



Blair L. Dawson
550 West Adams Street, Suite 300
Chicago, Illinois 60661
Blair.Dawson@lewisbrisbois.com
Direct: 312.463.3332

January 28, 2022

File No. 49905.53

VIA E-MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Medtipster in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute.

1. Nature of the Security Incident

Medtipster is a pharmacy benefit consultant and eligibility manager. Medtipster is based in Southfield, Michigan.

On August 25, 2021, Medtipster became aware of a possible data security incident event involving its network. Upon discovery, Medtipster took immediate steps to secure its systems. Additionally, Medtipster engaged independent computer forensic investigators to conduct an investigation to help determine what happened. The investigation found that an unauthorized person gained access to and may have acquired information stored in Medtipster's email environment. Medtipster immediately began investigating what information may have been involved in the incident.

On January 20, 2022, the investigation determined that the email environment contain protected health information belonging to certain individuals. Medtipster then worked diligently to determine the individuals who were impacted and their address information in order to provide notification of this incident.

2. Type of Information and Number of Maryland Residents Involved

The incident involved personal information for approximately **455** Maryland residents. The information involved in the incident may differ depending on the individual but may include name and medical information, such as prescription drug names and cost of drugs.

The affected individuals will receive a letter notifying them of the incident and providing additional steps they can take to protect their personal information. The notification letters will be sent via USPS First Class Mail on January 27, 2021. A sample copy of the notification letter sent to the affected individuals is attached.

3. Measures Taken to Address the Incident

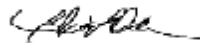
In response to the incident, Medtipster retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Medtipster also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

Finally, Medtipster is notifying the affected individuals and providing them with steps they can take to protect their personal information.

4. Contact Information

Medtipster is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Blair Dawson at 312-463-3332 or Blair.Dawson@lewisbrisbois.com.

Sincerely,



Blair L. Dawson of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

BLD:vh
Encl.: Sample Consumer Notification Letter



P.O Box 989728

West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

January 27, 2022

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident experienced by Medtipster that may have involved your personal information. At Medtipster, we take the privacy and security of the individuals we serve very seriously. This is why we are notifying you of the incident and informing you about steps you can take to help protect your personal information.

What Happened? On August 25, 2021, Medtipster became aware of a possible data security incident event involving its network. We conducted an investigation and hired independent computer forensic investigators to help determine what happened. Medtipster's investigation found that an unauthorized person gained access to and may have acquired information stored in its email environment. Medtipster immediately secured its environment and began investigating what information may have been involved in the incident.

On January 20, 2022, the investigation determined that protected health information belonging to individuals may have been accessed by the unauthorized actor. We have determined that your information may have been involved in the incident.

What Information Was Involved? The information potentially impacted is any information you provided to Medtipster and may include your name, address and personal health information related to your interaction with Medtipster.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. In addition, Medtipster is providing you with information about steps you can take to help protect your personal information, described below.

What You Can Do: You can follow the recommendations included with this letter to protect your personal information.

For More Information: If you have any questions about this letter, please call (833) 381-2294 Monday through Friday from 9 am - 9 pm Eastern Time. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Medtipster.com, LLC

Intentionally Left Blank

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. 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 also should 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 (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Experian P.O. Box 9701 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 740241 Atlanta, GA 30348 1-866-349-5191 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
---	---	--	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC at **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, D.C. 20580, or online at consumer.ftc.gov and www.ftc.gov/idtheft, or to the Attorney General in your state. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-410-528-8662	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 1-401-274-4400
--	---	---	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Review your Tax Filings: If you detect any suspicious activity relating to your tax filings, we encourage you to complete IRS Form 14039, Identity Theft Affidavit, which you can obtain at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. If you have other identity theft / tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. You should be especially aware of any requests, calls, emails, letters, or other questions about your financial accounts or from individuals purporting to be from the IRS or other entities from whom you would not be expecting contact. If you receive any type of unexpected request for personal information, you should not provide that information and instead contact the organization by phone to verify the request is legitimate.