THOMPSON HINE

ATLANTA | CHICAGO | CINCINNATI | CLEVELAND
COLUMBUS | DAYTON | LOS ANGELES | MINNEAPOLIS
NEW YORK | SILICON VALLEY | WASHINGTON, D.C.

October 22, 2026

VIA EMAIL TO consumer@ag.iowa.gov
Iowa Office of the Attorney General
Attn: Security Breach Notification
Hoover State Office Building, 1305 E. Walnut St.
Des Moines, IA 50319

RE: Supplemental Data Incident Notification

To Whom It May Concern:

We serve as counsel to Motility Software Solutions ("Motility"), a service provider that provides dealer management software to recreational vehicle and power sports dealers, located at 851 Trafalgar Ct #160w, Maitland, FL 32751. This is a supplemental notice to the original notice we filed dated September 29, 2025 regarding additional facts we learned since submission.

We previously notified this office that on or around August 19, 2025, Motility detected unusual activity within certain computer servers that support their business operations ("August 2025 Incident"). Upon discovery, Motility immediately investigated, and it was determined that an unauthorized actor deployed malware that encrypted a portion of their systems. Although the malware primarily restricted their access to corporate data, the forensic evidence suggests that before encryption the unauthorized actor may have removed limited files containing the personal data of their dealers' customers.

On September 2, 2026, during a routine file maintenance process, Motility discovered additional files that the unauthorized actor may have accessed during the August 2025 Incident that were not identified in the original investigation. On September 17, 2026, Motility identified the individuals whose information was contained in these files. Motility provided notice to the affected dealers on October 8, 2026. Motility has found no evidence of any new or continuing unauthorized access to our systems

On October 19, 2026, Motility, on behalf of those dealers, will begin providing written notification to the affected individuals whose sensitive personal data may have been impacted by this discovery, which included **approximately one (1) Iowa resident**. The aforementioned notifications were in substantially the same form as the one attached here (See Enclosure). Motility has offered each impacted Iowa resident **complimentary, twelve-month credit monitoring services** and has further established a dedicated call support line to answer any questions that impacted individuals may have about this incident.

Please do not hesitate to contact me if you have any questions regarding this matter. Motility does not waive any rights or defenses regarding the applicability of Iowa law, and this notification shall not be interpreted as an admission of wrongdoing or fault.

Sincerely,

Thomas F. Zych, Partner
Thompson Hine LLP
127 Public Square # 3900, Cleveland, OH 44114
Tom.Zych@thompsonhine.com | 216.566.5605

Enclosure: Data Incident Notice (Example)

<<Date>> (Format: Month Day, Year)

<<FIRST_NAME>> <<MIDDLE _NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS _1>>
<<ADDRESS _2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

Re: Important Notice of Data Security

Dear <<first_name>> <<last_name>>,

Motility Software Solutions ("**Motility**" or "**we**") understands the importance of protecting your personal data. Regrettably, the purpose of this letter is to inform you of a data security incident that may have involved your personal information. This notice is to provide you with details on what happened, what information was involved, what we are doing in response, and the steps you can take to protect yourself. Motility is providing **you with complimentary credit monitoring and identity theft protection services**, and we encourage you to enroll in these services.

What Happened?

In August 2025, Motility detected unusual activity within certain computer servers that support our business operations ("August 2025 Incident"). Upon discovery, Motility immediately investigated, and it was determined that an unauthorized actor deployed malware that encrypted a portion of our systems. Although the malware primarily restricted our access to corporate data, the forensic evidence suggests that before encryption the unauthorized actor may have removed limited files containing personal information.

On or about September 2, 2026, we discovered additional files that were not identified in our original investigation and that the unauthorized actor may have accessed during the August 2025 Incident. After this discovery, we conducted further analysis and determined that these files may have contained your personal information. Accordingly, we are notifying you that this information may have been affected by the August 2025 Incident.

We have found no evidence of any new or ongoing unauthorized access to Motility's systems. This notice relates solely to the August 2025 Incident and the newly identified files described above.

What Information Was Involved?

The files affected vary by individual but may have contained one or more of the following data elements: full name, postal address, e-mail address, telephone number, date of birth, social security number, driver's license number, and credit or debit card number, expiration date, and security code. At this time, we have no evidence of actual misuse of the information; nevertheless, we are issuing this notice so that you can take appropriate steps to safeguard your information.

What Are We Doing?

In response to the August 2025 Incident, we: 1) conducted a forensic investigation to determine the scope of the incident; 2) implemented additional security tools and measures to prevent recurrence; 3) restored system functionality from clean back-ups 4) established dark net monitoring; and 5) engaged counsel and other data

security providers to assist with our response. We have also arranged, at our own expense, for you to receive credit monitoring and identity theft protection services described below.

