

From: [Layman, James](#)
To: hliivamagi@ahdootwolfson.com
Cc: [Mishaan, Jessica](#); [Ferrari, Gabriela](#)
Subject: Public Records Request Response re Cencora
Date: Thursday, December 19, 2024 10:47:40 PM
Attachments: [2024-12-19 Cencora Breach PRA Response.pdf](#)
[CencoraPRRdocuments.zip](#)

Dear Ms. Liivamagi,

Please find attached a written response to your public records request, along with a zip file containing all responsive documents. Please let me know if you have any questions.

Best,

James

James Layman
Assistant Attorney General
Vermont Office of the Attorney General
Environmental and Public Protection Division
109 State Street
Montpelier, VT 05609-1001
802.828.2315
james.layman@vermont.gov



STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER, VT
05609-1001

December 19, 2024

Via email to: hliivamagi@ahdootwolfson.com

Re: Public Records Request

Dear Ms. Liivamagi and Mr. Ahdoot:

I write in response to your Public Records Act request received by the Attorney General's Office on December 16, 2024 in which you requested: "all documents relating to any investigation, review, or correspondence regarding the data breach that was disclosed by Cencora, Inc. ('Cencora') to the Securities Exchange Commission in a public filing on or about February 27, 2024, and to some affected consumers on or about May 17, 2024 (the 'Data Breach') (see Exh. A)."

In response to your request, we have identified 71 documents in our records related to the Cencora data breach. These documents consist of security breach reports filed with our office by various entities related to this breach, and samples of notice letters submitted by those entities. I have attached to this email a zip file containing the responsive documents.

Sincerely,

James Layman

James Layman
Assistant Attorney General
Environmental and Public Protection Division



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

May 15, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 16, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.



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.

0000001



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 IdentityWorksSM 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,



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 your 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 20001, 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.

May 20, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 20, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 20, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.



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

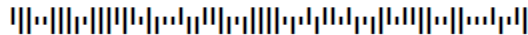
May 21, 2024

L3565-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01



APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY



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 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 obtained through its partnership with one such organization in connection with its 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 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, your 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 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 prevent incidents like this from occurring in the future.

We are also making resources available to those individuals whose information was involved. To help protect your identity, we are providing you with access to Experian IdentityWorksSM 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 to you, 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. 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,



Matthew Wolf
President, Biopharma Services
Lash Group

REFERENCE GUIDE

We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports, 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 may 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 your 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 20001, 202-727-3400, www.oag.dc.gov

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 Oregon Residents: You can report 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.

May 21, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 21, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 22, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.



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

May 22, 2024

L3623-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 NOV LASH
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 prescribed therapies through drug distribution, free trial offers, co-pay coupons, patient support and services, and other services. We take the privacy and protection of the information entrusted to us very seriously.

Cencora is writing to let you know about an event that involved your personal information that Cencora maintains in connection with its patient support programs on behalf of Novartis Pharmaceuticals Corporation. It is important to note that at this time, we have no evidence that your information has been used for any fraudulent purpose as a result of this incident. We are sending this letter to explain what happened, how your information was potentially impacted, 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 and cybersecurity experts. On April 10, 2024, Cencora confirmed that your personal information was impacted.

What Information Was Involved?

Based on Cencora’s investigation, personal information including your personal health 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 at this time that any of this information has been publicly disclosed, or that any information was misused for fraudulent purposes as a result of this incident. Out of transparency, Cencora is 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 and law enforcement. This investigation included determining whether personal information or personal health information was compromised. Cencora is also working with cybersecurity experts to review and enhance our systems and information security protocols in an effort to prevent incidents like this from occurring in the future.

0000001



Cencora is also making resources available to you. While we have no reason at this time 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 free credit monitoring and remediation services through Experian. 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 or in the event that you become a victim of fraud.

How do I Enroll in the Free Credit Monitoring 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 the free credit monitoring services, 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 free credit monitoring services, you must enroll by August 30, 2024. Please note that when signing up for monitoring services, you may be asked to verify personal information to confirm your identity.

Should you have any questions regarding the credit monitoring services, 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, Cencora strongly recommends you take the following steps:

- Enroll in the free credit monitoring services that we are offering to you. This will enable you to get alerts about any attempts to use your name and personal information 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. Cencora encourages 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 Cencora takes this matter very seriously and apologizes for the concern and inconvenience this may cause you.

