bluemercury, inc.

NOTICE OF DATA BREACH

February 22, 2017

On behalf of Bluemercury, I am writing to inform you about a recent incident involving unauthorized access of personal information about you. You may have received this information via an email. We regret that this incident occurred and appreciate your time to read this letter.

WHAT HAPPENED?

On February 7, 2017, we were informed that Aptos, our former digital platform provider, experienced a security incident last year that involved certain of its retail customers' websites, including www.bluemercury.com. Aptos has indicated intrusions to some of their systems began in February 2016 and ended in December 2016. During that time, we understand that cyber criminals placed malware on Aptos' servers and gained unauthorized access to Bluemercury's data. Although we ended our relationship with Aptos in September 2016, we have been assured that the malware has been removed and that the criminals no longer have access to their systems or data.

Aptos did not discover the intrusion until November 28, 2016. We understand that Aptos contacted Federal law enforcement agencies and the U.S. Department of Justice at that time. We also understand that Aptos was requested by law enforcement to delay notifying its retailer customers, including Bluemercury, so as not to interfere with their ongoing investigation. We also understand that law enforcement continues to investigate this incident.

WHAT INFORMATION WAS INVOLVED?

Aptos has informed us that attackers had access to data associated with approximately 54,000 client orders made before September 12, 2016 to include: First and Last Name; Address; Phone Number; Email; Address; and Debit or Credit Card Number with expiration dates. Aptos has indicated that no Credit Verification Values (CVV) or Social Security Numbers (SSN) associated with Bluemercury clients were retained or accessed.

WHAT ARE WE DOING?

We ended our relationship with Aptos in September 2016 for unrelated reasons. We have been working with Aptos to learn more about the incident. Aptos has indicated it retained a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard information. We have instructed Aptos to destroy any and all remaining Bluemercury client data.

WHAT CAN YOU DO?

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring credit reports. We recommend you immediately contact your credit or debit card company and inform them that your card information may have been compromised. Your bank or credit card provider will suggest appropriate steps to protect your account. You should review your bank and card statements regularly, and immediately report any suspicious activity to your bank or credit card provider. Payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

We at Bluemercury value our client relationship, appreciate your business and would like to provide as much assistance as we can. Just like it is a good practice to monitor your bank accounts, it is a good practice to monitor your identity. Therefore, as an additional service for our clients, we have arranged to have AllClear ID (www.allclearid.com) provide identity protection support for 12 months at no cost to you. AllClear ID's Identity Repair services are available to you starting on the date of this notice and can be used at any time during the next 12 months. This service is automatically available to you with no enrollment required. As you monitor your credit, if you spot a problem, simply call AllClear ID at 1-855-336-6688, provide your Reference Code {Reference_Code} and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

CONTACTING THE FEDERAL TRADE COMMISSION, LAW ENFORCEMENT & THE CREDIT BUREAUS

In addition, you may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.consumer.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 916-8800
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.equifax.com	www.experian.com	Chester, PA 19022
		www.transunion.com

You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:

(1) Equifax – (800) 349-9960
(2) Experian – (888) 397-3742
(3) TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number and other personal information. The fee to place a credit freeze varies based on where you live. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION

We regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact our support agents for this event at 1-855-336-6688 if you have any questions or concerns.

Sincerely,

Bernard LO Locft

Bernard F. Locraft,
Corporate Controller
Bluemercury, Inc
1010 Wisconsin Ave NW, #700,
Washington, District of Columbia 20007

ADDITIONAL INFORMATION FOR SOME STATES

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

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

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: Please contact state or local law enforcement to determine whether you can file or obtain a police report in regard to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/