

**LEWIS
BRISBOIS
BISGAARD
& SMITH LLP**
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

STATE OF NH
DEPT OF JUSTICE
2015 SEP 28 PM 12:19

JENNIFER A. COUGHLIN
DIRECT DIAL: 215.977.4081
JENNIFER.COUGHLIN@LEWISBRISBOIS.COM

September 23, 2015

Via First Class US 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 Security Incident

Dear Attorney General Foster:

We represent M&R Strategic Services, Inc. ("M+R"), 1901 L Street NW, Suite 800, Washington, District of Columbia 20036, and are writing to notify you of a data security incident that may affect the security of personal information of one (1) New Hampshire resident. 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, M&R Strategic Services, Inc., does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On August 10, 2015, M+R determined an unknown actor accessed without authorization its finance department email account and sent phishing emails to certain individuals and businesses affiliated with M+R. M+R immediately changed the credentials used to access the email account, enabled two-factor authentication, and communicated with certain recipients of the phishing email to encourage steps be taken to protect against unauthorized access to the recipients' information and systems. M+R consulted with its third-party forensic consultants regarding the security of the finance department email account and its systems. M+R additionally engaged independent, third-party forensic investigators to assist in their investigation into the security of their system and actions taken in the finance department email account by the unknown actor.

While these investigations are ongoing, M+R confirmed that emails stored within the email account at the time of unauthorized access contained the name and Social Security number of certain

individual third party vendors and the business name and tax identification number of certain vendors who are business entities. M+R is unaware of any exfiltration of information contained in the email account.

Notice to New Hampshire Residents

M+R has identified one (1) New Hampshire resident as being impacted by this incident. M+R will mail written notice of this incident to these affected New Hampshire residents on or about September 22, 2015, in substantially the same form as the letter attached hereto as *Exhibit A*. Additionally, M+R has identified one (1) New Hampshire business entity whose business name and tax identification number were stored within the finance department email account at the time of this incident. M+R is providing voluntary notice of this incident to the New Hampshire business on or about September 24, 2015, in substantially the same form as the letter attached hereto as *Exhibit B*.

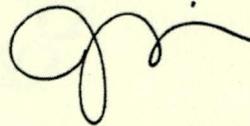
Other Steps Taken and To Be Taken

M+R's investigation into this incident is ongoing. M+R is providing individuals and businesses affected by this incident with helpful information on how to protect against identity theft and fraud. M+R is taking steps to prevent additional unauthorized access to the finance department email account or any other M+R email accounts and systems. M+R continues to monitor its systems for suspicious activity. In addition to providing notice of this incident to you, M+R is providing notice of this incident to other state regulators where required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4081.

Very truly yours,



Jennifer A. Coughlin of
LEWIS BRISBOIS BISGAARD & SMITH LLP

JAC:aw
Enc.

EXHIBIT A



September 22, 2015

[Name]
[Address]
[City, State Zip]

Dear [Name]:

M&R Strategic Services, Inc. ("M+R") is writing to inform you of a recent incident that may affect the security of your personal information. While we are unaware of any actual or attempted misuse of your personal information, we are writing to provide you with information regarding the event, steps we've taken since discovering the event, and what you can do to protect yourself against identity theft and fraud if you feel it is appropriate to do so.

What Happened? On August 10, 2015, M+R determined an unknown actor accessed its Finance Department email account and sent phishing emails to certain individuals and businesses affiliated with M+R. M+R immediately changed the credentials used to access the email account, enabled two-factor authentication, and communicated with certain recipients of the phishing email to encourage steps be taken to protect against unauthorized access to the recipients' information and systems. M+R consulted with its third-party forensic consultants regarding the security of the Finance Department email account and its systems. M+R additionally engaged independent, third-party forensic investigators to assist in their investigation into the security of their system and actions taken in the Finance Department email account by the unknown actor. While these investigations are ongoing, and M+R is unaware of any exfiltration of information contained in the email account, M+R has confirmed your name and Social Security number was contained in an email within the email account at the time unauthorized access to the email account occurred.

What is M+R Doing? M+R takes the security of your personal information seriously. In addition to taking the steps above, M+R is taking steps to prevent additional unauthorized access to the Finance Department email account or any other M+R email accounts and

systems. M+R continues to monitor its systems for suspicious activity. We are providing you with notice of this incident and information on how to better protect against identity theft and fraud, which is included in the attached Privacy Safeguards Information.