Sincerely,



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 U.S. Federal Trade Commission'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: To protect yourself from possible identity theft, consider placing 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. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

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 the following information:

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.)
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 your identity has been stolen, the FTC recommends that you take these additional steps.

0000001



- 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 20001, 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.

May 22, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 23, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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 B123106 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,



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 your 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.

0000001



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 20001, 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.



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

May 23, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.



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

May 23, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with Sumitomo Pharma America, Inc. f/k/a Sunovion Pharmaceuticals Inc. in connection with its 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 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 prevent incidents like this from occurring in the future.



0000001



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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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



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.

May 24, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 24, 2024



Re: Notice of Data Security Incident

Dear 

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 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 processed through its work assisting the GlaxoSmithKline Group of Companies and/or the GlaxoSmithKline Patient Access Programs Foundation. 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 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 prevent incidents like this from occurring in the future.

0000001



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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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



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.

May 28, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 28, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 28, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.



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

May 29, 2024



Re: Notice of Data Security Incident

Dear [Redacted]

Cencora, Inc. and its Lash Group affiliate partner with pharmaceutical companies, pharmacies, healthcare providers, and other companies to facilitate access to therapies through drug distribution, patient support and 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 its relationship with one such organization in connection with its customer 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 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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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

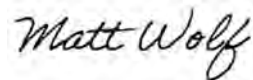
To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- 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,



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 your 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



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 20001, 202-727-3400, www.oag.dc.gov

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 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.

May 30, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.



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

May 30, 2024

L3895-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 SANOFI 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 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 its partnership with one such organization in connection with its 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 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 prevent incidents like this from occurring in the future.

0000001



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 IdentityWorksSM credit monitoring and remediation services for 5 years at no charge to you. These services provide you with alerts for 5 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

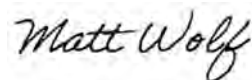
To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- 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,



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 your 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



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 20001, 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.

May 31, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 31, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 31, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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.

May 31, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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

0000001



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 prevent 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 IdentityWorksSM 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: [REDACTED]. 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,



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 your 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.

0000001



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 20001, 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>

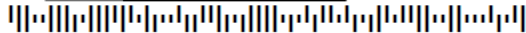
NYS Department of State's Division of Consumer
Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

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.

June 3, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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 prevent incidents like this from occurring in the future.



0000001



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 IdentityWorksSM 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: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by September 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

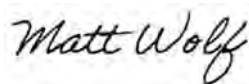
To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- 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,



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 your 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



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 20001, 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.



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

June 5, 2024



Re: Notice of Data Security Incident

Dear :

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 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 its partnership with one such organization in connection with its 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 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 prevent incidents like this from occurring in the future.



0000001



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 IdentityWorksSM 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: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by September 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,



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.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 your 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



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, <https://www.marylandattorneygeneral.gov>.

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>

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

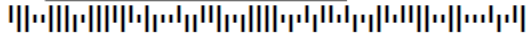
For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

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.



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

June 5, 2024



Re: Notice of Data Security Incident

Dear [Redacted]:

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 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 its partnership with one such organization in connection with its 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 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 prevent incidents like this from occurring in the future.



0000001



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 IdentityWorksSM 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: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by September 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,



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.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 your 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



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, <https://www.marylandattorneygeneral.gov>.

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>

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.



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.

0000001



Cencora is also making resources available to you. While we have no reason at this time 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 free access to Experian IdentityWorksSM credit monitoring and remediation services for 24 months. 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 Credit Monitoring and Remediation services?

While identity restoration assistance is immediately available to you, we also encourage you to activate the free 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 free credit monitoring services described above, you must enroll by September 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

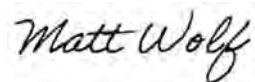
To help protect your personal information, we strongly recommend you take the following steps:

- Enroll in the free credit monitoring service that we are offering to you. This will enable you to get alerts about any attempts to use your personal information 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. Cencora encourages 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,



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.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 your 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



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, <https://www.marylandattorneygeneral.gov>.

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

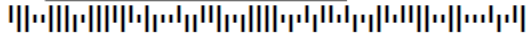
For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

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.



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

June 11, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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 prevent incidents like this from occurring in the future.



