

HANDOUT 1: STEPS TO TAKE BEFORE YOUR IDENTITY IS USED FRAUDULENTLY
(FOR ALL STUDENTS WHO WERE PART OF THE DATABASE THAT WAS HACKED)

Step 1: Contact ISSS

- Request that ISSS disclose to you all of your information that was included in the database when it was hacked into
- If the following information was NOT included in the database (and was therefore not accessible by anyone trying to steal your identity), the following steps may not be necessary. THIS DECISION IS UP TO YOU.
 - Social Security Number
 - Passport Number

Step 2: Contact Credit Bureaus (These are all free services)

A. Equifax Credit Information Services

1. Fraud Alert

a. What does this do?

- A fraud alert can be placed on a credit file.
- The fraud alert will remain on the credit file for **6 months**
 - You will have to again contact Equifax to place the fraud alert on the file once the original fraud alert has expired
- Once the fraud alert is placed on the credit file:
 - Your name will be removed from all **pre-screened credit offers**
 - **Complimentary credit reports** are provided to you
 - These are usually free throughout the duration of the fraud alert. Generally, one is automatically sent to you once the alert has been placed on the credit file.
 - You must request your credit reports after you receive the first complimentary report
 - Creditors are directed to **contact you** before approving any credit applications
 - Therefore, it is highly unlikely that you will be eligible for **instant credit**

b. How do I place a fraud alert on my credit file?

i. By phone

- Equifax has an automated system that can place a fraud alert on the credit file
- Contact: (888) 766-0008 or (800) 525-6285

ii. By Mail

- Include your name, address, social security number
- Include copies of two forms of identifications
 - (e.g.) driver's license, utility bill, social security card
- Request that a fraud alert be placed on your credit file
- Address:
 - Equifax Credit Information Services

**HANDOUT 1: STEPS TO TAKE BEFORE YOUR IDENTITY IS USED FRAUDULENTLY
(FOR ALL STUDENTS WHO WERE PART OF THE DATABASE THAT WAS HACKED)**

- Consumer Fraud Division
- P.O. Box 105069
- Atlanta, GA 30348

c. What if I don't have a credit file?

- Equifax says that they will shred any information sent to them by you, including the letter and additional documentation
- You will be sent a letter explaining that there is no credit file
- You should contact Equifax periodically in the event that credit file is created (either by you or by fraudulent means)
- You should check every 3-4 weeks at first

d. What are the negative consequences of the fraud alert?

- You will not likely be approved for instant credit (because the creditor must contact you before credit can be approved)
- The alert does not affect you negatively

e. Will Equifax contact me before the address on my credit file is changed?

- NO
- The address is typically changed when you contact a creditor regarding an address change. Once this occurs, the creditor then contacts the Credit Bureau regarding the change.
- It is up to you to monitor the credit report to be sure no fraudulent address changes have been made

B. TransUnion

1. Protective Statement

a. What does this do?

- A protective statement can be placed on a credit file.
- The protective statement will remain on the credit file for **1 year**
 - You will have to again contact TransUnion to place the protective statement on your credit file once the original fraud alert has expired
- Once the protective statement is placed on the credit file:
 - Your name will be removed from all **pre-screened credit offers**
 - **Complimentary credit reports** are provided to you
 - These are free throughout the duration of the protective statement. A credit report should be sent to you automatically once the alert has been placed on the credit file.
 - You must request additional credit reports after you receive the first complimentary report
 - Creditors are directed to **contact you** before approving any credit applications

**HANDOUT 1: STEPS TO TAKE BEFORE YOUR IDENTITY IS USED FRAUDULENTLY
(FOR ALL STUDENTS WHO WERE PART OF THE DATABASE THAT WAS HACKED)**

- Therefore, it is highly unlikely that you will be eligible for **instant credit**

b. How do I place a protective statement on my credit file?

i. By phone

- TransUnion has an automated system that can place a fraud alert on the credit file
- Contact: (800) 680-7289

ii. By Mail

- Include your name, address, social security number
- Include copies of two forms of identifications
 - (e.g.) driver's license, utility bill, social security card
- Request that a protective statement be placed on your credit file
- Address:
 - TransUnion Fraud Victim Assistance Dept.
 - P.O. Box 6790
 - Fullerton, CA 92834

c. What if I don't have a credit file?

- TransUnion will create a file for you if no file currently exists
- This new file will have a protective statement placed on it

d. What are the negative consequences of the fraud alert?

- You will not likely be approved for instant credit (because the creditor must contact you before it can be approved)
- The alert **does not affect** you negatively

e. Will TransUnion contact me before the address on my credit file is changed?