Identity Monitoring Services

To help alleviate any concerns that you may have with respect to this or other cybersecurity incidents, we are offering identity monitoring services now to all that may have been affected by this incident. **We have secured the services of LifeLock to provide identity monitoring for twelve (12) months**. LifeLock is a global leader in risk mitigation and response. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to **Norton.com/offers**
2. Below the THREE protection plan boxes, you may enter the **Promo Code: MSSXXXX** and click the **"APPLY"** button.
3. Your complimentary offer is presented. Click the Yellow **"START MEMBERSHIP"** button.
4. A Popup will appear to enter your Member ID **<<MEMBER ID>> and click "APPLY"**
5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL directions in this email*).

Alternatively, to activate your membership over the phone, please call: 800-899-0180

You will have until January 15th, 2027, to enroll in this service.

What You Can Do

Although there is no evidence that your personal information has been misused, there are several steps that you can take to better protect yourself and your personal information more generally. If you identify any unauthorized or suspicious payment-card activity, promptly contact the financial institution that issued the card. You may also wish to ask the financial institution whether it recommends closing the affected account, replacing the card, or taking other protective measures. We recommend you remain vigilant and regularly review your credit card bills, bank statements, and credit reports for any unauthorized activity. Promptly report incidents of suspected identity theft or fraud to your local law enforcement agency, the Federal Trade Commission, your state Attorney General, your financial institution, and to one of the three nationwide consumer reporting agencies to have such incidents removed from your credit file. You should change your passwords regularly, and refrain from using easily guessed passwords and re-using the same passwords for multiple accounts. Be vigilant against third parties attempting to gather information by deception, and exercise extreme caution when clicking on unknown or suspicious website links. See the attachment for additional information with respect to certain security services that may be available to you.

* * * * * * * * * *

We regret that this incident occurred and apologize for any inconvenience it may cause. Protecting your information remains our highest priority, and we are committed to maintaining the trust you and our clients place in us. If you have any questions, please contact us at 866-718-6490.

Sincerely,

Motility Software Solutions, Inc.

Additional Information: Data Security Information

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com, call toll free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111.
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742.
- TransUnion, PO Box 2000, Chester, PA 19016, https://www.transunion.com, 1-800-916-8800.

When you receive your credit report: (i) review it carefully, (ii) look for accounts you did not open, (iii) look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security Number). You should also look in the "inquiries" section for names of creditors from whom you have not requested credit. You should notify the consumer reporting agencies immediately of any inaccuracies in your report or if you see anything you do not understand. The consumer reporting agency and staff will review your report with you. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), http://www.ftc.gov/idtheft.

If you are a resident of Iowa, Maryland, Massachusetts, New York, North Carolina, Oregon, or Rhode Island, you may contact and obtain information to avoid identity theft from your state Attorney General at the following:

- Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, 1-515-281-5164, https://www.iowaattorneygeneral.gov/.
- Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 or 1-410-576-6300, www.marylandattorneygeneral.gov.
- New York Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.
- North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6400 or 1-877-566-7226, https://ncdoj.gov/.
- Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-503-378-4400, https://www.doj.state.or.us/.
- Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, https://riag.ri.gov/.

Massachusetts. If you are a resident of Massachusetts, you: have the right to file and obtain a copy of a police report; are allowed to place, without charge, a security freeze on your credit reports; and, may contact and obtain information from and/or report identity theft to your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contactus.html.

Rhode Island. If you are a resident of Rhode Island, please note that approximately 1,407 Rhode Island residents are receiving this notice. Pursuant to Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze on your report as described below and note that fees may be required to be paid to the consumer reporting agencies.

Fraud Alerts: 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. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. 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.

Credit Freezes: 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 personal identification number ("PIN") 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 get access to 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. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses listed above.

To request a security freeze, you will need to provide the following information: (i) Your full name (including middle initial as well as Jr., Sr., II, III, etc.), (ii) Social Security number, (iii) Date of birth, (iv) If you have moved in the past five years, provide the addresses where you have lived over the prior five years, (v) Proof of current address such as a current utility bill or telephone bill, (vi) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.), (vii) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act ("FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The Federal Trade Commission has published a list of the primary rights created by the FCRA, available at (www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The Federal Trade Commission's list of FCRA rights includes the following:

You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request. Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12

months. You are also entitled to a free report if a company takes adverse action against you, like 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 are 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. You have the right to ask for a credit score. You have the right to dispute incomplete or inaccurate information. Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Consumer reporting agencies may not report outdated negative information. Access to your file is limited. You must give your consent for reports to be provided to employers. You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report. You may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

Note: The delivery of this notice has not been delayed as a result of a law enforcement investigation.