What Can You Do? You can review the additional information included in the attached Privacy Safeguards Information on how to better protect against identity theft and fraud. You can contact Todd Addams at M+R with questions or concerns, Monday through Friday, 9 a.m. to 6 p.m. ET, at 202-478-6127.

M+R takes privacy and data security very seriously, and would like to apologize for any inconvenience or concern 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,

A handwritten signature in black ink, appearing to read "Marlee Miller". The signature is fluid and cursive, with the first name "Marlee" being more prominent than the last name "Miller".

Marlee Miller
Chief Operating Officer

PRIVACY SAFEGUARDS INFORMATION

You may also take action directly to further protect against possible identity theft or financial loss. We 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, 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, 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:

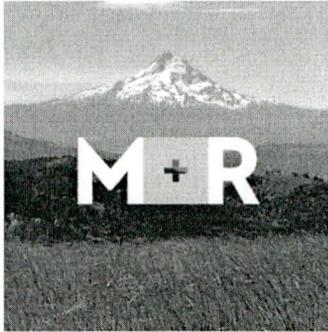
Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call
800-349-9960)
[www.equifax.com/help/cr
edit-freeze/en_cp](http://www.equifax.com/help/cr
edit-freeze/en_cp)

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888-397-3742
[www.experian.com/freeze/center
.html](http://www.experian.com/freeze/center
.html)

TransUnion Fraud
Victim Assistance
P.O. Box 6790
Fullerton, CA 92834
Fraud Division
800-680-7289
[www.transunion.com/fr
eeze](http://www.transunion.com/fr
eeze)

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, 877-ID-THEFT (877-438-4338); TTY: 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 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.

EXHIBIT B



September 22, 2015

[Business Name]
[Address]
[City, State Zip]

Dear [Business Name]:

M&R Strategic Services, Inc. ("M+R") is writing to inform you of a recent incident that may affect the security of your business information. While we are unaware of any actual or attempted misuse of your business information, we are writing to provide you with information regarding the event, steps we've taken since discovering the event, and what you, as the business owner, can do to protect against identity theft and fraud if you feel it is appropriate to do so.

What Happened? On August 10, 2015, M+R determined an unknown actor accessed its Finance Department email account and sent phishing emails to certain individuals and businesses affiliated with M+R. M+R immediately changed the credentials used to access the email account, enabled two-factor authentication, and communicated with certain recipients of the phishing email to encourage steps be taken to protect against unauthorized access to the recipients' information and systems. M+R consulted with its third-party forensic consultants regarding the security of the Finance Department email account and its systems. M+R additionally engaged independent, third-party forensic investigators to assist in their investigation into the security of their system and actions taken in the Finance Department email account by the unknown actor. While these investigations are ongoing, and M+R is unaware of any exfiltration of information contained in the email account, M+R has confirmed your business name and tax identification number was contained in an email within the email account at the time unauthorized access to the email account occurred.

What is M+R Doing? M+R takes the security of your business information seriously. In addition to taking the steps above, M+R is taking steps to prevent additional unauthorized

access to the Finance Department email account or any other M+R email accounts and systems. M+R continues to monitor its systems for suspicious activity. We are providing notice of this incident and information on how to better protect against identity theft and fraud, which is included below.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft by reviewing account statements and monitoring free 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, 877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. Equifax can be contacted at: PO Box 105069, Atlanta, GA 30348, 800-525-6285, www.equifax.com. Experian can be contacted at: PO Box 2002, Allen, TX, 75013, 888-397-3742, www.experian.com. TransUnion can be contacted at: PO Box 2000, Chester, PA 19022-2000, 800-680-7289, www.transunion.com. You can further educate yourself regarding the prevention of identity theft by contacting your state Attorney General's Office and the Federal Trade Commission. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, 877-ID-THEFT (877-438-4338), TTY: 866-653-4261, www.ftc.gov/idtheft. **For Maryland businesses**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

If you have any questions or concerns, please contact Todd Addams at M+R, Monday through Friday, 9 a.m. – 6 p.m. ET, at 202-478-6127.

M+R takes privacy and data security very seriously, and would like to apologize for any inconvenience or concern 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 business information.

Sincerely,



Marlee Miller
Chief Operating Officer