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 ELECTRONIC MAIL (CONSUMER@AG.IOWA.GOV)
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319

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 22,880 Iowa 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

/s/ Brian Middlebrook

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

Attachment 1: Protecting Yourself

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<Activation code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code <<Engagement Number>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and ***<<ENROLLMENT DEADLINE>>.*** Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. **Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies.** To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert.

- **Initial Alert:** You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least 90 days

- **Extended Alert:** You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a **credit freeze**, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 74021	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft: Federal Trade Commission; Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon and West Virginia: It is required by state law to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report using the contact information listed above.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023; www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400; www.riag.ri.gov

Office of the Illinois Attorney General
Identity Theft Hotline
100 W Randolph St, Fl. 12
Chicago, IL 60601
1-866-999-5630; www.illinoisattorneygeneral.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226; www.ncdoj.com

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Connecticut, Massachusetts, Rhode Island and West Virginia: You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above.

*FAIR CREDIT REPORTING ACT***.** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Note - Identity theft victims and active duty military personnel have additional rights.