0000001



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 IdentityWorksSM 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: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by September 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

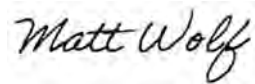
To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- 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,



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.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 your 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



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, <https://www.marylandattorneygeneral.gov>.

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>

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.

June 20, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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, Social Security number, 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 prevent 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 IdentityWorksSM 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: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by September 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

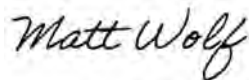
To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- 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,



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.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 your 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

0000586



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, <https://www.marylandattorneygeneral.gov>.

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>

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

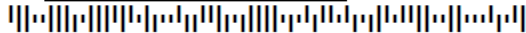
For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

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.



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

July 8, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

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 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 its partnership with one such organization in connection with its 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 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 prevent incidents like this from occurring in the future.



0000001



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 IdentityWorksSM 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: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by September 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,



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.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 your 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



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, <https://www.marylandattorneygeneral.gov>.

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>

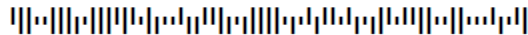
NYS Department of State's Division of Consumer
Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

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.

July 30, 2024



Re: Notice of Data Security Incident

Dear 

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 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 its partnership with one such organization in connection with its 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 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 prevent incidents like this from occurring in the future.



0000001



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 IdentityWorksSM 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: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by November 29, 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

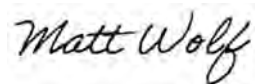
To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- 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 to block that credit from being established 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,



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.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 your 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.

0000001



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 20001, 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, or <https://www.marylandattorneygeneral.gov>.

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>

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.



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

October 8, 2024



Re: Notice of Data Security Incident

Dear [REDACTED]:

TheraCom, L.L.C. ("TheraCom"), a mail-order specialty pharmacy owned by Cencora, Inc., dispenses prescription medication often at no charge to individuals enrolled in patient assistance programs. 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 TheraCom has regarding shipments of prescription medications to you.

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 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. As part of our investigation, we reviewed the impacted data to determine whether personal information was compromised in any way. On August 14, 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 your first name, last name, address, and medical treatment information. 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.



1 West First Avenue
Conshohocken, PA 19428
www.cencora.com

0000835



M1804-L01

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 prevent 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 IdentityWorksSM 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 or 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: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by January 31, 2025. 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 1-833-918-8818. 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 1-833-918-8818. Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,

Guy Payette
President, TheraCom, L.L.C.

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 your 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 20001, 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, <https://www.marylandattorneygeneral.gov>.

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>

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.

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Wednesday, May 29, 2024 9:32:52 AM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Wed, 05/29/2024 - 13:30

Submitted by: Anonymous

Submitted values are:

Name

Abbott

Street Address

100 Abbott Park Road
Abbott Park, Illinois. 60064

Name

Gregory Parks

Title

Partner

Dated

2024-05-29

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Other Commercial

Total (Including VT residents)

2910

Total VT Residents

3

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discov ered

2024-04-10

Consumer Notification(s)

2024-05-29

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice_Abbott_5-29-2024.pdf](#) (231.95 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Tuesday, May 21, 2024 1:06:05 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Tue, 05/21/2024 - 17:02

Submitted by: Anonymous

Submitted values are:

Name

AbbVie Inc.

Street Address

1 North Waukegan Road
North Chicago, Illinois. 60064-6400

Name

Gregory Parks

Title

Partner

Dated

2024-05-21

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside Counsel to Lash Group

(please select one)

Health Care

Total (Including VT residents)

272433

Total VT Residents

280

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

Yes

Breach Occured

2024-02-21

Breach Dis covered

2024-04-10

Consumer Notification(s)

2024-05-21

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_AbbVie.pdf](#) (219.4 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Tuesday, May 21, 2024 1:47:26 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Tue, 05/21/2024 - 17:46

Submitted by: Anonymous

Submitted values are:

Name

Acadia Pharmaceuticals Inc.

Street Address

12830 El Camino Real, Suite 400
San Diego, California. 92130

Name

Gregory Parks

Title

Partner

Dated

2024-05-21

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

40389

Total VT Residents

91

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024- 02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-21

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Letter.pdf](#) (306.18 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Thursday, June 20, 2024 3:11:48 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Thu, 06/20/2024 - 19:10

Submitted by: Anonymous

Submitted values are:

Name

Acrotech Biopharma Inc.

