MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

Drummers Lane, Suite 302
Wayne, PA 19087

October 27, 2017

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL:

Attorney General Gordon J. MacDonald
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 MacDonald:

Our office represents Interstate Plastics, Inc. ("Interstate Plastics"), 3299 Ramos Circle, Sacramento, California 95827. We are writing to provide you with notice of an event that may impact the security of personal information relating to approximately seventeen (17) New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Interstate Plastics does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Background

On or around July 24, 2017, Interstate Plastics identified suspicious code on its e-commerce website, www.interstateplastics.com, and determined it was a sign of a sophisticated cyber-attack. Interstate Plastics removed the code and began investigating with the assistance of third-party forensic investigators. Additional malicious code was identified and removed on August 25, 2017. It was determined that the code was capable of collecting payment information entered into the website's customer check out page by customers. The investigation further determined that this incident may impact payment cards used to make purchases on the e-commerce site between May 29, 2017, and August 25, 2017. This incident did not impact customer information received by Interstate Plastics via phone orders.

The investigation determined the only customer information collected by the malware was customer name, address, card number, expiration date, and CVV. Interstate Plastics' investigation found evidence that information relating to e-commerce customers who made purchases between May 29, 2017, and August 25, 2017, may have been collected by the malware. Additionally, the investigation was unable to rule out that an unauthorized actor may have also accessed a database containing customer information, including name address, card number, expiration date, and CVV, from certain transactions earlier than July 24, 2017. Therefore, in an abundance of caution, Interstate Plastics is providing notice to these customers as well.

Notice to New Hampshire Residents

On October 27, 2017, Interstate Plastics mailed written notice to approximately seventeen (17) New Hampshire residents whose payment card information may be affected by this incident. Such notice is being provided in substantially the same form as the letter template attached here as ***Exhibit A***.

Other Steps Taken and to Be Taken

In addition to written notice of this incident, Interstate Plastics is providing impacted and potentially impacted individuals with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file, the contact information for the national consumer reporting agencies, how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

Interstate Plastics is also providing written notice of this incident to other state regulators and the major consumer reporting agencies, as necessary.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 267-930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL:atw
Enclosure

EXHIBIT A

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name1>>,

We recently learned that we were the victims of a sophisticated cyber-attack that may affect the security of your payment information. As such, we are providing you with information about the incident, steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? We have been investigating unusual code on the e-commerce section of www.interstateplastics.com with third-party forensic investigators to determine what the code does and how it was placed on our e-commerce site. On or around July 24, 2017, we identified suspicious code on our e-commerce site and determined it was a sign of a sophisticated cyber-attack. We removed the code and began investigating with the assistance of third-party forensic investigators. Additional malicious code was identified and removed on August 25, 2017. It was determined that the code was capable of collecting payment information entered into our online check out page. The investigation further determined that this incident may impact payment cards used to make purchases on our e-commerce site between May 29, 2017 and August 25, 2017. The investigation also determined a database containing customer payment information from certain transactions earlier than July 24, 2017, may have been subject to unauthorized access. This incident did not impact phone orders.

What Information Was Involved? Since discovering the code, we have been working with the third-party forensic investigators to determine what happened, what information was affected and to whom that information may relate. The investigation has determined the following information could be collected by the malicious code: name, address, card number, expiration date, and CVV. This same type of information was contained in the database that also may have been subject to unauthorized access. You are receiving this notice because your payment information was potentially collected by the malware and/or your payment information was contained in the database.

What We Are Doing. We take this event, and the security of your information, seriously. In addition to taking the steps detailed above and providing notice to you, we have implemented additional procedures to further protect the security of customer debit and credit cards including the removal of the malicious code at issue. In addition, we continue to work with third-party forensic investigators to ensure the security of our systems and will continue to work to secure your information in the future. We are also notifying certain state regulators of this incident as required.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Your Information* for additional information on how to better protect against identity theft and fraud. We encourage you to remain vigilant against incidents of identity theft by reviewing your account statements regularly and monitoring your credit reports for suspicious activity.

For More Information. The trust of our customers is paramount to us. Should you have any questions about the content of this letter or ways you can better protect yourself from the possibility of identity theft, we encourage you to call the dedicated assistance line, staffed by professionals who are experienced in working through situations like this, at 888-201-6144 between 9:00 a.m. and 9:00 p.m. EST, Monday through Friday, excluding major holidays.

Sincerely,

Cole Klokkevold,
CEO

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports 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
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
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, lift 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
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call 1-800-349-9960)
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
PO Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 10 Rhode Island residents may be impacted by this incident. Customers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, customers will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed as a result of a law enforcement investigation.