a student, request referral information.
2. Notify your **long distance carrier** about any calls that you or members of your household did not make
3. **Contact the local police department**
  - Use their non-emergency line
  - Explain what has happened
  - They will then direct you to the appropriate department and explain what information you need to provide to file a police report
  - Insist on filing a written report and be sure to get a copy
4. **Contact the Federal Trade Commission**
  - Contact the **Federal Trade Commission** (FTC) to report the identity theft, if you have not already done so. 1-877-ID-THEFT [1-877-438-4338]
5. **Notify ALL three credit bureaus**
  - Contact information is listed under Question 2
  - Request a copy of your credit report
  - Place fraud alerts on your credit files, if you have not already done so

**Question 10: What if my identity has been used fraudulently to open bank accounts, credit Cards, utilities, or any other services in my name?**

1. **Contact Legal Services for Students**
  - If you are a KU student and qualify for our services, schedule an appointment to meet with a Legal Services for Students staff member regarding identity theft.
  - If you are not a student, request referral information.
2. **Contact the business where the account is has been opened**
  - By telephone or in writing
  - Inform them that you are a fraud victim who would like to file a fraud claim
  - Each creditor has a process for investigating your claim
  - Cooperate completely with the request of the credit grantor, so you can be assured you are not held responsible for payment on the account
3. **Notify your local police department**
  - Use their non-emergency line
  - Explain what has happened
  - They will then direct you to the appropriate department and explain what information you need to provide to file a police report
  - Insist on filing a written report and be sure to get a copy
4. **The Federal Trade Commission**
  - Contact the **Federal Trade Commission** (FTC) to report the identity theft, if you have not already done so.
  - 1-877-ID-THEFT [1-877-438-4338]
5. **Notify ALL three credit bureaus**
  - Contact information is listed under Question 2
  - Request a copy of your credit report
  - Place fraud alerts on your credit files, if you have not already done so