After Identity Theft (Handout)

Identity theft is the crime of obtaining the personal or financial information of another person with the intention of assuming that person's identity in order to make purchases or borrow money. As a victim, you may feel upset and overwhelmed knowing that someone has access to your private information. Remember that recovering from identity theft is possible. By breaking the process down into eight steps and using the right resources, you'll protect yourself and move towards a life after identity theft.

Types of Identity Theft

Financial identity theft can occur in several different ways. One common instance is when an identity thief makes charges on one of your existing accounts. In this case, you may become aware of the fraudulent charges when your financial institution contacts you asking if you recognize a particular transaction. In an effort to minimize the impact of the theft, your bank or credit union may block additional transactions until they are able to verify whether the charges are in fact yours or not. Or you may become aware of the fraud when you review your account transaction history and notice a transaction that you don't recognize. This occurs when the thief has obtained your account numbers or your physical debit or credit card.

The other type of financial identity theft happens when the thief fraudulently opens an account in your name. The scammer likely has access to your name, social security number, and other personal information. Often, they will use an address and phone number different than the consumer's in order to conceal the account for a longer period of time. That way when the creditor sends a statement or reaches out by phone, the consumer is not tipped off to the fact that the account has been created. Typically, you don't become aware of the existence of the account until checking your credit report.

Liability for Fraudulent Transactions

There are several federal laws that help consumers limit their liability for fraudulent transactions for both credit and debit cards. For credit card transactions, The Fair Credit Billing Act (FCBA) limits a consumer's liability for a lost or stolen credit card to $50. Even if an identity thief charged a balance of $500 on a credit card, the consumer would only be legally responsible for $50 of the fraudulent transactions. However, many financial institutions provide greater protection than what is required by the law, and may not hold a consumer liable for any amount of fraudulent transactions. Check with your financial institution to determine if you have more protection.

When it comes to fraudulent debit card transactions, there is a different law in place. The Electronic Fund Transfer Act limits the liability for a lost or stolen debit or ATM card to $50 if you report it within two business days of noticing the card is lost or stolen. If you report it after two business days but within 60 days, your liability is limited to $500. If you wait more than 60 days to report the card lost or stolen, then there is no limit to your liability for the fraudulent transactions. This means that you could lose all of the money in your account, plus your maximum overdraft line of credit if you set one up.

Act Quickly

If you have been the victim of identity theft, do not wait to respond. Not only will you limit your liability for the fraudulent transactions, you can stop the fraud from making a mess of your life. You may feel uncertain about what to do first. But by springing into action and following these eight steps, you will be able to rebuild your financial life.

Step 1: Call Companies Where Fraud Occurred

If a credit card or bank account has been used or opened illegally, you should contact the creditor or financial institution immediately to inform them. Depending on the type of fraud that occurred and the amount of your financial or personal information that was compromised, your financial institution will advise you of the necessary next steps.

© BALANCE 2020 | REV1120

If an existing account was charged, the financial institution will likely require a new account number and card to be issued, but may not require that the account be closed. In the event that a new account was fraudulently created, that account will need to be closed. If a checking or savings account was compromised, the financial institution may close the account. In either instance, future account statements should be monitored carefully for evidence of new fraud.

Because it is difficult to concretely determine where an identity thief acquired your personal or financial information, this is also a good time to change your online banking login information along with your PINs (Personal Identification Number). The more difficult you make it for the thief to access your personal and financial information, the better.

Step 2: Obtain Credit Report and Set Fraud Alerts

The best approach to recovering from identity theft is to do a thorough review of your accounts, and take precautions to halt further fraud from occurring. A key step is to obtain a copy of your credit report from each of the three credit reporting bureaus. You are entitled to a free copy of your credit report from the Annual Credit Report Request Service from each of the three major credit reporting bureaus (Experian, TransUnion and Equifax) once every twelve months by visiting www.annualcreditreport.com, or calling 877.322.8228. When you receive your credit reports, review the information very carefully to ensure that you recognize every account listed on the report. (We will review in a later step how to correct your credit report if it contains fraudulent accounts).

You will also want to set a fraud alert. This requires additional verification before any new accounts are opened, which may include a phone call to verify that you are actually the one trying to open an account. This service is free. Plus, once you set a fraud alert with one credit reporting bureau, they must notify the other two credit reporting bureaus about it. An initial fraud alert will last for 90 days. But if you think you're still at risk for identity theft after the initial time period, you can request another 90-day alert.

