BRIAN MIDDLEBROOK
BMIDDLEBROOK@GRSM.COM

JOHN T. MILLS
JTMILLS@GRSM.COM

GORDON&REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

ATTORNEYS AT LAW
1 BATTERY PARK PLAZA, 28TH FLOOR
NEW YORK, NY 10004
WWW.GRSM.COM

November 21, 2022

VIA CERTIFIED MAIL, RETURN RECEIPT REQUESTED
Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of Data Security Incident
Our File No: 1239238

To Whom It May Concern:

Our client, Receivables Performance Management, LLC ("RPM"), a national leader in accounts receivable management, understands the importance of protecting personal information and is making this notification to your Office in accordance with applicable law following a recent data security incident.

On or about May 12, 2021, RPM became aware of a data security incident that impacted its server infrastructure and took our systems offline. RPM responded immediately by physically disconnecting all equipment and began undertaking necessary efforts to restore its systems. Immediately following the incident and over a 36-hour time frame, RPM rebuilt its shared servers from the ground up and removed and re-installed all collection and dialing software on all equipment. RPM also retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised.

The forensic investigation determined that first access to RPM's systems occurred on approximately April 8, 2021, with the ransomware launched on May 12, 2021. While the findings of the forensic investigation were not conclusive, the data security incident *may have* resulted in unauthorized access to and/or acquisition of certain data on RPM's systems. As a result, in an abundance of caution, RPM began undertaking extensive efforts to gather and review this data to identify the presence of any personal information.

RPM began this process by identifying and collecting all data that may have been accessed or acquired in connection with the data security incident. Given the complexities of RPM's server infrastructure, these efforts were extensive. RPM thereafter undertook a comprehensive, time intensive data review process, including manual review, of these documents to identify the presence of any personal information. This process concluded on or around October 2, 2022. Through this review process, RPM identified the presence of personal information in the files that were reviewed. **Please note that it is entirely possible that any specific personal information**

was not impacted as a result of the incident. RPM also obtained confirmation to the best of its ability that the information is no longer in possession of the third party(ies) associated with this incident.

Nonetheless, RPM is providing notification of the incident via U.S. mail and electronic mail in accordance with applicable law beginning on November 18, 2022, including 6,625 New Hampshire residents. A sample copy of the notification letter is attached. As noted in the attachment, RPM has included in the notification an offer to provide complimentary credit monitoring and identity theft protection services to the potentially impacted individuals. Additionally, RPM has established a toll-free call center to answer any questions that the potentially impacted individuals may have regarding the incident, as well as to assist the potentially impacted individuals in enrolling in the credit monitoring and identity theft protection services. RPM is also providing notification of this incident to the three major credit reporting agencies.

As stated above, RPM responded immediately to the data security incident by physically disconnecting all equipment and began undertaking necessary efforts to restore its systems. Immediately following the incident and over a 36-hour time frame, RPM rebuilt its shared servers from the ground up and removed and re-installed all collection and dialing software on all equipment. RPM also retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised. At all relevant times, RPM maintained and continues to maintain comprehensive policies and procedures to protect the information maintained on its servers and systems, including a written information security management policy. Please be advised that RPM is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

Should you have any questions or require additional information, please do not hesitate to contact me.

Best regards,

GORDON REES SCULLY MANSUKHANI, LLP

Brian Middlebrook, Esq.
John T. Mills, Esq.

Enclosures

RECEIVABLES PERFORMANCE MANAGEMENT
Return Mail Processing Center
P.O. 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>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Receivables Performance Management ("RPM") understands the importance of protecting your information and is writing to inform you that it recently identified and addressed a security incident that may have involved your personal information. This notice describes the incident, outlines the measures that RPM has taken in response, and advises you on steps you can take to further protect your information.

What Happened? On or about May 12, 2021, RPM became aware of a data security incident that impacted its server infrastructure and took our systems offline. RPM responded immediately by physically disconnecting all equipment and began undertaking necessary efforts to restore its systems. Immediately following the incident and over a 36-hour time frame, RPM rebuilt its shared servers from the ground up and removed and re-installed all collection and dialing software on all equipment. RPM also retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised.

What Information Was Involved? The forensic investigation determined that first access to RPM's systems occurred on approximately April 8, 2021, with the ransomware launched on May 12, 2021. While the findings of the forensic investigation were not conclusive, the data security incident *may have* resulted in unauthorized access to and/or acquisition of certain data on RPM's systems. As a result, in an abundance of caution, RPM began undertaking extensive efforts to gather and review this data to identify the presence of any personal information.

RPM began this process by identifying and collecting all data that may have been accessed or acquired in connection with the data security incident. Given the complexities of RPM's server infrastructure, these efforts were extensive. RPM thereafter undertook a comprehensive, time intensive data review process, including manual review, of these documents to identify the presence of any personal information. This process concluded on or around October 2, 2022. Through this review process, RPM identified the presence of your personal information in the files that were reviewed, including Social Security number. **Please note that it is entirely possible that your specific personal information was not impacted as a result of the incident.** RPM also obtained confirmation to the best of its ability that the information is no longer in the possession of the third party(ies) associated with this incident.

What We Are Doing. As stated above, RPM responded immediately to the data security incident by physically disconnecting all equipment and began undertaking necessary efforts to restore its systems. Immediately following the incident and over a 36-hour time frame, RPM rebuilt its shared servers from the ground up and removed and re-installed all collection and dialing software on all equipment. RPM also retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised. Please be advised that RPM is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

FREE CREDIT MONITORING/INSURANCE: Additionally, we are offering you a free <<CMLength>>-month membership to TransUnion *my*TrueIdentity credit monitoring service. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. **This product also includes various features such as up to $1,000,000 in identity theft insurance with no deductible, subject to policy limitations and exclusions. TransUnion *my*TrueIdentity is completely free to you** and enrolling in this program will not hurt your credit score. For more information on identity theft protection and TransUnion *my*TrueIdentity, including instructions on how to activate your complimentary <CM Length>>-month membership, please see the additional information attached to this letter. ***TO TAKE ADVANTAGE OF THE FREE CREDIT MONITORING OFFER, YOU MUST ENROLL BY <<ENROLLMENT DEADLINE>>.***

What You Can Do. We are aware of how important personal information is to you. We encourage you to protect yourself from potential harm associated with this incident by **enrolling in the credit monitoring service**, closely monitoring all mail, email, or other contact from individuals not known to you personally, and to avoid answering questions or providing additional information to such unknown individuals. We also remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements, explanation of benefits statements, and credit reports for unauthorized activity, and to report any such activity or any suspicious contact whatsoever to law enforcement if warranted.

For More Information. For further information on steps you can take to prevent against possible fraud or identity theft, please see the attachments to this letter. RPM understands the importance of protecting your personal information, and deeply regrets any concern this may have caused to you. **Should you have any questions and would like further information regarding the information contained in this letter, please do not hesitate to contact 877-237-5382 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.**

Sincerely,

Howard George
Chief Executive Officer
Receivables Performance Management