Street Address

279 Princeton Hightstown Road
East Windsor, New Jersey. 08520

Name

Gregory Parks

Title

Partner

Dated

2024-06-20

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

10406

Total VT Residents

23

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-06-20

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Social Security Number, Medical Records/Health Information

(select all that apply)

Written

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[Acrotech Individual Notice Letter.pdf](#) (411.64 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Monday, May 20, 2024 4:32:00 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Mon, 05/20/2024 - 20:29

Submitted by: Anonymous

Submitted values are:

Name

Alexion Pharmaceuticals, Inc.

Street Address

121 Seaport Boulevard
Boston, Massachusetts. 02210

Name

Gregory Parks

Title

Partner

Dated

2024-05-20

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to the Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

1734

Total VT Residents

2

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-20

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Letter.pdf](#) (278.82 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Tuesday, May 21, 2024 3:36:54 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Tue, 05/21/2024 - 19:35

Submitted by: Anonymous

Submitted values are:

Name

Alkermes, Inc.

Street Address

900 Winter Street
Waltham, Massachusetts. 02451

Name

Gregory Parks

Title

Partner

Dated

2024-05-21

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

11734

Total VT Residents

5

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-21

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Letter.pdf](#) (306.18 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Thursday, May 30, 2024 9:15:18 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 05/31/2024 - 01:13

Submitted by: Anonymous

Submitted values are:

Name

Amgen Inc.

Street Address

One Amgen Center Drive
Thousand Oaks, California. 91320

Name

Gregory Parks

Title

Partner

Dated

2024-05-30

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

1649867

Total VT Residents

886

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-30

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Redacted 5-30-24.pdf](#) (237.86 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Wednesday, June 5, 2024 2:48:21 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Wed, 06/05/2024 - 18:47

Submitted by: Anonymous

Submitted values are:

Name

Bausch Health Companies Inc.

Street Address

400 Somerset Corporate Blvd.
Bridgewater, New Jersey. 08807

Name

Gregory Parks

Title

Partner

Dated

2024-06-05

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

10330

Total VT Residents

7

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-06-05

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Letter 6.5.24.pdf](#) (227.95 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Wednesday, June 5, 2024 8:43:27 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Thu, 06/06/2024 - 00:40

Submitted by: Anonymous

Submitted values are:

Name

Bausch + Lomb

Street Address

400 Somerset Corporate Blvd
Bridgewater, New Jersey. 08807

Name

Gregory Parks

Title

Partner

Dated

2024-06-05

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

5120

Total VT Residents

1

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

< b>Breach Discovered

2024-04-10

Consumer Notification(s)

2024-06-05

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Letter 6.5.24.pdf](#) (227.95 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Monday, May 20, 2024 12:55:51 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Mon, 05/20/2024 - 16:52

Submitted by: Anonymous

Submitted values are:

Name

Bayer Corporation

Street Address

100 Bayer Boulevard
Whippany, New Jersey. 07981

Name

Gregory Parks

Title

Partner

Dated

2024-05-20

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to the Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

102520

Total VT Residents

167

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

B reach Discovered

2024-04-10

Consumer Notification(s)

2024-05-20

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Letter.pdf](#) (278.82 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Friday, May 17, 2024 2:18:45 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 05/17/2024 - 18:17

Submitted by: Anonymous

Submitted values are:

Name

Bristol Myers Squibb Company and Bristol Myers Squibb Patient Assistance Foundation

Street Address

Route 206 & Province Line Road
Princeton, New Jersey. 08543

Name

Gregory Parks

Title

Partner

Dated

2024-05-17

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

2916417

Total VT Residents

3603

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified? Yes

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-17

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[BMS_L01_SAS_1.pdf](#) (221.56 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Thursday, May 23, 2024 2:56:28 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Thu, 05/23/2024 - 18:53

Submitted by: Anonymous

Submitted values are:

Name

Dendreon Pharmaceuticals LLC

Street Address

1700 Saturn Way
Seal Beach, California. 90740

Name

Gregory Parks

Title

Partner

Dated

2024-05-23

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

49787

Total VT Residents

62

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-23

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice \(5.23.2024\).pdf](#) (237.19 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Friday, May 24, 2024 1:09:36 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 05/24/2024 - 17:08

Submitted by: Anonymous

Submitted values are:

Name

Endo Pharmaceuticals Inc.

