

## After Identity Theft – A Quick Reference Guide

Discovering that you are a victim of identity theft is a harrowing and unfortunate experience. Though the attack can occur in only a few minutes, the ramifications can last for years. We certainly hope it never happens to you, but the fact is that business owners are increasingly being targeted. Since you must act quickly when addressing identity attacks, Alliance Technologies is happy to provide this quick reference guide for protecting both yourself and your business.

### Immediate – Do these things as quickly as possible

First, create an Identity Theft folder and keep printouts of every communication throughout this process. Where possible use certified mail to communicate with other parties so that you can maintain a record. Contact your legal counsel and ask for advice. You should also read these sources for more valuable information:

- <http://www.privacyrights.org/fs/fs17a.htm>
- <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>

Next, contact the fraud departments of all three credit bureaus and request that a fraud alert be placed on your file. Call the FTC Identity Theft Hotline. If the loss exceeded \$500k, you should contact your local FBI office as well.

Equifax: 888-766-0008	Experian: 888-397-3742	Transunion: 800-680-7289	FTC: 877-438-4338
-----------------------	------------------------	--------------------------	-------------------

Finally, you should determine the possible scope of damages by building a list of each credit card, ATM card, banking, and investment account that you have. Cancel each card and call each company to have it reissued. Change each account's spoken password and PIN to something new and unique. Remember that brokerage accounts are not protected in the same way as credit, checking, and savings accounts. Losses from these accounts can be significantly higher, so be sure to contact those companies to ask about what you can do.

### Short Term – Do these things within a few days

Within a few days, you should begin working up a public relations plan for your business. As much as we'd like to keep such incidents from going public, if anyone involved in the theft wishes to recoup their money through insurance, a police report will likely be required. Police reports are read by news agencies, so the story is likely to break. The sooner you take control of the situation, the more control you will be able to maintain. Be sure to communicate to family members, employees, clients, and vendors, as they all will be concerned as to how the incident will impact them.

If you have a web presence, get the word out via Twitter, Facebook, and your blog. Regardless, you should contact the local news outlets and try to frame the incident as a story. Explain what happened, how it fits in the world as a whole and how everyone is at risk. Explain what you did to minimize your losses and what you are doing to minimize your risk in the future.

Once your plan is in place, you can file an identity theft report with the police. This will enable you to extend the credit agencies' fraud alerts to a full seven years. These agencies will send you a notice that will allow you to extend the alerts as well as get free copies of your credit reports. Once you have your credit reports, be sure to review them and go through the process of correcting inaccuracies. Consider using this sample letter: <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf>

As you work with the credit agencies, build a list of all entities that opened fraudulent accounts and tell each bureau to remove any inquires due to fraudulent access. Verify that you have received a new account number and undergone a password or PIN reset for each active account listed. If you had new bank accounts set up fraudulently, notify ChexSystems at 800-428-9623.

To minimize the risk of an infected workstation being used to re-take control of your accounts, purchase a new PC dedicated for online financial transactions. The cost of a low-powered PC is much lower than the potential losses. This PC should run a modern and maintainable operating system such as Windows 7 or OSX 10.6. It should be running a modern antimalware system like Sophos or Kaspersky. Ideally, it should not be running third party software like Adobe Reader, Flash, or Oracle Java. From this system, log into each financial website and change your passwords and security questions. For additional security, do not use factual answers to your security questions, as attackers can often uncover this information from public sources.

Lastly, to verify the security of your environment, have a vulnerability assessment performed. This assessment should examine administrative rights, operating system patch levels, and application patch levels. It should also ensure your antimalware software is sufficient and current.

### **Mid Term – Do these things after two to four months**

Sometime between two and four months after the incident, things should be calming down. It is important to maintain your momentum to keep things relatively secure. In the US you are entitled to a free copy of each of your credit reports every year. The reports that you received earlier do not count against this total because they were a response to fraud. Call 877-322-8228 and request a copy of each report. Note the date you do this, as you will not be able to receive another free report for a year. As you review these reports, look for new accounts being opened in your name. If this is occurring, call the fraud departments in the table on page 1 and report them.

To remain proactive, consider doing the following:

- Putting a freeze on your credit report: <http://www.consumersunion.org/pdf/security/securityIA.pdf>
- Opting out of pre-approved credit offers: [www.optoutprescreen.com](http://www.optoutprescreen.com)
- Removing your name from the direct marketing association: [www.dmchoice.org](http://www.dmchoice.org)
- Adding your phone numbers to the do not call list: [www.donotcall.gov](http://www.donotcall.gov)
- Order your earnings report from: [www.ssa.gov/online/ssa-7004.html](http://www.ssa.gov/online/ssa-7004.html)

Finally, follow through on as many recommendations from the vulnerability assessment as is financially feasible.

### **Long Term – Do these things over the next several years**

Sadly, identify theft is forever. Constant vigilance is required, but fortunately it becomes easier. Starting at the one year anniversary of your last request of your free credit report, request one every four months. This way, by the end of a year, you have collected all three of your reports, and have been able to detect and correct issues proactively.

Be sure to also monitor your other accounts, such as health insurance claims and store-specific credit cards. You can do some of this by using [www.myidscore.com](http://www.myidscore.com) to track your likelihood of identity theft.