

May 27, 2008

Attorney General Douglas F. Gansler
200 St. Paul Place
Baltimore, MD 21202-2202

RE: Important Notice Regarding Potential Data Security Breach

Dear Attorney General:

On May 16, 2008, we were advised by the company that hosts our On-line Store website that an external virus (known as the SQL virus) accessed their server and may have attacked the credit card information of certain Altman Weil customers. Upon learning of this unauthorized breach and attack, on that same day, Altman Weil immediately authorized the hosting company to shut the site down so that access is no longer possible. We were told by the hosting company that the server on which the On-line Store resided was password protected and had current firewalls and security protection, but we understand that the SQL virus may nonetheless have accessed credit card information for 21 residents of MD.

We are actively investigating this attack and are also addressing this incident to fully determine the extent to which credit card information of our customers may have been accessed. We are looking for any help that your office or other state and/or federal agencies might be able to provide in assisting us to identify and pursue those responsible for this attack.

Here are the steps we have taken to date, we:

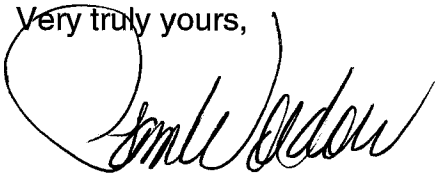
1. On May 16, 2008, notified the Merchant Bank, Bryn Mawr Trust of the potential security breach.
2. On May 16, 2008, learned that Bryn Mawr Trust outsources the actual credit card functions of the Merchant Bank to TransFirst.
3. On May 16, 2008, contacted TransFirst and notified it of the potential security breach and was informed that it would notify the three credit card companies, Visa, MasterCard and American Express.
4. On May 16, 2008, Altman Weil independently notified Visa, MasterCard, and American Express of the potential security breach.
5. On Saturday, May 24, 2008, notified all card holders whose cards were current (i.e. the expiration dates had not kicked in yet) by telephone calls placed.
6. Notified all card holders by letter of the situation and the possible risk, see attached generic sample letter dated between May 23 and May 27, 2008.

7. Notified the following law enforcement agencies:
 - a. Local police department located in Newtown Square, Pennsylvania, where Altman Weil is located on May 23, 2008.
 - b. Secret Service's ECTF and Electronic Crimes Working Group on May 24, 2008.
 - c. Every state Attorney General in the states where potentially affected cardholders reside on May 27, 2008.
 - d. Federal Trade Commission on May 27, 2008.
 - e. Office of Thrift Supervision on May 27, 2008.
 - f. Office of the Comptroller of the Currency on May 27, 2008.
 - g. Federal Deposit Insurance Corporation on May 27, 2008.
 - h. Board of Governors of the Federal Reserve System on May 27, 2008.
8. Assured that the hosting company has preserved logs and electronic evidence, has logged all actions taken, and has not altered or compromised the systems.
9. Retained forensic auditors at are own expense to undertake a thorough technical investigation of the cause and extent of the breach.
10. Committed to be back in touch with those customers who might be at risk with further information, once we have it.

If there are other agencies we should contact or other steps that your office recommends we take, please let us know.

Thank you very much for your assistance.

Very truly yours,



Pamela H. Woldow
General Counsel
Altman Weil, Inc.

Enclosure



Altman Weil, Inc.
Two Campus Blvd.
Newtown Square, PA 19073
610-886-2000 Fax: 610-359-0467
www.altmanweil.com

May 27, 2008

Personal and Confidential

RE: Important Notice Regarding _____ Credit Card Account # xxxxxxxx_____.

Dear Valued Customer:

On May 16, 2008, we were advised that an external virus accessed our On-line Store and may have accessed the credit card information of certain customers. Upon learning of this unauthorized breach and attack, we immediately shut the site down. While the server on which the On-line Store resides was password protected and had appropriate firewalls and security protection, this virus may nonetheless have accessed your credit card information

We are actively investigating this incident to fully determine the extent to which credit card information of our customers may have been accessed, and wanted to alert you that your credit card information may be at risk. You should therefore consider taking the following steps:

- 1) Notify your credit card company of the security issue and monitor your credit card account for suspicious activity;;
- 2) Place a fraud alert on your account with the three national credit bureaus Equifax: 800-525-6285; Experien: 888-EXPERIEN; TransUnion: 800-680-7289;
- 3) Obtain and review a free copy of your credit report. To order, visit annualcreditreport.com or call 1-877-322-8228;
- 4) Visit the Federal Trade Commission's web site (www.ftc.gov) for additional information on how to protect yourself.

We are also working with the appropriate law enforcement agencies to pursue those responsible for this attack. For more information contact JoAnn Miller at Altman Weil, Inc. at 610-886-2006.

Altman Weil, Inc.



FOR LETTERS GOING TO MARYLAND RESIDENTS

[Altman Weil Letterhead]

May ____, 2008

RE: Important Notice Regarding _____ Credit Card Account # xxxxxxxx _____.

Dear Valued Customer:

On May 16, 2008, we were advised that an external virus accessed our On-line Store and may have accessed the credit card information of certain customers. Upon learning of this unauthorized breach and attack, we immediately shut the site down. While the server on which the On-line Store resides was password protected and had appropriate firewalls and security protection, this virus may nonetheless have accessed your credit card information

We are actively investigating this incident to fully determine the extent to which credit card information of our customers may have been accessed, and wanted to alert you that your credit card information may be at risk. You should therefore consider taking the following steps:

- 1) notify your credit card company of the security issue and monitor your credit card account for suspicious activity
- 2) place a fraud alert on your account with the three national credit bureaus
Equifax: (800) 525-6285; Experien (888) 397-3742; TransUnion: (800)-680-7289
- 3) obtain and review a free copy of your credit report. To order, visit annualcreditreport.com or call 1-877-322-8228
- 4) contact the Maryland Attorney General at (410) 576-6300 or 1 (888) 743-0023 toll-free in Maryland, or at the website: http://www.oag.state.md.us/ to obtain information regarding steps to take to avoid identity theft
- 5) contact the Federal Trade Commission's web site (www.ftc.gov) for additional information on how to protect yourself from identity theft.

We are also working with the appropriate law enforcement agencies to pursue those responsible for this attack. For more information contact Joann Miller, at Altman Weil, Inc. at 610-886-2006, or via e-mail at: jamiller@altmanweil.com.

Altman Weil, Inc.