8/12/2014
Dear {customer name}:

We want to make you aware that TheNaturalOnline.com has recently been the victim of unauthorized access to our customers' payment card data. This unauthorized access may impact guests who made credit or debit card purchases online or by phone from 4/22/2014 to 7/17/2014. Your trust is a top priority at The Natural, and we deeply regret the inconvenience this security breach may cause you. The privacy and protection of your information is something we take very seriously, and we have worked swiftly to resolve the incident.

We began investigating the incident as soon as we learned of it, and have determined that compromised information included customers' credit and debit card numbers and expiration dates, as well as names, addresses, and phone numbers. Account numbers and passwords used during the above purchase period may have also been affected.

Our security team continues to investigate this infringement and is thoroughly examining additional measures we can take to prevent future incidents. Additionally, we alerted financial institutions immediately after confirming the unauthorized access and are currently putting our resources behind these efforts.

We recommend that you change your password at TheNaturalOnline.com and review the enclosed *Data Breach FAQ* and *Information about Identity Theft Protection* to help guard you against identity theft or fraud.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months, at no cost to you. The following identity protection services start on the date of this notice and can be used any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready to help safeguard your identity, and is automatically available to you with no enrollment required. If a problem arises, simply call (877) 615-3771, provide the Reference Code **redemption_code-value-goes-here**, and a dedicated investigator will help recover any financial losses, reestablish your credit, and make sure your identity is properly restored. AllClear ID maintains an A+ rating at the Better Business Bureau.

We understand that a situation like this creates stress and anxiety regarding the safety of your credit or debit card data at The Natural. Our brand has been built on a foundation of trust with our guests, and we want to reassure you that the cause of this issue has been addressed. Please be assured that you can continue to shop with confidence at TheNaturalonline.com.

If you have further questions or concerns about this incident, feel free to contact The Natural assistance line at (877) 615-3771. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Nick Barretta, CEO
The Natural

Data Breach FAQ:

1. What happened?

On July 15 2014, we learned that criminals forced their way into our system, gaining access to guest credit /debit card information and personal information.

2. What specific information may have been disclosed about me?

- Customer name
- Credit or debit card number
- The card's expiration date
- CVV
- Customer address
- Customer email
- Phone number
- Password used to create an account, if an account was created

3. Where did this happen and why was my information in this place?

This happened at TheNaturalOnline.com and the information was there because you made a purchase and used your credit/debit card to pay between the dates of 4/22/2014 to 7/17/2014.

4. What did you do when the information was accessed?

We immediately started a forensic investigation and on 7/17/2014 we closed the access point that the criminals used and removed the malware they left behind.

5. What are you doing about this so it does not happen again?

We closed the access point that the criminals used and we implemented additional security measures and procedures to reduce the likelihood that this ever happens again.

6. Were there other individuals affected by this breach, or am I the only one?

Yes, there were other users that were affected by the breach.

7. What does it mean if my information was stolen? What are the risks?

The primary risk is credit card fraud and increased exposure to consumer scams, such as; phishing, web scams and social engineering. We want to help our guests protect themselves by providing information and resources about these scams. See below for more details.

8. Was my spouse or other family members' information also affected?

If they shopped with their credit/debit card at TheNaturaOnline.com from 4/22/2014 to 7/17/2014 then they may have been affected, otherwise they should have not been affected.

9. Has the person who accessed the information been caught?

No, but we are continuing to conduct a thorough investigation.

10. Have you notified the police?

No, but The Natural notified the necessary credit card companies, credit bureaus and attorney generals.

11. Will we receive any additional information or updates?

We continue to conduct a thorough investigation and are committed to updating you on developments that could impact you.

12. What kind of scams do I need to watch out for?

Following an event like a data breach, it's common to see fraudsters use emails, texts, phone calls and fake websites to try to steal your personal information.

- **Social Engineering:** Using fraud or deception to manipulate people into performing actions or divulging information that they would normally not share.
- **Social Engineer:** A scam artist who contacts individuals via phone, email, text message or even in person to gather information for the purposes of fraud, data system access, identity theft and more.
- **Phishing:** A social engineer uses a fake email to trick recipients into giving up credit card information, passwords or other sensitive information. The email may appear to come from a trusted source, such as a reputable company or bank, and often includes personal details so it appears the sender knows you.
- **Smishing:** Similar to Phishing (see above), a social engineer sends a fake Short Message Service (SMS) text message to your cell phone, announcing that you've won a prize or offer from a trusted company or bank if you follow a link to a website and enter a code. Clicking the link can expose your phone to malware.
- **Pretexting:** When a social engineer impersonates someone with authority and creates a fake scenario to trick unsuspecting individuals into sharing private or sensitive information.

13. What are some things I can do to avoid social engineering scams?

- Never give out private or personal information, including financial details, unless you can verify the identity of the person or organization contacting you.
- Don't respond to texts or emails coming from a contact you don't recognize, and don't click on links. Instead, if you need to check on your account, type the site address you want to visit into your browser and securely log into your account.
- Don't send money to strangers; scam artists often insist that you wire money, especially overseas, because it's difficult to trace the transaction.
- Keep an eye on your monthly statements. If your account information is stolen, fraudsters can use it to charge purchases or commit crimes in your name. Watch for unusual charges such as "membership fees" and other goods or services you didn't authorize. If you see a charge you don't recognize, contact your account provider immediately.

14. What are some red flags that indicate I might be dealing with a social engineer?

Some common red flags that help identify a social engineer include:
- Refusal to provide contact or call-back information
- Acting rushed, pressed for time or intimidating
- Name-dropping
- Extremely friendly
- May seem to know some personal information already, but is asking for more
- Poor grammar or spelling
- The links or attachments in an email seem suspicious

15. What should I do if I suspect I've been contacted by a social engineer?

If you think you may have been scammed, there are a number of things you can do to protect yourself:

-Report the incident to the Federal Trade Commission, or, if you live outside the U.S., file a complaint at www.econsumer.gov. You can also report scams to your state Attorney General.
- Forward email spam to spam@uce.gov.

16. Does The Natural stores my credit card information?

We do not store any of your sensitive credit card information on our servers. We utilize a secure third party service (authorize.net) to maintain your credit card data.

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338),
www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity

theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

The next 2 paragraphs are regarding incidents involving personal health information. Disregard if not applicable to your situation.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. 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. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a

security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

Terms of Use for AllClear Secure

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:
* Automatic 12 months of coverage;
* No cost to you - ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident, eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Secure services, you must:

* Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
* Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
* Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
* Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

* Due to
- Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
-Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
* Incurred by you from an Event that did not occur during your coverage period;
* In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.
Other Exclusions:
* AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
* AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy;

AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur;
* AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud; and
* You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to "phishing" scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail: support@allclearid.com
Mail: AllClear ID, Inc., 823 Congress Avenue Suite 300, Austin, Texas 78701
Phone: 1.855.434.8077