1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

June 4, 2024

Via Online Reporting
Maine Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Medjet and MedjetAssist - Notice of Data Event

To Whom It May Concern:

We represent Medjet and MedjetAssist ("Medjet"), the premier global air medical transport and travel security membership program that is based in Birmingham, Alabama. This letter is being provided pursuant to the Maine Notice of Risk to Personal Data Act, 10 ME. REV. STAT. ANN. § 1346, *et seq* (2019), which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of Maine.

On October 17, 2023, Medjet's computer network was disrupted by computer malware rendering certain systems temporarily offline. Medjet restored its systems to normal business operations without significant impact on its services and commenced an investigation into the nature and scope of the event. On or about December 5, 2023, Medjet learned that certain data from its network could have been taken during the period of unauthorized access. As a result, Medjet commenced a thorough review of its server data for the presence of sensitive information. On or about May 10, 2024, Medjet completed that review and confirmed sensitive information was present within its files at time of the incident. Medjet has no knowledge of any actual or attempted misuse of any client information during this time. The information potentially accessible includes client name, address, and Social Security number.

Medjet began providing written notice of the incident to impacted individuals on January 5, 2024, to which no Maine residents were identified in the preliminary review. Upon completion of the server data review, Medjet is notifying Maine residents by U.S. regular mail on June 3, 2024. A sample copy of the notice letter is attached for your records as "***Exhibit A***". Medjet provided this notification to 9 residents of Maine. The investigation is now complete, no additional waves of notification will be needed.

Medjet's notification includes a brief description of the incident, encouragement for remaining vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements and credit reports, reporting any suspicious activity to the financial institution or the appropriate service provider, and to filing a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. Medjet also enclosed documentation containing contact information for the major consumer reporting bureaus, state-specific regulators, a dedicated call center, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so. As an added precaution, Medjet is offering all affected Maine residents 12 months of identity theft monitoring and restoration services through Kroll at no cost. The notice to the affected individuals includes instructions on the use of this product.

Following the incident, Medjet revised its network architecture. Medjet also partnered with computer forensics professionals to thoroughly investigate the incident and provide notice to its clients out of an abundance of caution. Medjet continues to utilize complex password requirements and multi-factor authentication. Medjet will continue to review its network for opportunities to strengthen the existing security measures in place and help prevent a future incident from occurring. Finally, Medjet also notified other state regulators as required.

I believe this provides you with all information necessary for your purposes and to comply with Maine law. However, if anything further is needed, please contact me.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

FMG LAW Freeman Mathis & Gary LLP

Exhibit "A"

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (Re: Notice of Data [Event/Breach])>>

Dear <<first_name>> <<last_name>>:

Medjet and MedjetAssist takes the privacy and security of our customers' information seriously. As part of that commitment, we are notifying you of an event that impacted our computer network. Please read this letter carefully.

What Happened?

On October 17, 2023, Medjet's computer network was disrupted by computer malware rendering certain systems temporarily offline. We restored our systems to normal business operations without significant impact on our services and commenced an investigation into the nature and scope of the event. On or about December 5, 2023, we learned that certain data from our network could have been taken during the period of unauthorized access. As a result, we commenced a thorough review of our server data for the presence of sensitive information. On or about May 10, 2024, we completed that review and confirmed your information was present within our files at time of the incident. We stress that we have received no indication of any actual or attempted misuse of any client information during this time. Nonetheless, we believe it is important to notify our clients about this event and provide you with the enclosed resources.

What Information Was Involved?

Your <<b2b_text_2 (data elements)>> were present in files on our network during the period of unauthorized access. We reiterate that our investigation has not definitively confirmed files containing your information were taken from the network, and we have no knowledge of any actual or attempted misuse of your information at this time.

What We Are Doing.

We take this event and the security of personal information entrusted to us very seriously and have taken steps to help mitigate the potential for harm and prevent this from happening again. Following the incident, we revised our network architecture. We also partnered with computer forensics professionals to thoroughly investigate the incident and provide notice to our clients out of an abundance of caution. We continue to utilize complex password requirements and multi-factor authentication. We will continue to review our network for opportunities to strengthen our existing security measures in place and help prevent a future incident from occurring.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for twelve (12) months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Instructions for how to enroll in the offered services are below.

What You Can Do.

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or issuing bank immediately. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, should you find it appropriate to do so.

Our offer of identity monitoring services includes Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. To enroll at no cost:

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Kroll Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is also contained within the enclosed "Additional Steps to Help Protect Your Information".

For More Information.

Medjet regrets any concern or inconvenience this event has caused or may cause you. We remain committed to protecting the information entrusted in our care. If you have any other questions about this event, you may call (866) 992-0669, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your unique Kroll Membership Number listed above ready when you call.

Sincerely,

John F. Gobbels
Vice President & Chief Operating Officer
Medjet & MedjetAssist

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Initial fraud alerts will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for up to seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online using the above contact information. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online using the above contact information. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain Additional Information about the steps you can take to avoid identity theft from the following entities:

- **District of Columbia Residents:** District of Columbia Attorney General may be contacted at 400 6th Street, NW, Washington, D.C. 20001; https://oag.dc.gov; and (202) 727-3400;
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division may be contacted at 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.marylandattorneygeneral.gov, and toll-free at (888) 743-0023 or (410) 528-8662;
- **New Mexico Residents:** You have certain rights under the FCRA, which you can read about by visiting https://consumer.ftc.gov/articles/0070-credit-your-consumer-rights and https://consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0070-credit-and-your-consumer-rights_1.pdf. For more information review www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; or contact Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580;
- **New York Residents:** New York Attorney General may be contacted at Office of Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov, and (800) 771-7755;
- **North Carolina Residents:** Office of the Attorney General of North Carolina may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, https://ncdoj.gov, (919) 716-6400;
- **Rhode Island Residents:** Office of the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and (401) 274-4400. Under Rhode Island law, you have the right to obtain a police report. [#] Rhode Island residents were impacted by this incident;
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). This notification was not delayed by law enforcement.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.