Street Address

1400 Atwater Drive
Malvern, Pennsylvania. 19355

Name

Gregory Parks

Title

Partner

Dated

2024-05-24

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

11452

Total VT Residents

9

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-24

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice 5.24.2024.pdf](#) (235.65 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Monday, May 20, 2024 4:11:46 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Mon, 05/20/2024 - 20:05

Submitted by: Anonymous

Submitted values are:

Name

Genentech, Inc.

Street Address

1 DNA Way
South San Francisco, California. 94080

Name

Gregory Parks

Title

Partner

Dated

2024-05-20

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

80854

Total VT Residents

36

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-20

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Letter.pdf](#) (278.82 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Wednesday, May 22, 2024 1:57:28 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Wed, 05/22/2024 - 17:55

Submitted by: Anonymous

Submitted values are:

Name

Grifols USA, LLC and Grifols Shared Services North America, Inc.

Street Address

2410 Grifols Way
Los Angeles, California. 90032

Name

Gregory Parks

Title

Partner

Dated

2024-05-22

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside Counsel to Lash Group

(please select one)

Health Care

Total (Including VT residents)

8091

Total VT Residents

10

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

Yes

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-22

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice \(5.22.2024\).pdf](#) (233.17 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Friday, May 24, 2024 3:12:22 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 05/24/2024 - 19:07

Submitted by: Anonymous

Submitted values are:

Name

GlaxoSmithKline Group of Companies and the GlaxoSmithKline Patient Access Programs Foundation

Street Address

c/o David Kessler, Norton Rose Fulbright US LLP, 1301 Avenue of the Americas
New York, New York. 10019

Name

Gregory Parks

Title

Partner

Dated

2024-05-24

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

747585

Total VT Residents

386

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

Yes

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-24

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Electronic, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L 01 Individual Notice_GSK_5-24-2024.pdf](#) (263.39 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Monday, June 3, 2024 6:35:10 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Mon, 06/03/2024 - 22:33

Submitted by: Anonymous

Submitted values are:

Name

Heron Therapeutics, Inc.

Street Address

4242 Campus Point Court, Suite 200
San Diego, California. 92121

Name

Gregory Parks

Title

Partner

Dated

2024-06-03

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

56331

Total VT Residents

8

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-06-03

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice 6.3.24.pdf](#) (219.07 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Thursday, May 23, 2024 11:16:00 AM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Thu, 05/23/2024 - 15:14

Submitted by: Anonymous

Submitted values are:

Name

Incyte Corporation

Street Address

1801 Augustine Cut-Off
Wilmington, Delaware. 19803

Name

Gregory Parks

Title

Partner

Dated

2024-05-23

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside Counsel to Lash Group

(please select one)

Health Care

Total (Including VT residents)

36040

Total VT Residents

62

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

Yes

Breach Occured

2024-02-21

Breach Disco vered

2024-04-10

Consumer Notification(s)

2024-05-23

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice 5.23.2024.pdf](#) (258.01 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Tuesday, May 28, 2024 1:38:24 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Tue, 05/28/2024 - 17:33

Submitted by: Anonymous

Submitted values are:

Name

Johnson & Johnson Patient Assistance Foundation, Inc.

Street Address

P.O. Box #0367
Chesterfield, Missouri. 63006

Name

Gregory Parks

Title

Partner

Dated

2024-05-28

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

1241911

Total VT Residents

723

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-28

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Redacted 5-28-24.pdf](#) (263.38 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Tuesday, May 28, 2024 3:19:31 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Tue, 05/28/2024 - 19:13

Submitted by: Anonymous

Submitted values are:

Name

Johnson and Johnson Services, Inc.

Street Address

One Johnson & Johnson Plaza
New Brunswick, New Jersey. 08933

Name

Gregory Parks

Title

Partner

Dated

2024-05-28

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside Counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

411160

Total VT Residents

244

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-28

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice 5.28.2024.pdf](#) (263.38 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Wednesday, May 15, 2024 4:54:50 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Wed, 05/15/2024 - 20:52

Submitted by: Anonymous

Submitted values are:

Name

Marathon Pharmaceuticals, LLC/PTC Therapeutics, Inc.

