TOTAL PHASE

STATE OF NH
DEPT OF JUSTICE
2017 APR 13 AM 11:23

March 24, 2017

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Notice of Data Security Incident

Dear Madam / Sir:

On March 16, 2017, Total Phase discovered that it had been the victim of a cyber attack. Cyber attackers installed unauthorized code on our website to harvest information from customers' web browsers during the checkout process.

The attack affected customers who placed orders or entered information on Total Phase's online store checkout pages from March 10 through March 16. The potentially compromised data is limited to information entered on the checkout pages of Total Phase's online store.

This information included the customer name, billing and shipping addresses, credit card number, expiration date and CVV, company name, and phone number. Their Total Phase username and password may also have been compromised if they were entered on the checkout page during the impacted time period.

A total of 1 resident of New Hampshire was affected in this attack.

There is no evidence that the attackers gained access to data stored in any Total Phase database. Total Phase does not store customer credit card information. Therefore, credit card information that was not used in the checkout process during the impacted time period would not have been disclosed.

In response to this incident, Total Phase promptly halted access to our website. All instances of the unauthorized code were removed and a security audit was performed to verify the integrity of our servers. As a precautionary measure, all affected users had their password reset.

On March 24, 2017, Total Phase sent email notices to the affected users to inform them of the breach and to be vigilant for credit card fraud.

A copy of the notice is attached. In the notice, Total Phase offered 12 months of identity monitoring services from Experian at no cost to the affected user. Total Phase has also created an internal working group to support the affected users.

Best regards,

Gil Ben-Dov
CEO, Total Phase, Inc.

Enclosure

2350 Mission College Boulevard • Suite 1100 • Santa Clara, CA 95054
Phone +1-408-850-6550 • www.totalphase.com

TOTALPHASE

March 28, 2017

«FirstLastname»
«Company_»
«billaddr1»
«billaddr2»
«billcity», «billstate» «billzip»

Dear «firstname»,

Total Phase is writing to inform you of a recent incident affecting the security of your personal information when you placed an order on Total Phase's website. We value your privacy and deeply regret that this incident occurred.

What Happened?
On March 16, 2017, Total Phase discovered that it had been the victim of a cyber attack. Cyber attackers installed unauthorized code on our website to harvest information from customers' web browsers during the checkout process on Total Phase's website.

When Total Phase learned of this breach, we promptly halted access to our website. All instances of the unauthorized code were removed and a security audit was performed to verify the integrity of our servers.

The attack affected customers who placed orders or entered information on Total Phase's online store checkout pages from March 10 through March 16. You are receiving this notice because you placed an order or started but did not complete an order during those dates.

What Information Was Involved?
The attack involved the capture of information from customers' web browsers during the checkout process on Total Phase's online e-commerce site. The potentially compromised data is limited to information entered on the checkout pages of Total Phase's online store.

This information included your name, billing and shipping addresses, credit card number, expiration date and CVV, company name, and phone number. Your Total Phase username and password may also have been compromised if they were entered on the checkout page during the impacted time period.

There is no evidence that the attackers gained access to data stored in any Total Phase database. Total Phase does not store customer credit card information. Therefore, credit card information that was not used in the checkout process during the impacted time period would not have been disclosed.

2350 Mission College Boulevard • Suite 1100 • Santa Clara, CA 95054
Phone +1-408-850-6550 • www.totalphase.com

TOTALPHASE

What Are We Doing?
We have identified the cause of the incident and are investing in our systems and security processes to prevent another incident from occurring.

As a precautionary measure, we have reset the password of your Total Phase account. You will need to generate a new password by clicking on the "Forgot your password?" link on the login page.

We also want to ensure that you have resources to protect your personal information. Total Phase is working with Experian to provide you with a one-year membership to a fraud resolution service at no cost to you. For more details, please see the information below.

What You Can Do
As mentioned above, you can sign up for one year of identity protection service at no cost by following the instructions in this letter. We also recommend that you monitor your credit card statements for suspicious activity. In addition, we have provided more information below on measures that you may want to take to protect your identity.

For More Information
Maintaining the integrity of our customers' personal information is extremely important to us. We sincerely apologize for any inconvenience that this incident has caused and are committed to keeping you informed of any important developments in the investigation.

To receive your activation code or if you have any questions, please do not hesitate to contact us by email at websecurity@totalphase.com.

Sincerely,

Gil Ben-Dov
CEO, Total Phase
www.totalphase.com

TOTALPHASE

Enrolling in Experian IdentityWorks

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks℠ as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Email us at websecurity@totalphase.com to request your activation code.
- Visit the Experian IdentityWorks website to enroll - www.experianidworks.com/3bcreditone
- Enroll by June 30, 2017 (Your code will not work after this date.)

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by June 30, 2017. Be prepared to provide engagement number DB01119 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only*
- Credit Monitoring: Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE™: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

TOTALPHASE

Protective Measures You Can Take

The following resources are available to help you protect your personal information and monitor your accounts for suspicious activity.

Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling 877-322-8228 or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

When you receive your credit report(s), please review them carefully. Look for any accounts you did not open, requests for your credit report from anyone that you did not apply for credit with, or inaccuracies regarding your personal identifying information, such as your home address or social security number. If you see anything you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report or listed below and ask them to have information relating to fraudulent transactions deleted:

Experian	Equifax	TransUnion
P.O. Box 9554	P.O. Box 740256	P.O. Box 6790
Allen, TX 75013	Atlanta, GA 30374	Fullerton, CA 92834
www.experian.com	www.equifax.com	www.transunion.com
888-397-3742	800-525-6285	800-680-7289

Additionally, you can obtain information from the Federal Trade Commission about taking steps to avoid identity theft at: http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Flagging Your Credit Report

To further protect you from the possibility of identity theft, each of the national credit reporting agencies provides the ability to place a fraud alert or security freeze on your credit files. A fraud alert notifies any creditors that access your credit report that you may be the victim of fraud and encourages them to take additional steps to protect you from fraud. Placing a fraud alert is as simple as calling the numbers above for each or any of the credit reporting agencies and requesting that a fraud alert be placed on your credit file. Whether or not you find any signs of fraud on your credit reports, we recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should also remain vigilant over the next two years by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.