MULLEN COUGHLIN LLC

Jim Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 29, 2016

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

Our office represents SwervePoint, LLC ("SwervePoint"), 75 Sylvan Street, Danvers, MA 01923. We are writing to provide you with notice of an event that may impact the security of personal information relating to sixteen (16) New Hampshire residents. By providing this notice, SwervePoint, LLC does not waive any rights or defenses regarding the applicability of New Hampshire law, applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Background

On October 6, 2016, SwervePoint discovered that an unidentified third party had injected malicious code into its e-commerce platform. The e-commerce platform is used to host customer company websites that sell company-branded merchandise. The malicious code enabled the unidentified third party to acquire credit card information while the purchase took place. Our investigation revealed that this exploit existed on the e-commerce platform between February 10, 2016 and June 2, 2016. The investigation revealed no evidence of the malicious code in our current environment and no evidence of unauthorized access to any other customer information.

The information that may have been obtained by the unidentified third party included individuals' names, billing addresses, full credit card numbers, expiration date and CVV numbers. Individuals' email address and SwervePoint-hosted company store password may also have been obtained.

Notice to New Hampshire Residents

While the investigation is ongoing, the personal information of sixteen (16) New Hampshire was contained in an account accessed by the unauthorized third party. On November 29, 2016, SwervePoint mailed written notice of this incident to the affected individuals in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

SwervePoint worked with third party investigators to confirm the timeframe and scope of the incident and to ensure the malicious code had been removed. We also worked with the investigators, along with other subject matter experts, to ensure the security of our customers' data and to implement a remediation plan to improve security in our network. We are notifying credit card issuers to make them aware of the issue.

In addition to the steps taken above, we are also providing notice of this incident to you, along with information on how to better protect against identity theft and fraud. We are also offering affected individuals a fraud-prevention product: one year of CSID Protector services, which includes CyberAgent® Internet Surveillance, Identity Theft Insurance and Identity Restoration coverage.

In addition to providing notice of this incident to your office, SwervePoint is providing notice of this incident to other regulators and consumer reporting agencies where required.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 267-930-4798.

Very truly yours,

Jim Prendergast of
MULLEN COUGHLIN LLC

JP:hp
Enclosure

EXHIBIT A

SwervePoint
THE COMMUNICATIONS MERCHANDISE FIRM

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>:

SwervePoint, LLC ("SwervePoint"), the host and operator of the <<CLIENT>>, is writing to inform you of an incident that may affect the security of the credit card(s) that you used to make one or more purchases from the <<CLIENT>> earlier this year. We are providing this notice to ensure that you are aware of the incident so that you may take steps to protect your financial information.

What Happened? On October 6, 2016, SwervePoint discovered that an unidentified third party had injected malicious code into its e-commerce platform used on the <<CLIENT>>. The malicious code enabled the unidentified third party to acquire credit card information while the purchase took place. Our investigation revealed that this exploit existed on the <<CLIENT>> site between February 10, 2016 and June 2, 2016. The preliminary investigation revealed no evidence of the malicious code in our current environment and no evidence of unauthorized access to any other customer information.

What Information Was Involved? The information that may have been obtained by the unidentified third party included your name, billing address, full credit card number, expiration date and CVV number. Your email address and <<CLIENT>> password may also have been obtained.

What is SwervePoint Doing? SwervePoint takes the security of its customers' financial information extremely seriously. Upon learning of this incident, we worked with third party investigators to confirm the timeframe and scope of the incident and to ensure the malicious code had been removed. We also worked with the investigators, along with other subject matter experts, to ensure the security of our customers' data and to implement a remediation plan to improve security in our network. We are notifying credit card issuers to make them aware of the issue.

In addition to the steps taken above, we are also providing notice of this incident to you, along with information on how to better protect against identity theft and fraud. We are also offering you a fraud-prevention product: one year of CSID Protector services, which includes CyberAgent® Internet Surveillance, Identity Theft Insurance and Identity Restoration coverage at no cost to you. The enclosed Privacy Safeguards contains information on protecting against identity theft and fraud and instructions on how to enroll and receive the complimentary credit monitoring and identity restoration services.

What Can You Do? Remain vigilant for potential unauthorized activity by regularly reviewing your account statements, and promptly reporting any suspicious activity. We also encourage you to regularly change your online account passwords. You should review the additional information included in the attached Privacy Safeguards on how to better protect against identity theft and fraud. You can also enroll to receive the complimentary access to one year of CSID Protector services.

For More Information. Should you have any questions regarding this incident, please call 844-319-9618 Monday through Friday, 9:00 am – 9:00 pm ET.

We apologize for the inconvenience this incident has caused you. We want to assure you that we continue to take appropriate actions to protect the privacy and security of your information.

Sincerely,

Kevin Phoenix
Principal, Operations & Administration

PRIVACY SAFEGUARDS

To help you monitor your information, we are providing you with one year of CSID Protector services, which includes CyberAgent® Internet Surveillance, Identity Theft Insurance and Identity Restoration coverage at no cost to you. If you are a victim of fraud, simply call CSID at (877) 926-1113 by **November 12, 2017**, and a dedicated Identity Theft Restoration agent will help you restore your identity. Please provide the PIN Code below as proof of eligibility.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate your CSID Protector coverage. The sign-up process is conducted online via CSID's secure website https://www.csid.com/csid1yprotector/. You will need your individual CSID PIN Code <<Code>>. This PIN Code can only be used once and cannot be transferred to another individual. Once you have provided your PIN Code, you will be prompted to answer a few security questions to authenticate your identity, including: previous addresses, names of creditors and payment amounts.

Should you have any questions regarding the coverage or the sign-up process, please contact CSID Member Services at (877) 926-1113 or email support@csid.com. Once you have enrolled and created your username and password, you will return to CSID's page to log in and access your personal information on future visits.

You may take action directly to further protect against possible identity theft or financial loss. We encourage you to regularly change all your Internet passwords. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	www.transunion.com/securityfreeze
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	1-888-909-8872
www.equifax.com/help/credit-freeze/en_cp		

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. For Rhode Island residents, the Attorney General's office can be contacted at http://www.riag.ri.gov/index.php, consumers@riag.ri.gov or (401) 274-4400.