Street Address

500 Warren Corporate Center Drive
Warren, New Jersey. 07059

Name

Gregory Parks

Title

Partner

Dated

2024-05-15

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

4444

Total VT Residents

6

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

Yes

Breach Occured< br />2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-15

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Redacted 5-15-24.pdf](#) (215.17 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Tuesday, July 30, 2024 9:58:46 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Wed, 07/31/2024 - 01:57

Submitted by: Anonymous

Submitted values are:

Name

Merck, Sharp & Dohme Corp.

Street Address

126 East Lincoln Avenue P.O. Box 2000
Rahway, New Jersey. 07065

Name

Gregory Parks

Title

Partner

Dated

2024-07-30

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

12559

Total VT Residents

2

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02- 21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-07-30

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

Experian

Provider

2 years

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[Lash_Individual Letter.pdf](#) (231.16 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Wednesday, May 22, 2024 2:15:04 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Wed, 05/22/2024 - 18:13

Submitted by: Anonymous

Submitted values are:

Name

Novartis Pharmaceuticals Corporation

Street Address

One Health Plaza
East Hanover, New Jersey. 07936

Name

Gregory Parks

Title

Partner

Dated

2024-05-22

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

182279

Total VT Residents

119

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-22

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice - Novartis - 5-22-24.pdf](#) (247.97 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Monday, July 8, 2024 4:15:44 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Mon, 07/08/2024 - 20:14

Submitted by: Anonymous

Submitted values are:

Name

Otsuka Patient Assistance Foundation

Street Address

508 Carnegie Center Dr.
Princeton, New Jersey. 08540

Name

Gregory Parks

Title

Partner

Dated

2024-07-08

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

39368

Total VT Residents

9

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-07-08

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Letter 7.8.24.pdf](#) (230.35 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Friday, May 31, 2024 4:13:21 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 05/31/2024 - 20:09

Submitted by: Anonymous

Submitted values are:

Name

Otsuka America Pharmaceutical, Inc.

Street Address

2440 Research Blvd.
Rockville, Maryland. 20850

Name

Gregory Parks

Title

Partner

Dated

2024-05-31

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

41402

Total VT Residents

10

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

< b>Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-31

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Redacted 5-31-24.pdf](#) (304.99 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Friday, June 7, 2024 4:40:32 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 06/07/2024 - 20:38

Submitted by: Anonymous

Submitted values are:

Name

Pfizer Inc.

Street Address

66 Hudson Boulevard East
New York, New York. 10001

Name

Gregory Parks

Title

Partner

Dated

2024-06-07

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

116970

Total VT Residents

142

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-06-07

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice \(Pfizer\) 6.7.24.pdf](#) (236.39 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Thursday, May 16, 2024 2:56:19 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Thu, 05/16/2024 - 18:28

Submitted by: Anonymous

Submitted values are:

Name

Pharming Healthcare, Inc.

Street Address

10 Independence Blvd
Warren, New Jersey. 07059

Name

Gregory Parks

Title

Partner

Dated

2024-05-16

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

3717

Total VT Residents

2

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-16

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[Template Individual Notification Pharming, Lash Group 5-16-24.pdf](#) (249.36 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Friday, May 31, 2024 4:25:02 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 05/31/2024 - 20:23

Submitted by: Anonymous

Submitted values are:

Name

Rayner Surgical Inc.

Street Address

1255 Lynnfield Road Suite 257
Memphis, Tennessee. 38119

Name

Gregory Parks

Title

Partner

Dated

2024-05-31

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel

(please select one)

Health Care

Total (Including VT residents)

84848

Total VT Residents

2

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discoverer d

2024-04-10

Consumer Notification(s)

2024-05-31

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Redacted 5-31-24.pdf](#) (304.99 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Wednesday, May 22, 2024 7:47:59 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Wed, 05/22/2024 - 23:46

Submitted by: Anonymous

Submitted values are:

Name

Regeneron Pharmaceuticals, Inc.

Street Address

777 Old Saw Mill River Road
Tarrytown, New York. 10591

Name

Gregory Parks

Title

Partner

Dated

2024-05-22

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

1199605

Total VT Residents

2656

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

Yes

Breach Occured

202 4-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-22

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice \(5.22.2024\).pdf](#) (233.17 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Friday, May 31, 2024 3:22:32 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 05/31/2024 - 19:20

Submitted by: Anonymous

Submitted values are:

Name

Sandoz Inc.

