

October 17, 2022

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Email:

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Cybersecurity Incident Involving Symbia Logistics

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Symbia Logistics, (“Symbia”), is a national logistics company located at 15965 E 32nd Ave, Suite A, Aurora, Colorado, with respect to a recent cybersecurity incident that was first discovered by Symbia on July 6, 2021 (hereinafter, the “Incident”). Symbia takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that Symbia has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On July 6, 2021, Symbia discovered the Incident when their systems experienced a ransomware event. Upon discovery of the incident, Symbia promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation determined that there was unauthorized access to potentially personal information on November 1, 2021. A data mining firm was engaged and began work on Symbia’s systems on February 4, 2022. The amount of data was quite large for the data mining firm to review. Therefore, Symbia immediately began a thorough review of the potentially accessed files to identify the individuals whose sensitive information was present at the time of the incident. Symbia worked to identify the notice population and this was completed by Symbia on September 2, 2022. This step was necessary so that Symbia could send a notice of the incident to ensure the potentially impacted individuals are aware of this Incident.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

Although Symbia is unaware of any fraudulent misuse of information, it is possible that individuals' full name, Social Security number, and driver's license may have been exposed as a result of this unauthorized activity.

As of this writing, Symbia has not received any reports of related identity theft since the date of the incident (July 6, 2021 to present).

2. Number of Maryland residents affected.

A total of 179 Maryland resident(s) may have been potentially affected by this incident. Notification letters to these individuals were mailed on October 17, 2022, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Symbia is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Symbia moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, Symbia has taken several remediation steps to prevent a future incident like this from occurring; such as: deploying enterprise leaders in XDR solutions to provide a comprehensive security solution across our organization; installing multi-factor authentication to provide a level of identity verification beyond basic login credentials; MDM and endpoint security solutions to secure and manage mobile devices in our environment; completed a third party security audit to identify and update any existing vulnerabilities within our environment; holding weekly meetings to review security logs and any vulnerabilities discovered in the environment; implemented a secure password manager that requires multi-factor authentication to obtain access, continually stayed updated on device firmware and security; added a third party security company to provide fully-managed protection, monitoring and response services including a 24/7 Security Operations Center; and continue our onsite, offsite and cloud-based backup solutions. Lastly, Symbia informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although Symbia is not aware of any actual or attempted misuse of the affected personal information, offered 12 months of complimentary credit monitoring and identity theft restoration services through IDX to all individuals to help protect their identity. Additionally, Symbia provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

Symbia remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A



Symbia Logistics
15965 E 32nd Ave, Suite A
Aurora, CO 80011

Via First-Class Mail
October 17, 2022

<First Name> <Last Name>
<Address1> <Address2>
<City>, <State> <Zip>

Re: Notice of Data Breach

Dear <First Name> <Last Name>,

Symbia Logistics ("Symbia") is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On July 6, 2021, Symbia discovered the Incident when their systems experienced a ransomware event. Upon discovery of the incident, Symbia promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation determined that there was unauthorized access to potentially personal information on November 1, 2021. A data mining firm was engaged and began work on Symbia's systems on February 4, 2022. The amount of data was quite large for the data mining firm to review. Therefore, Symbia immediately began a thorough review of the potentially accessed files to identify the individuals whose sensitive information was present at the time of the incident. Symbia worked to identify the notice population and this was completed by Symbia on September 2, 2022. This step was necessary so that Symbia could send a notice of the incident to ensure the potentially impacted individuals are aware of this Incident.

As of this writing, Symbia has not received any reports of related identity theft since the date of the incident (July 6, 2021 to present).

To Enroll, Please Call:

[TFN]

[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)

Enrollment Code: [XXXXXXXXXX]

What Information Was Involved?

Although Symbia has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the following information related to you may have been subject to unauthorized access: name; address; Social Security number; and driver's license. **Please note that no financial information; such as: credit card number; debit card number; or banking information was impacted.**

What We Are Doing

Data privacy and security is among Symbia's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, Symbia moved quickly to investigate, respond, and confirm the security of our systems. Specifically, Symbia has taken several remediation steps to prevent a future incident like this from occurring; such as: deploying enterprise leaders in XDR solutions to provide a comprehensive security solution across our organization; installing multi-factor authentication to provide a level of identity verification beyond basic login credentials; MDM and endpoint security solutions to secure and manage mobile devices in our environment; completed a third party security audit to identify and update any existing vulnerabilities within our environment; holding weekly meetings to review security logs and any vulnerabilities discovered in the environment; implemented a secure password manager that requires multi-factor authentication to obtain access, continually stayed updated on device firmware and security; added a third party security company to provide fully-managed protection, monitoring and response services including a 24/7 Security Operations Center; and continue our onsite, offsite and cloud-based backup solutions. Lastly, Symbia informed our law firm and began identifying the potentially affected individuals in preparation for notice.

In light of the incident, we are also providing you with twelve (12) months of complimentary credit monitoring and identity theft restoration services through IDX. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the credit monitoring services we are making available to you at no cost. The deadline to enroll is January 24, 2023.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call <PHONE NUMBER> (toll free) Monday through Friday, during the hours of 8:00 a.m. and 5:00 p.m. MST (excluding U.S. national holidays).

Symbia sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Brian. P. Grady
Chief Financial Officer
Symbia Logistics



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-814-1703 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity. IDX Call Center will be open October 24, 2022.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.