



Notice of Security Breach

Security breaches have become increasingly common in recent years. As more and more companies use computer systems to “warehouse” their customers’ personal information, the potential for “leaks” of this information increases. These leaks can occur in a number of ways:

- **Computer Hacking** - A large number of these breaches are attributable to computer hacking, where hackers break into seemingly secure computer systems and steal consumers’ personal information to use for their own benefit.
- **Employee Misconduct** - Employees may violate company policy and abuse their privileges to access consumers’ personal information and then use or sell it.
- **Unintentional Release** - Many security breaches occur accidentally. A company unintentionally prints your Social Security number on a label that is then sent out through the mail, or a document containing the personal information of thousands of customers is accidentally released to the public.

Illinois law requires companies to notify you when there has been a breach of security and your personal information may be at risk. These notifications do not necessarily mean that your identity has been stolen, but they should be taken seriously. Illinois law requires companies that suffer breaches to notify consumers within a “reasonable time.” Many larger companies stagger their notification letters, so if you know someone who received a letter before you, that does not necessarily mean that the company did not act reasonably.

Most large companies have a procedure in place that is implemented the moment they learn of a security breach. This procedure could include a special toll-free number or website with frequently asked questions or important and useful links. Many companies will work with one or all of the credit reporting agencies to set up credit monitoring services for affected consumers.

We encourage consumers to utilize the special toll-free numbers or websites set up by companies who have suffered breaches. Similarly, if the breach notification letter offers credit monitoring services, we recommend that consumers take advantage of that offer. It is probably not necessary to pay for these services, and they are often offered at no charge to affected consumers.

A security breach of your personal information will not entitle you to all of the protections that a victim of identity theft would receive, but there are still several steps you can take to protect yourself.

Breach Checklist

- **Check with your creditors.** Work with your credit card companies, banks and other lenders to determine if any suspicious or unauthorized activity has occurred on your accounts.
- **Place an initial fraud alert on your credit report. Order your free copy of your credit report and review it for problems.** Contact the toll-free number of any of the three consumer reporting companies to place a fraud alert on your credit report. You only need to contact one of the three companies because that company is required to contact the other two. Initial fraud alerts last for one year.

- **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016

Once you place a fraud alert on your file, you are entitled to a free copy of your credit report. The credit reporting agencies will send you a letter telling you how to order your free report. When you receive your credit reports, review them carefully and look for any suspicious activity.

- **Consider accepting the breached company's offer of free credit monitoring.** After a breach, some companies offer those affected by the breach free credit monitoring services. Credit monitoring is a service that alerts you to key changes on your credit report so that you can take action if it is not a change that you requested. This is a helpful service that can alert you to new accounts, but you also should always remain vigilant about checking your existing accounts on a regular basis for unauthorized charges and dispute unauthorized charges immediately.
- **Consider placing account alerts on your financial accounts so that you will receive a notice of any withdrawals over a certain amount of money that you can specify.** If you receive an alert for a withdrawal that you did not initiate, then you should contact your financial institution immediately.
- **Remain alert.** This is always a good idea, but it is especially important in the first year following a security breach notification. Take advantage of your right to one free copy of your credit report from each of the three consumer reporting companies per year. Request a report from one of the reporting companies every four months and carefully review this report for suspicious activity. To obtain the free reports, call 1-877-322-8228 or order online at www.annualcreditreport.com.

Be on the lookout for warning signs that your information is being misused. Such signs include:

- Receiving credit cards for which you did not apply;
 - Being denied credit or offered credit at less favorable terms for no apparent reason;
 - Receiving calls or letters from debt collectors or businesses about merchandise or services you did not buy; and
 - Missing bills and other pieces of mail.
- **Be aware that if there are unauthorized charges on your credit report, you may be the victim of identity theft.**

For more information, please contact us.

Chicago
100 W. Randolph Street
Chicago, IL 60601
(312) 814-3000
TTY: (800) 964-3013

Springfield
500 S. Second Street
Springfield, IL 62701
(217) 782-1090
TTY: (877) 844-5461

Carbondale
601 S. University Avenue
Carbondale, IL 62901
(618) 529-6400/6401
TTY: (877) 675-9339

Please visit www.IllinoisAttorneyGeneral.gov