Morgan Lewis

Gregory T. Parks
Partner
215.963.5170
gregory.parks@morganlewis.com

May 17, 2024

VIA EMAIL TO CONSUMER@AG.IOWA.GOV

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents The Lash Group, LLC ("Lash Group"), and we are writing to notify your office on behalf of Lash Group and its customer, Bristol Myers Squibb and/or the Bristol Myers Squibb Patient Assistance Foundation ("BMS / BMS PAF") about the nature and circumstances of a recent data security incident at Lash Group.

On April 10, 2024, Lash Group identified individuals whose personally identifiable information had been exfiltrated from certain databases in Lash Group's information systems. Lash Group maintained this information through the programs it managed or manages on behalf of BMS / BMS PAF. Lash Group notified BMS / BMS PAF on April 18, 2024 that its files may have been impacted.

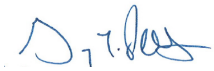
Through its investigation, Lash Group has determined that the information involved may have included first name, last name, address, date of birth, health diagnosis, and/or medications/prescriptions. Although there is no current indication that the personal information has been used for any fraudulent purpose, notifications are being sent by mail to the affected individuals to explain what happened, what information was involved, what has been done, and how affected individuals can contact Lash Group and obtain more information. Two years of credit monitoring are being offered to affected individuals.

Since learning of this incident, Lash Group has engaged third-party cyber experts to conduct an investigation to better understand what happened and to prevent a similar incident in the future. Lash Group has also taken steps to strengthen the security of its systems, and it will continue with these efforts.

Further information about what mitigations have been completed to date and what further mitigations are recommended to the individuals in question can be found in the enclosed notification that Lash Group and BMS / BMS PAF are sending to 31,009 Iowa residents via mail on May 17, 2024.

If you have any questions, please feel free to contact me.

Regards,



Gregory T. Parks

Enclosure

cencora

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 17, 2024

L3295-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 BMS ADULT NON-CA
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: Notice of Data Security Incident

Dear Sample A. Sample:

Cencora, Inc. and its Lash Group affiliate, partner with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support services, business analytics and technology, and other services. We take very seriously the protection of the information entrusted to us in providing these services.

We are writing to let you know about an event that involved your personal information that Lash Group has through the patient support and access programs it manages on behalf of Bristol Myers Squibb and/or the Bristol Myers Squibb Patient Assistance Foundation. It is important to note that we have no evidence at this time that your information has been disclosed for any purpose other than intended to support administration of the program(s) to which you are/were enrolled, however, as a result of this incident, we are taking precautionary measures and sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to address this situation. Please read this letter carefully, because it provides details about what happened and what we are doing about it.

What Happened?

On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, Cencora immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and outside lawyers. On April 10, 2024, we confirmed that some of your personal information was affected by the incident.

What Information Was Involved?

Based on our investigation, personal information was affected, including potentially your first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions. There is no evidence that any of this information has been or will be publicly disclosed, or that any information was or will be misused for fraudulent purposes as a result of this incident, but we are communicating this to you so that you can take the steps outlined below to protect yourself.

What We Are Doing

Immediately upon learning of this incident, we launched an investigation with the assistance of cybersecurity experts, law enforcement, and outside lawyers. Determining whether personal information or personal health information was compromised in any way has been one of the top priorities of this effort so that we could notify potentially affected individuals. Please be assured that we are also working with cybersecurity experts to reinforce our systems and information security protocols in an effort to avoid incidents like this from occurring in the future.

We are also making resources available to those individuals whose information was involved. While we have no reason to believe that your information was used for any fraudulent purpose as a result of this incident, to help protect your identity, we are providing you with access to Experian IdentityWorks[SM] credit monitoring and remediation services for 24 months at no charge to you. These services provide you with alerts for two years from the date of enrollment when changes occur to your credit file. These services also provide you with proactive fraud assistance to help with any questions that you might have and identity restoration assistance in the event that you become a victim of fraud.

How do I enroll for the free services?

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection and credit monitoring tools available through Experian IdentityWorks. To enroll in these services at no charge, visit www.experianidworks.com/plus and follow the instructions provided. When prompted please provide the following unique code to receive services: ABCDEFGHI. In order for you to receive the monitoring services described above, you must enroll by August 30, 2024. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Should you have any questions regarding the Credit Monitoring services, have difficulty enrolling, or require additional support, please contact Experian at 1-833-918-1728. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do

To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and restoration assistance if you were not the one who initiated it.
- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

For More Information

If you have questions or concerns or learn of any suspicious activity that you believe may be related to this incident, please call 1-833-918-1728. Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,

Matt Wolf

Matthew Wolf
President, Biopharma Services
Lash Group

REFERENCE GUIDE

If you suspect that you are a victim of identity theft or credit fraud, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the FTC's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible if there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer credit reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov

Place a Fraud Alert on Your Credit File: A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below.

Equifax	**Experian**	**TransUnion**
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241 Atlanta, Georgia 30374-0241	P.O. Box 9532 Allen, Texas 75013	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus using the same contact information noted above.

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security number; (3) Date of birth; (4) If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years; (5) Proof of current address, such as a current utility bill or telephone bill; (6) A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and (7) If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft.

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov

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

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services.