



November 28, 2017

VIA OVERNIGHT DELIVERY

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED
NOV 29 2017
CONSUMER PROTECTION

To Whom It May Concern:

Pursuant to your state's law, The Image Group hereby notifies your office of an incident that could potentially affect the personal information of one (1) New Hampshire resident.

On approximately November 17, 2017, The Image Group discovered and promptly resolved a temporary security vulnerability on our eCommerce platform. The company had been using Payflow Pro tokenization for payment card processing but, upon inspection, learned that Payflow Pro contained a vulnerability that allowed some credit card numbers to be susceptible to interception while in transit to Paypal between October 17, 2017 and November 17, 2017. During this period of time, the following information related to certain The Image Group customers may have been vulnerable to unauthorized access: name, email address, delivery/billing address, credit card type, and credit card number.

The Image Group immediately launched a comprehensive review to investigate and remediate the intrusion, including engaging a third-party expert and notifying the Federal Bureau of Investigation. The company also upgraded to a different PayPal payment card processing system that does not contain such vulnerability to prevent this from happening again. Since The Image Group transitioned to this new system, it has detected no additional suspicious activity.

The Image Group is providing direct notification to the one (1) New Hampshire customer who may have been affected.

Accordingly, please find enclosed a copy of the written notice sent to the New Hampshire resident on November 28, 2017.

Sincerely,

Lisa Hoverson
Chief Financial Officer
Enclosures

1255 Corporate Drive • Holland, OH 43528
419.866.3300 • 800.860.2111 • fax 419.866.3309

TOLEDO • CLEVELAND • ANN ARBOR • COLUMBUS



1255 Corporate Drive • Holland, OH 43528

Chris Dingee
463 Winnacunnet Rd Apt 310
Hampton, NH 03842

NOTICE OF A DATA INCIDENT

11/28/2017

Dear Chris,

WHAT HAPPENED?

On approximately November 17, 2017, The Image Group discovered and promptly resolved a temporary security vulnerability on our eCommerce platform. The company had been using Payflow Pro tokenization for payment card processing but, upon inspection, learned that Payflow Pro contained a vulnerability that allowed some credit card numbers to be susceptible to interception while in transit to Paypal between October 17, 2017 and November 17, 2017.

WHAT INFORMATION WAS INVOLVED?

We are sending you this letter as a cautionary measure because we believe that certain information about you -- your name, email address, delivery/billing address, credit card type, and credit card number -- may have been vulnerable to unauthorized access.

WHAT ARE WE DOING?

The Image Group regrets this incident, and immediately launched a comprehensive review to investigate and remediate the intrusion, including engaging a third-party expert and notifying the Federal Bureau of Investigation. The company also upgraded to a different PayPal payment card processing system that does not contain such vulnerability to prevent this from happening again. Since The Image Group transitioned to this new system, it has detected no additional suspicious activity.

FOR MORE INFORMATION

For further information and assistance, please contact The Image Group toll-free at 888-780-8316 between 8 a.m. to 5 p.m. EST Monday through Friday.

WHAT YOU CAN DO

Additionally, we have enclosed information on steps you can take to further protect your information.

The Image Group takes this matter very seriously and deeply regrets any inconvenience or concern that this matter may cause you.

Sincerely,

The Image Group

Lisa Hoverson
Chief Financial Officer

WHAT YOU CAN DO

Review Your Account Statements. As a precautionary measure, we recommend that you review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, or the Federal Trade Commission. In some states, you may also obtain a police report regarding this incident.

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the 3 major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>. Or you can elect to purchase a copy of your credit report and optional remediation services by contacting one of the three national credit reporting agencies shown below.

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016
---	--	---

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.IdentityTheft.gov> or call 1-877-ID-THEFT (877-438-4338). **North Carolina residents** may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.

Consider Placing a Fraud Alert on Your Credit Report. You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

OTHER IMPORTANT INFORMATION

Security Freeze. In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, cell phone, or any service that requires a credit check. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift, or remove the security freeze; however, this fee may be less in certain states (in MA, up to \$5). In order to place a security free, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. You must separately place a security freeze on your credit file with each credit reporting agency.