jackson lewis

Jackson Lewis P.C.
200 Connell Drive
Suite 2000
Berkeley Heights, NJ 07922
Tel 908 795-5200
Fax 908 464-2614
www.jacksonlewis.com
Richard J. Cino - Managing Principal

JASON C. GAVEJIAN
Email: Jason.Gavejian@jacksonlewis.com

March 5, 2020

VIA OVERNIGHT MAIL
Office of Attorney General
Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification[4]

Dear Attorney General MacDonald:

Please be advised that on February 8, 2020, our client, Lonza America, Inc. ("Lonza"), learned that personal information of state residents may have been subject to unauthorized access or acquisition as the result of a cyberattack which occurred at a third-party vendor of Lonza (the "Incident"). Based on the investigation, it appears the Incident occurred between January 4, 2020 and January 16, 2020. The data elements involved may have included name, birth date, Social Security numbers, driver's license number, passport number, state/federal identification number, financial account information, and/or medical or health information.

Immediately upon learning about the Incident, Lonza commenced an investigation to determine the scope of the Incident and identify those potentially affected. This included Lonza working with its information technology team and third-party forensic experts in an effort to ensure the Incident did not result in any additional exposure to personal information, and to determine what information may have been accessed or acquired. The investigation determined that the unauthorized actor may have gained access to a hard drive of the vendor which contained Lonza data but was unable to determine what information contained within the drive was access or acquired as a result of this Incident. Thus, Lonza engaged a firm to perform data mining on the impacted files/folders on the drive to determine whether they contained any personal information.

Based on the results of the data mining, it appears that 88 individuals could have been affected, including 4 New Hampshire residents. In light of this Incident, Lonza plans to begin notifying individuals in the next several days. Lonza will also provide one year of free credit monitoring to all affected individuals. A draft copy of the notification that will be sent is enclosed with this letter.

As set forth in the enclosed letter, Lonza has taken numerous steps to protect the security of the personal information of all individuals. In addition to continuing to monitor this situation, Lonza is reexamining its current privacy and data security policies and procedures to find ways of reducing the risk of future data incidents. Lonza is also reviewing its technical security policies and procedures and making

[4] Please note that by providing this letter Lonza is not agreeing to the jurisdiction of State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

jackson lewis.

improvements where it can to minimize the chances of this happening again. Should Lonza become aware of any significant developments concerning this situation, we will inform you.

***

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS P.C.

s/ Jason C. Gavejian
Jason C. Gavejian

JCG:tcm
Enclosure

4819-8469-0357, v. 1

Lonza
412 Mt. Kemble Ave.
Morristown, NJ 07960

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

Re: Notice of Data Breach

Dear _____:

At Lonza, we value our employees and respect the privacy of your information, which is why we are writing to inform you we recently learned that some of your personal information may have been subject to unauthorized access or acquisition as the result of a data incident that occurred at a third-party vendor of Lonza. While we are not aware of any misuse of your information, we apologize for any inconvenience this may cause you and assure you that we have worked diligently to resolve this matter and continue to deploy measures to avoid these types of incidents from occurring in the future. Below you will also find instructions and a code redeemable for one year of credit monitoring with Experian.

What Happened?

On February 8, 2020, Lonza discovered that your personal information may have been accessible to an unauthorized actor as a result of a cyberattack at the third-party vendor (the "Incident"). Based on the investigation, it appears the Incident occurred at the vendor between January 4, 2020 and January 16, 2020. After conducting a thorough internal investigation, we have no reason to believe that any Lonza systems were compromised. The Incident only occurred on the systems of this third-party vendor.

What Information Was Involved?

The type of data accessed or acquired may have included personal information such as your name, birth date, Social Security number, driver's license number, passport number, state/federal identification number, financial account information, and/or medical or health information.

What We Are Doing.

Lonza values your privacy, and immediately upon learning about the Incident we launched an investigation to determine the scope of the Incident and identify those affected. This included working with our information technology team and third-party forensic experts in an effort to ensure the Incident did not result in any additional exposure to personal information, and taking steps to confirm the integrity of Lonza's electronic systems. We also worked with

third-party experts to determine what information may have been at risk. This investigation is on-going, and Lonza will notify you if there are any significant developments.

Lonza has also reported the Incident to the Federal Bureau of Investigation ("FBI") to assist in our investigations and best protect our employees from any incidents like this in the future. This communication was not delayed at the request of law enforcement.

As an added precaution, we have arranged for credit monitoring and identity restoration services to be provided to you by Experian. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks℠ as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **[date]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **[URL]**
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **[customer service number]** by **[enrollment end date]**. Be prepared to provide engagement number **[engagement number]** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do.

In addition to taking advantage of the credit monitoring and identity restoration services outlined above, there are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to the below and www.ExperianIDWorks.com/restoration for this information.

Other Important Information.

We treat all personal information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. Unauthorized access to personal information and similar incidents are difficult to prevent in all instances; however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again.

For More Information.

For more information, for further assistance, or if you have questions or concerns you should call [Insert Number] from [Hours]. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

Lonza North America Inc.
Brad Luria
General Counsel, North America

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
- Place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies.
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

2. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. You may contact the FTC by visiting www.ftc.gov or www.consumer.gov/idtheft, calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that you are the victim of identity theft, you should contact local police and/or your state Attorney General. You can also report such activity to the Fraud Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

3. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

4. If you believe you are a victim of identity theft you should immediately report same to law enforcement and/or your state attorney general.

5. *For Maryland Residents*: The contact information for the Maryland Office of the Attorney General is: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Telephone: (888) 743-0023; website: http://www.oag.state.md.us. us.

6. *For New Mexico Residents*: 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 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. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf

7. *For North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: www.ncdoj.com/.

8. *For Rhode Island Residents*: The contact information for the Rhode Island Office of the Attorney General is: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; Telephone: (401) 274-4400; website: http://www.riag.ri.gov. The total number of affected individuals is currently unknown.