# MORRISON MAHONEY LLP

COUNSELLORS AT LAW

[redacted]

B[redacted]

MASSACHUSETTS
BOSTON
FALL RIVER
SPRINGFIELD
WORCESTER

CONNECTICUT
HARTFORD

ENGLAND
LONDON

NEW HAMPSHIRE
MANCHESTER

NEW JERSEY
PARSIPPANY

NEW YORK
NEW YORK

RHODE ISLAND
PROVIDENCE

December 18, 2014

STATE OF NH
DEPT OF JUSTICE
2014 DEC 22 AM 11:58

NH Department of Justice
33 Capitol Street
Concord, NH 03301
Attn.: Security Breach Notification

Dear Sir or Madam:

We represent ID Parts, LLC, a Massachusetts limited liability company (the "Company") that owns and operates a website for the sales of automotive parts (IDParts.com). We are writing to notify you of a breach of security involving the credit card information of approximately 12,000 individuals, including 200 New Hampshire residents. Upon discovering the breach of security, the Company promptly took measures to protect the type of information that was involved in the incident.

On October 28, 2014, the Company discovered that malicious code had been inserted into the functions that process customer payment information through their website. Without their knowledge or consent, this malicious code took customer credit card numbers, expiration dates and CVV/CVV2 security codes when such information was entered by customers as part of the electronic ordering process and then transmitted the information via e-mail to an unknown third party. From the Company's investigation, it does not appear that the malicious code captured or e-mailed any customer names, addresses or phone numbers. Also, purchases made using PayPal, check or money order or a credit card saved to the customer's account gateway were not targeted or affected by the malicious code.

The Company has not been able to determine the exact date on which the malicious code was inserted into their website or the precise method by which their computer system was hacked. In or around early October 2014, Company was first alerted to a potential security breach by American Express, who had identified the Company's website as a common point of purchase in a fraud investigation. The Company believes that the credit card information obtained through the malicious code was used to submit fraudulent chargers to customer accounts. Following that notification from American Express, the Company undertook a prompt

investigation, which suggests that the hack and insertion of malicious code into their website occurred in January 2014.

The malicious code was immediately disabled upon discovery on October 28, 2014. At that time, the Company isolated the code in a development environment for investigation and testing. The Company also conducted a server-wide search of related code and did not identify any additional instances of the malicious code. The Company has since changed the passwords on all system accounts associated with their domain. Based on server access logs, it does not appear that any unauthorized user currently has access to the server. The Company is undertaking a thorough review of their data security policies and procedures to protect against the unauthorized access to customer information and reduce the likelihood of the recurrence of the similar attacks in the future.

Because the Company does not store or maintain customer credit card information with customer names and addresses, the Company needed to match credit cards used during the relevant time frame to specific customers using the last four digits of the credit card numbers. Through this process, they have identified 200 New Hampshire residents that may have been affected by this breach of security. Given the nature of the incident, the Company has notified the three major credit reporting agencies but has not made a report to law enforcement.

In accordance with New Hampshire's data security law, the Company is undertaking to notify the New Hampshire residents that may have been affected by this breach of security. A copy of the form of notification letter that the Company is sending to New Hampshire residents is enclosed. We anticipate that these mailings will be completed by December 22, 2014.

Should you have any questions or need further information about our investigation or notification, please contact me or my colleague Matthew Henning.

Sincerely,

Rachel M. Davison

Enclosure

IDParts.com
90 Corporate Park Drive
Pembroke MA 02359
www.idparts.com

December 22, 2014

##A6792-L01-0000001 T- 00000001 **********3-DIGIT 159
SAMPLE A SAMPLE
APT ABC
123 ANY STREET
ANYTOWN, US 12345-6789

Dear Sample A Sample:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to notify you of a breach of security that may have involved information from your credit card ending in 6789. To our knowledge, the breach of security did not involve your name, address or phone number. Upon discovering the breach of security, we promptly took measures to protect the type of information that was involved in the incident.

On October 28, 2014, we discovered that malicious code had been inserted into the functions that process customer payment information through our website (IDParts.com). Without our knowledge or consent, this malicious code took customer credit card numbers, expiration dates and CVV/CVV2 security codes when such information was entered by customers as part of the electronic ordering process and then transmitted the information via e-mail to an unknown third party. It does not appear that the malicious code captured any customer names, addresses or phone numbers. Also, purchases made using PayPal, check or money order or a credit card saved to the customer's account gateway were not targeted or affected by the malicious code. The information currently available suggests that the hack and insertion of malicious code into our website occurred in January 2014.

Upon discovery of the breach of security, the malicious code was immediately disabled. We conducted a server-wide search of related code and did not identify any additional instances of the malicious code. We have changed the passwords on all system accounts associated with our domain. Based on server access logs, it does not appear that any unauthorized user currently has access to the server. In addition, we are undertaking a thorough review of our data security policies and procedures to protect data from unauthorized use and reduce the likelihood of the recurrence of similar attacks in the future.

Given the nature of the incident, we have notified the three major credit reporting agencies but we have not made a report to law enforcement. However, we suggest that you contact your local law enforcement agency or attorney general and the Federal Trade Commission, in the event of actual or suspected identity theft. We also recommend that you contact the issuer of any credit card you may have used to purchase products through our website and close your account.

0000001

In addition, you should be vigilant about reviewing your credit card and other financial statements for any suspicious or unauthorized activity and monitoring your credit report for any unexplained activity. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, by calling (877) 322-8228, or by completing an Annual Credit Report Request Form (which can be printed at www.annualcreditreport.com/manualRequestForm.action) and mailing it to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348

Alternatively, you may elect to purchase a copy of your credit report from the three national credit reporting agencies listed below.

There are various other resources available to help protect against identify theft, including the placement of a fraud alert or security freeze on your credit file. Please be aware that placing a security freeze on your credit report may delay, interfere with or prevent the timely approval of any requests that you make for new loans, credit, mortgages, employment, housing or other services. The following national credit reporting agencies can assist you with placing a fraud alert or security freeze on your credit report, or you may purchase a copy of your credit report from them.

Equifax
(888) 766-0008 (for fraud alerts)
(800) 685-1111 (for credit reports and security freezes)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
(888) 397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289 (for fraud alerts)
(800) 888-4213 (for credit reports)
(888) 909-8872 (for security freezes)
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

Additional information about how to avoid and deal with identity theft, including fraud alerts and security freezes, is available from:

Federal Trade Commission
(877) ID-THEFT
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft

Your state attorney general and/or your state department of consumer affairs may also have guidance available if there is fraudulent activity on your credit report or if you suspect that your identity has been compromised.

We appreciate your business and sincerely apologize for any inconvenience this may cause. We strongly encourage you to take precautions now to help prevent and detect any misuse of your credit card information. In addition, we have established a dedicated line with representatives that can guide you through any questions you may have regarding the incident itself or the information contained in this letter. This line can be reached toll-free at (877) 238-2074, Monday through Friday, 9:00 a.m. to 7:00 p.m. EST. In order to have a representative assist you, you must have your reference number available. Your reference number is 3263121014.

Very truly yours,

Peter Noble, Manager