cencora

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

June 7, 2024

L4222-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 PFI - LASH ADULTS
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 and services, business analytics and technology, and other services. We take the privacy and protection of the information entrusted to us in providing these services very seriously.

Cencora is writing to let you know about an event that involved your personal information that Lash Group has in order to support Pfizer Inc.'s patient support programs. It is important to note that we have no evidence at this time that your information has been used for any fraudulent purpose as a result of this incident, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do in response to 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, Cencora confirmed that 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, Cencora launched an investigation with the assistance of cybersecurity experts, law enforcement, and outside lawyers. This investigation included determining whether personal information or personal health information was compromised. Cencora is also working with cybersecurity experts to enhance our systems and information security protocols in an effort to prevent incidents like this from occurring in the future.

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.consumerfinance.gov 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

0000001

[redacted]

L4222-L01