



P.O. Box 309  
Waterbury Center, VT 05677

Monday, March 22, 2010

Mr. John Doe  
1 Main Street  
Mapleville, IL 60222

## NOTICE OF POTENTIAL CREDIT CARD INFORMATION BREACH

Dear John Doe,

We are very sorry to be writing to advise you of a vulnerability that has been discovered in our web server that may have put your personal information, including your credit card information, name, address, email address and phone number at risk of exposure to an unauthorized party by means of an **SQL Injection** attack.

This method of attack is executed by the insertion of code directly into a dialog box (such as where a user might type their name, or a search term) which can then be executed on an underlying database, returning information to the screen. This type of attack has been on the rise in companies large and small because attackers are now using 'bots to scan websites for this vulnerability. Even though your information was encrypted on our website, we suspect that the attackers also cracked the encryption code.

We have closed this vulnerability on our website by not allowing executable code to be inserted into any dialog boxes. We have also hired a third party vendor to scan our site at regular intervals for this and any new vulnerability that may arise. Additionally, we are enrolled in a program to bring our site to the highest level of compliance with the Payment Card Industry (PCI) Data Security Standards (DSS). State and Federal law enforcement agencies have been notified and we have contacted the three major credit reporting agencies of the potential breach which should assist you should there be any erroneous entries on your credit report.

While we do not know if your information was compromised, we are contacting all of our customers who made a purchase on our website from December 1st 2009 through February 10th 2010 to warn them of the possibility. This is the period of time that we suspect that the vulnerability was exploited. We urge you to take action to monitor your credit card accounts in order to minimize your potential risk of illegal use of your cards and of identity theft. We also recommend that you check your credit report and consider placing a fraud alert statement to your credit file. You may also wish to place a freeze on your credit report. Please see the back of this page for further information and instructions for these and other actions.

We are deeply sorry for this lapse in security. We take your privacy and your trust very seriously and are committed to protecting your information from unauthorized access at every juncture.

Please contact me at paul@hbdirect.com or call me during regular business hour at 1/800/222-6872 if you have any questions (email is preferred).

Sincerely,  
Paul Ballyk, President

Below is a check list of suggestions you may wish to consider or investigate to see how you can best protect yourself.

1. Review your bank, credit card and debit card account statements over the next twelve to twenty-four months and immediately report any suspicious activity to your bank or credit union.

2. Monitor your credit reports with a major credit reporting agency. Below are the three major credit reporting agencies. Contact the credit reporting agency if you find:

- Accounts you did not open
- Inquiries from creditors that you did not initiate.
- Inaccurate personal information, such as home address or Social Security number

**Equifax**

1-800-685-1111  
P.O. Box 740241  
Atlanta, GA 30374-0241  
www.equifax.com

**Experian**

1-888-397-3742  
P.O. Box 2104  
Allen, TX 75013  
www.experian.com

**TransUnion**

1-800-916-8800  
P.O. Box 2000  
Chester, PA 19022  
www.transunion.com

3. If you do find suspicious activity on your credit reports or other account statements, call your local police or sheriff's office and file a **report of identity theft**. Get a copy of the police report as you may need this to clear up your records, and this may also give you access to some services that are free to identity theft victims.

4. If you find suspicious activity on your credit reports or on your other account statements, consider placing a **fraud alert** on your credit files so creditors will contact you before opening new accounts. To place the alert with all three agencies, contact any one of them by phone, or enter this URL in your browser.  
<https://www.experian.com/fraud/center.html>.

5. If you find suspicious activity on your credit reports or on your other account statements, consider placing a **security freeze** on your credit report so that the credit reporting agencies will not release information about your credit without your express authorization. A security freeze may cause a delay should you wish to obtain credit, but it does provide extra protection against an identity thief obtaining credit in your name without your knowledge. Additionally, it may cost a small fee to get or remove, but if you have filed a report with your state police, this service is free in most states. You can get more by contacting the credit bureaus at the following addresses:

**Experian:** <https://www.experian.com/freeze/center.html>

**Equifax:** [http://www.equifax.com/home/en\\_us](http://www.equifax.com/home/en_us) | Look under Fraud Alerts & Freeze

**TransUnion:** <http://www.transunion.com> | Look under Identity Theft

6. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you check your credit report for the next two years. In most states, you are eligible for a free credit report each year.