Step 3: Report ID Theft to Federal Trade Commission (FTC)

Now that you have contacted the companies where the fraud occurred, obtained your credit reports, and set fraud alerts, the next step is to report the theft to the Federal Trade Commission (FTC). You can report the fraud either online at https://www.identitytheft.gov/Assistant# or by calling (877) 438-4338. Based on the information that you enter or provide over the phone, IdentityTheft.gov will create the tools you need to begin your recovery, including:

- **A personal recovery plan**
- **Pre-filled letters to send to merchants, banks, and others affected by the identity theft**
- **An Identity Theft Report, which is your official statement about the crime**

Your Identity Theft Report provides you with a summary of the fraudulent activity all in one place–this will be very helpful in subsequent steps. Your recovery plan will guide you through your steps, and update as you complete different necessary tasks. It will also track your progress and pre-fill your personal information, dates and data across other necessary forms, saving you from inputting the information over and over again.

Step 4: File a Police Report

Remember, identity theft is a crime. By filing a police report and reporting the theft to local authorities, you may be able to provide valuable information that will assist in stopping additional theft from occurring in the future. When you contact your local law enforcement, you can fill out the report in person or possibly online. To submit the police report, you will likely need to provide a copy of the FTC Identity Theft Report (from Step 3) along with:

- **Government-issued photo ID**
- **Proof of address**
- **Proof of theft (bills, notices, credit report)**

Step 5: Correct Credit Report information

Dispute any fraudulent items on your credit reports with each of the three major credit-reporting bureaus. Once a dispute is submitted, the bureau is required to investigate and respond within 30 days (45 days if the report was obtained through the Annual Credit Report Request Service).

Victims of identity theft are entitled to receive additional free credit reports in order to ensure that fraudulent information has in fact been removed after the investigation period of your dispute. Disputes can made by submitting a form online through the credit bureau's website or mailing a letter to the credit bureaus (please see contact information on page 4). You can use the Sample Dispute letter on page 5 to create your own.

Step 6: Consider an Extended Fraud Alert or Credit Freeze

If you have created an Identity Theft Report, you can get an extended fraud alert on your credit file. When you place an extended alert, you can get two free credit reports within 12 months from each of the three nationwide credit-reporting companies, who must take your name off marketing lists for prescreened credit offers for five years (unless you ask them to put your name back on the list). The extended alert lasts for seven years.

Remember, a fraud alert requires any creditor to verify your identity when someone applies for credit under your name. If you feel like a fraud alert will not provide enough protection, you can place a security freeze on your credit report. With a freeze, your report is off limits to any creditor or other business that doesn't have a pre-existing relationship with you. Since most creditors will not grant credit without a credit check, this makes it extremely difficult for a thief to get credit in your name.

If you want to apply for credit yourself (or rent an apartment or do anything else that requires a credit check), you can have the freeze lifted by giving direct authorization through a 10-digit PIN (either temporarily or permanently), but it may slow down the application process. Depending on the credit reporting bureau and your state, there may be a cost for both placing and removing a credit freeze. To learn more about the possible fees associated with placing credit freezes at each credit reporting bureau, please visit https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp, https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/, and https://www.transunion.com/credit-freeze/credit-freeze-information-by-state.

Another option is a credit lock. Similar to credit freezes, a credit lock restricts most lender's access to your credit report, and can provide you with an additional sense of security. However, it is much easier to unlock than unfreeze your credit. You can simply use your computer or mobile device any time (a PIN is not required).

It is important to understand that credit locks are not governed by state law. Rather they are the result of a contract between you and the credit reporting bureau. So if a thief fraudulently accesses your credit file while a freeze is in place, you will have more protections under state law than you would under a contract with a bureau. The bureaus tend to market credit locks as a faster and more convenient alternative to credit freezes, but freezes provide more protection.

Step 7: Contact Social Security Administration

Depending on the type of personal information that was stolen, you may need to take additional action with the Social Security Administration. Your first step is to create a My Social Security account at https://www.ssa.gov/myaccount/. Even if you haven't been a victim on identity theft, it is still a good idea to create a My Social Security account because it removes the risk of an identity thief potentially creating one in your name.

With an account, you can review the earnings posted to your record on your Social Security Statement and the benefits that you're currently receiving (if applicable). By reviewing this information, you can determine if your social security number has been compromised. Also, if you see any inconsistencies such as benefits distributed in your name that you did not request, you'll want to contact your local Social Security Administration right away. Locate your local office by visiting https://secure.ssa.gov/ICON/main.jsp or calling (800) 772-1213.

In the event that you need to obtain a replacement social security card, you may be able to apply online through your My Social Security account if you meet certain criteria. If you do not meet the criteria, you will need to fill out an application that you can drop-off or mail to your local social security office. The following article helps you determine if you need a new social security number: https://www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number.