Street Address

100 College Rd W
Princeton, New Jersey. 08450

Name

Gregory Parks

Title

Partner

Dated

2024-05-31

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

5479

Total VT Residents

1

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discov ered

2024-04-10

Consumer Notification(s)

2024-05-31

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Redacted 5-31-24.pdf](#) (304.99 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Thursday, May 30, 2024 4:38:34 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Thu, 05/30/2024 - 20:37

Submitted by: Anonymous

Submitted values are:

Name

Sanofi US Services Inc.

Street Address

55 Corporate Drive
Bridgewater, New Jersey. 08807

Name

Gregory Parks

Title

Partner

Dated

2024-05-30

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

1742019

Total VT Residents

1560

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

Yes

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-30

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

5 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice \(Sanofi\) 5.30.24.pdf](#) (234.67 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Tuesday, May 28, 2024 1:13:34 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Tue, 05/28/2024 - 17:11

Submitted by: Anonymous

Submitted values are:

Name

Smith & Nephew, Inc.

Street Address

1450 East Brooks Road
Memphis, Tennessee. 38116

Name

Gregory Parks

Title

Partner

Dated

2024-05-28

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[215-963-5170](tel:215-963-5170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

14578

Total VT Residents

2

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-28

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Redacted 5-28-24.pdf](#) (263.38 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Thursday, May 23, 2024 3:51:55 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Thu, 05/23/2024 - 19:50

Submitted by: Anonymous

Submitted values are:

Name

Sumitomo Pharma America, Inc.

Street Address

84 Waterford Dr.
Marlborough, Massachusetts. 01752

Name

Gregory Parks

Title

Partner

Dated

2024-05-23

Firm Name (if other than entity)

Morgan, Lewis & Bockius

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

130689

Total VT Residents

15

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-23

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Individual Notice \(Sumitomo\) 5.23.24.pdf](#) (230.27 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach Submissions](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Friday, May 31, 2024 3:31:08 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Fri, 05/31/2024 - 19:30

Submitted by: Anonymous

Submitted values are:

Name

Takeda Pharmaceuticals U.S.A., Inc.

Street Address

95 Hayden Avenue
Lexington, Massachusetts. 02421

Name

Gregory Parks

Title

Partner

Dated

2024-05-31

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside counsel to The Lash Group, LLC

(please select one)

Health Care

Total (Including VT residents)

100794

Total VT Residents

69

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach Discovered

2024-04-10

Consumer Notification(s)

2024-05-31

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

2 years

Provider

Experian

Brief Description of Service

Credit monitoring and identity theft protection services

Please attach Form of Consumer Notice

[L01_Redacted 5-31-24.pdf](#) (304.99 KB)

From: vt-noreply@egov.gov on behalf of [Office of the Vermont Attorney General](#)
To: [AGO - Security Breach](#)
Cc: CencoraSupport@morganlewis.com
Subject: Webform submission from: VERMONT STATE SECURITY BREACH REPORTING FORM
Date: Tuesday, October 8, 2024 6:49:52 PM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Submitted on Tue, 10/08/2024 - 22:49

Submitted by: Anonymous

Submitted values are:

Name

TheraCom, L.L.C.

Street Address

1 West First Avenue
Conshohocken, Pennsylvania. 19428

Name

Gregory Parks

Title

Partner

Dated

2024-10-08

Firm Name (if other than entity)

Morgan, Lewis & Bockius LLP

Telephone

[2159635170](tel:2159635170)

Email

CencoraSupport@morganlewis.com

Relationship to Entity whose information was compromised

Outside Counsel to TheraCom, LLC

(please select one)

Health Care

Total (Including VT residents)

9271

Total VT Residents

19

If the number of consumers notified exceeds 1,000 have the consumer reporting agencies been notified?

N/A

Breach Occured

2024-02-21

Breach D iscovered

2024-08-14

Consumer Notification(s)

2024-10-08

(select all that apply)

External system breach (e.g., hacking)

(select all that apply)

Medical Records/Health Information

(select all that apply)

Written, Substitute Notice

Has anything been offered?

Yes

Duration

24 months

Provider

Experian IdentityWorks

Brief Description of Service

Credit monitoring and identity protection.

Please attach Form of Consumer Notice

[10-1 TheraCom-AG Ntc Form-VT Sample Ntc.pdf](#) (274.85 KB)