- NO
- The address is typically changed when you contact a creditor regarding an address change. Once this occurs, the creditor then contacts the Credit Bureau regarding the change.
- It is up to you to monitor the credit report to be sure no fraudulent address changes have been made

C. Experian

1. Security Alert

a. What does this do?

- The security alert will be on your credit file for **90 days**
 - You will have to again contact Experian to place the fraud alert on the file once the original fraud alert has expired

**HANDOUT 1: STEPS TO TAKE BEFORE YOUR IDENTITY IS USED FRAUDULENTLY
(FOR ALL STUDENTS WHO WERE PART OF THE DATABASE THAT WAS HACKED)**

- Once the fraud alert is placed on the credit file:
 - Creditors will be alerted to confirm your identification before granting credit in your name
 - Complimentary credit reports are provided if:
 - You request a report in writing and states that you believe information on their report is inaccurate due to fraud
 - Include:
 - Name
 - Address
 - Date of birth
 - Social Security Number
 - Addresses you have lived at in the past 5 years when corresponding with Experian

b. How do I place a security alert on my credit file?

i. By phone:

- Experian has an automated system that can place a fraud alert on the credit file
- Contact: (888) 397-3742

ii. Online:

- www.experian.com/consumer

iii. In writing:

- Request that a security alert be placed on your credit file
- Include the following information:
 - Your full name, address, Social Security number, date of birth
 - Any additional addresses you have lived at in the last five years.
- Address:
 - Experian National Consumer Assistance
 - P.O. Box 1017
 - Allen, TX 75013
 -

D. What do I need to do once the alert is on my credit file?

- It is still **YOUR responsibility** to monitor your credit file for any unauthorized activity
- During the period of the fraud alert, you are generally entitled to free credit reports from each bureau that you contacted to place a fraud alert on your credit file
- You must be **vigilant** about checking your credit report every few months

Step 3: Contact anyone you maintain an account with, including financial account providers, creditors, and utility/service providers

- Banks, Credit Unions, credit card companies, loan providers, utility companies, etc.

A. What can they do to ensure my accounts are secure before anyone tries to use my account without my permission?

- This varies from account provider to account provider
- Some account providers can do very little before any fraudulent activity actually occurs.
- Some account providers have monitoring systems in place even prior to you contacting them that will notify them if any unusual activity takes place in your account
 - Monitoring systems may include:
 - Account monitoring: any irregular account activity will notify the account provider to contact you to confirm that you authorized the activity
 - Large account withdrawals
 - Address changes
 - Check orders
 - Fraud detections
- Even if your institution has a monitoring system, it is still **YOUR RESPONSIBILITY** to monitor your monthly statements from your account providers and account providers
 - Please be meticulous about checking each transaction and making sure you authorized it.

B. Should I still contact them even if no one has fraudulently used my used my identity or account information yet?

- **YES**
- Let your account provider know you are the potential victim of identity theft
 - Most places will then note this on your account
 - Request that they contact you before any address changes are made
 - Once this happens, you may be required to show proper identification before making any withdrawals, cashing any checks, etc.

**HANDOUT 1: STEPS TO TAKE BEFORE YOUR IDENTITY IS USED FRAUDULENTLY
(FOR ALL STUDENTS WHO WERE PART OF THE DATABASE THAT WAS HACKED)**

Step 4: Contact the Federal Trade Commission (FTC)

- This is the U.S. Federal Government's centralized identity theft complaint database.
- If you are a victim of identity theft, contact the FTC
 - www.consumer.gov/idtheft
 - 877-ID-THEFT [877-438-4338]
 - www.ftc.gov
- The FTC collects complaints from identity theft victims and shares their information with law enforcement nationwide
- Information may also be shared with government agencies, consumer reporting agencies and companies where the fraud was perpetrated to **help resolve identity theft related problems.**
- **Contact them immediately. You do not have to wait until someone actually uses your identity.**

Step 5. Change your Driver's License Number

- Kansas Department of Motor Vehicles has no way to flag potential driver's license fraud in their system

1. Do I really need to change my driver's license number?

a. YES, If:

- If you currently use your Social Security Number as your Driver's License number

2. How do I change my driver's license number?

- Go to the Kansas Department of Motor Vehicles office in Lawrence
- Contact Information:
 - 785-843-9593
 - 1035 N 3rd St., Suite 122, Lawrence, Kansas
- Hours: Tuesday - Friday 7:00 to 5:45
- Cost: \$10.00
- You must have your:
 - Current driver's license
 - Passport and I-94 form

3. What if my driver's license has been issued in another state?

- You will have to contact that state's Department of Motor Vehicles for more information OR
- You can apply for a Kansas Driver's License
 - See above information