

October 23, 2014

Dear Customer:

We are writing to inform you of a recent data security incident which likely involved some of your personal information. As you made a purchase on our website, [www.sinclairinstitute.com](http://www.sinclairinstitute.com) between August 3, 2014 and August 28, 2014, your credit card information may be affected.

Keeping customer information secure is a top priority for us, and we deeply regret any inconvenience. We take this matter very seriously and we worked quickly to resolve the incident by putting our full resources behind this matter. The threat was removed from our site on August 28, 2014 and over the next weeks we added additional layers of security to prevent recurrence.

Although we have no reason to believe that your personal information has been or will be misused as a result of this incident, we are notifying you to advise you to remain vigilant by reviewing your account statements (including but not limited to bank, credit card and debit card statements) and monitoring free credit reports.

Attached is some helpful information and credit reporting resources for your review. If you feel you need further information or assistance after reviewing this letter and the referenced materials, please contact our Customer Service Director, Al Cole at 919-644-8100, extension 3192 during normal business hours.

On behalf of *The Sinclair Institute*, I wish to express our sincere regret that this incident occurred and any inconvenience or concern it may cause you. Please be assured that we take our role in safeguarding your personal information very seriously, and that we have taken all appropriate measures to address the cause of the issue and to prevent a recurrence.

Thank you for your understanding.

Sincerely,

David Groves,  
President

### What happened?

We were informed by our hosting partner on August 28, 2014 that login information and customer information for some of Sinclair's customers had likely been illegally obtained. We were informed that the breach began on August 3, 2014 when certain computer files were modified without authorization so as to allow customer information to be illegally accessed. Customer information involved included login codes and passwords, customer name and address, birthday, phone number, email address and credit card information (credit card number, expiration date and CVV). We requested and obtained copies of the affected files from our hosting partner and launched an internal investigation to independently verify the nature and scope of the incident and confirm that personal information was no longer accessible. We also contacted the FBI to report the incident.

### Who should I contact?

If you find any suspicious activity on your credit reports or on an account statement, or have reason to believe your information is being misused, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to your local law enforcement authorities, your state's attorney general and/or the Federal Trade Commission. To file a complaint with the FTC, go to [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (877-438-4338).

You should consider placing a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open new accounts or change your existing accounts. You may call any one of the three major credit reporting companies listed below to confirm your fraud alert. Once one credit reporting company confirms the alert, the other two are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

**Experian:** 1-888-397-3742; [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013

**Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374

**TransUnion:** 1800 680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division; P.O. Box 6790, Fullerton, CA 92834.

Additional information is available at [www.annualcreditreport.com](http://www.annualcreditreport.com).

### What else can I do to protect myself?

To further protect yourself, you may have the right to put a credit freeze, also known as a security freeze, on your credit file. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

Further information on fraud alerts and security freezes, as well as further information on how to protect yourself from identity theft, is available from each of the credit reporting companies listed above, and from the Federal Trade Commission ("FTC") at [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/). You may also contact the FTC at 877-438-4338 or by writing to the FTC at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.