McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

April 25, 2019

VIA U.S. MAIL

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: L&M Fleet Supply – Incident Notification

Dear Attorney General Delaney:

McDonald Hopkins PLC represents L&M Fleet Supply ("L&M Supply"). I am writing to provide notification of an incident at L&M Supply that may affect the security of personal information of seventy one (71) New Hampshire residents. L&M Supply's investigation is ongoing and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, L&M Supply does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

L&M Supply recently engaged external forensic investigators to commence a prompt and thorough investigation after suspicious activity within its e-Commerce server was identified. As a result of this review, L&M Supply learned that certain customer credit and debit card information may have been obtained by an unauthorized party from its payment portal when purchased through L&M Supply's online store from December 5, 2018 to January 21, 2019. After an extensive forensic investigation, L&M Supply discovered on April 9, 2019 that residents' personal information may have been acquired in this incident. The information included the affected residents' names and credit or debit card number, card expiration date, and CVV (3 or 4 digit code on the front or back of the card). Purchases made through L&M Supply's store locations were not impacted by the incident.

L&M Supply's investigation is ongoing. Nevertheless, out of an abundance of caution, L&M Supply wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. L&M Supply provided the affected residents with written notification of this incident commencing on or about April 23, 2019 in substantially the same form as the letter attached hereto. L&M Supply is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. L&M Supply is advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit

files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At L&M Supply, protecting the privacy of personal information is a top priority. L&M Supply is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. L&M Supply will continue to evaluate and modify its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Dominic A. Paluzzi

Encl.

L&M Fleet Supply
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

"QUALITY AT A DISCOUNT"

[redacted]

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear [redacted],

We wanted to make you aware of a recent data security incident involving potential unauthorized access to some of our customers' payment card data used at *www.landmsupply.com*. The privacy and security of your personal information is of utmost importance L&M Fleet Supply ("L&M") and we are routinely evaluating and improving our security and payment systems to ensure your information is secure.

What Happened?

After suspicious activity within our e-Commerce server was identified, we immediately engaged external forensic investigators, commenced a prompt and thorough investigation into the incident, and contained the issue. As a result of this review, we learned that certain customer credit and debit card information may have been obtained by an unauthorized party from our payment portal when purchased through our online store from December 5, 2018 and January 21, 2019. Purchases through our store locations were *not* impacted by this incident.

What Information Was Involved?

On April 9, 2019 we discovered that the information that may have been acquired in this incident included your name, credit or debit card number, card expiration date and CVV (3 or 4 digit code on the front or back of the card).

What We Are Doing

Because we value our relationship with you, we wanted to make you aware of the incident. We also wanted to let you know what we are doing to further secure your information, and suggest steps you can take. Since learning of the incident, we have implemented enhanced security safeguards to help protect from similar intrusions. We are conducting ongoing monitoring of our website and payment portal to ensure that they are secure and cleared of any malicious activity. The payment card networks have also been notified so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

What You Can Do

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

As a best practice, you should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you.

For More Information

Your trust is a top priority for L&M, and we deeply regret the inconvenience this may have caused. The privacy and protection of our customers' information is a matter we take seriously.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8 a.m. to 5 p.m. Central Time.

Thank you,

[redacted]

[redacted]

– OTHER IMPORTANT INFORMATION –

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right under the federal Fair Credit Reporting Act (FCRA) to request that the credit reporting agency delete that information from your credit report file.

In addition, under the FCRA, 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 also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. 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. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. 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. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report, at no charge. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware 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. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.