Step 8: Contact the Internal Revenue Service (IRS)

The Internal Revenue Service (IRS) combats tax-related identity theft with an aggressive strategy of prevention, detection, and victim assistance. Tax-related identity theft occurs when someone uses your social security number to file a tax return claiming a fraudulent refund. You may be unaware that this has happened until you efile your return, only to discover that another return has already been filed using your social security number. Or, the IRS may send you a letter saying they have identified a suspicious return using your number. Be alert to possible tax-related identity theft if you are contacted by the IRS or your tax professional/provider about:

- **More than one tax return was filed using your SSN**
- **You owe additional tax, refund offset or have had collection actions taken against you for a year even though you did not file a tax return**
- **IRS records indicate you received wages or other income from an employer for whom you did not work**

If your social security number is compromised, and you know or suspect that you're a victim of tax-related identity theft, you should respond immediately to any IRS notice by calling the number provided. You will also want to complete IRS Form 14039, Identity Theft Affidavit, if your efiled return is rejected because of a duplicate filing under your social security number. You will need to attach the form to your return and mail according to the instructions. For more information, visit https://www.irs.gov/identity-theft-fraud-scams or call the IRS at (800) 908-4490.

In order to minimize your exposure to tax identity theft and other scams, remember that the IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Resources

Equifax
To order a credit report: (800) 685-1111
To report fraud: (888) 766-0008
PO Box 740241, Atlanta, GA 30374
www.equifax.com

Experian
(888) 397-3742
PO Box 2104, Allen, TX 75013
www.experian.com

TransUnion
To order credit report: (800) 888-4213
To report fraud: (800) 680-7289
PO Box 2000, Chester, PA 19022
www.transunion.com

Annual Credit Report Request Service
(877) 322-8228
PO Box 105281, Atlanta, GA 30348
www.annualcreditreport.com

Federal Trade Commission
(877) 382-4357
Identity theft hotline: (877) 438-4338
600 Pennsylvania Avenue NW, Washington, DC 20580
http://www.ftc.gov/

Social Security Administration
(800) 772-1213
Identity theft hotline: (877) 438-4338
600 Pennsylvania Avenue NW, Washington, DC 20580

Sample Dispute Letter

[Your name]
[Account Number at company, if available]
[Date of birth or other identifying information requested by company]
[Your return address]
[Date]

[Company Name]
[Company address for receipt of direct disputes]

Re: Disputing error[s] on credit report

Dear [Name of company],

I am writing to request a correction of the following information that appears on my [Equifax, Experian, TransUnion] consumer report:

Dispute 1 [These are examples. Pick the ones that apply to your credit report.]

- **Account Number or other information to identify account:** [Insert account number or other information such as account holder names and past addresses. This is especially important if you have had multiple accounts with the same company.]
- **Dates associated with item being disputed:** [Insert the date that appears on your report. This helps ensure that the correct account is identified by the company and to identify which aspects of the report are being disputed. You can still file a dispute if you don't have this date.]
- **Explanation of item being disputed:**
    - o I'm the victim of identity theft and I don't recognize one or more of the accounts on my report. [You may wish to include a copy of the Identity Theft Report from https://identitytheft.gov/ describing the identity theft.]

Dispute 2 [Continue numbering for each disputed item on your report and include the same information]

[Include the following sentence if you are including a copy of your credit report or other supporting documentation. "I have attached a copy of my report with the accounts in question circled."]

Thank you for your assistance.

Sincerely,
[Your name]

© BALANCE 2020 | REV1120

After Identity Theft Checklist

❑ Step 1: Call Companies Where Fraud Occurred

- Inform them of the fraud
- Close account (if necessary)
- Change logins, passwords and PINS

❑ Step 2: Obtain Credit Report and Set Fraud Alerts

- Visit www.annualcreditreport.com to obtain credit report from 3 major credit reporting bureaus
- Review each report carefully
- Set fraud alerts with each credit reporting bureau

❑ Step 3: Report ID Theft to Federal Trade Commission (FTC)

- Visit https://www.identitytheft.gov/Assistant# or call (877) 438-4338 to complete Identity Theft Report
- Follow established recovery plan

❑ Step 4: File a Police Report

- Contact local law enforcement to inform of theft
- Provide a copy of your FTC Identity Theft Report

❑ Step 5: Correct Credit Report information

- Submit disputes to each credit reporting bureau that contains fraudulent account information
- Can be completed online at the credit bureau's website or by mailing a dispute letter

❑ Step 6: Consider an Extended Fraud Alert or Freeze

- Extended fraud alerts last for seven years
- Credit freezes last until you remove them

❑ Step 7: Contact Social Security Administration

- Create a My Social Security account at https://www.ssa.gov/myaccount/
- Review the earnings posted to your record
- Contact Social Security if you see inconsistencies

❑ Step 8: Contact the Internal Revenue Service (IRS) (if applicable)

- Respond immediately to any IRS notice by calling the number provided

Schedule your Personal Financial Checkup today for helpful guidance and more tips!

Marina Botros
Online Signup: www.truliant.org/tawcheckup
Email: Marina.Botros@truliantfcu.org
Phone: 336.659.1955, option 7, ext. 2702