Lonza

Emilee Terry
Associate General Counsel
360 Interstate North Parkway
Suite 450
Atlanta, GA 30339

www.Lonza.com

January 24, 2018

State of New Hampshire
Office of the Attorney General Gordon MacDonald
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3658

Dear Mr. MacDonald,

Lonza has just finalized an internal investigation into the cause and scope of a recent data breach and an assessment of whether misuse of such data occurred or is reasonably likely to occur. Pursuant to RSA 359-C:20, we are now contacting your office in advance of providing notice to the affected individuals.

At the end of December, Lonza's IT Security group became aware that twelve of our employees' WorkDay accounts were accessed by an unauthorized entity sometime in November or December 2017. Two of these employees are located in the State of New Hampshire. After investigating the situation, Lonza determined that hackers were able to access these employees' log-in credentials through a phishing attack. I have attached a draft of the notices that Lonza plans to send to the affected employees in New Hampshire this week.

The notice provides additional details of the incident, including enhanced security measures Lonza has already adopted to prevent future breaches. I have also attached a letter that Lonza will be providing along with the notice, which explains how the impacted employees can sign up for credit monitoring services offered by Lonza at no cost to these employees.

Finally, Lonza will be providing communication to its employees who were not affected, informing them of the incident, how to prevent such occurrences in the future, and is planning additional company-wide training on data breach prevention.

Please do not hesitate to contact me with any questions.

Sincerely,

Emilee Terry

Lonza

[Letter to Payroll Impacted Employee]

Employee Name
ADDRESS
ADDRESS
ADDRESS

January __, 2018

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 of a data breach that recently occurred. While this breach was limited in scope, it affected some of your personal information.

What Happened?

In the fall of 2017 Lonza employees were exposed to several phishing attempts, some of which resulted in hackers accessing a small number of employees' credentials. On December 29, 2017 Lonza became aware that certain employees' WorkDay accounts were accessed by an unauthorized entity sometime in November or December of 2017. As a result, the hackers were able to view an account holder's personal information and reroute direct deposit paychecks into a bank account that they could access.

What Information Was Involved?

While we cannot confirm exactly what information was viewed, this incident potentially provided access to any and all of your personal information that is stored on this WorkDay platform.

What We Are Doing.

Lonza values your privacy, and upon learning about the unauthorized access of certain employees' WorkDay accounts, Lonza immediately launched an internal investigation. We have completed the investigation of this incident as it relates to your WorkDay account, and Lonza has begun enhancing security measures to prevent future breaches. At this time, Lonza has already implemented new security measures to protect employees' WorkDay accounts, including requiring an additional approval step before changing payment elections in a WorkDay account.

In addition to taking steps to enhance our data protection measures, Lonza is now offering you and the other employees impacted by this data breach two years of free credit monitoring provided through Experian. Please review the enclosed "Steps You Can Take to Further Protect Your Information" and the attached letter for additional instructions on enrolling for this service.

Finally, for those employees whose payroll direct deposti was intercepted as a result of the unauthorized access, Lonza has already re-deposited the lost amounts into your account.

Lonza

What You Can Do.

Please also review the enclosed "Steps You Can Take to Further Protect Your Information" for further information on steps that you can take to protect your personal information and instructions on how to receive free credit monitoring services for two years.

Other Important Information.

In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with your ability to apply for a new credit card or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift, or remove the security freeze.

For More Information.

For more information and further assistance, please contact **Lorraine Mercede** at 201 683-2919 or via email at Lorraine.mercede@lonza.com.

Sincerely,

Walter Fux
Data Privacy Officer

Lorraine Mercede
Head of HR Service Center-Americas

Lonza

Steps You Can Take to Further Protect Your Information

1. Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

2. Credit Report Monitoring

In addition, Lonza has arranged with Experian to provide you with credit monitoring services for two years, at no cost to you. The attached letter provides you with a summary of the benefits as well as instructions for enrolling in the service. To take advantage of this offer, you must enroll by **April 30, 2018**.

3. Credit Reporting Services

For your reference, contact information for the three national credit reporting agencies is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

4. Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

5. Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

Lonza

[Letter to Non-Payroll Impacted Employee]

Employee Name
ADDRESS
ADDRESS
ADDRESS

January __, 2018

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 of a data breach that recently occurred. While this breach was limited in scope, it affected some of your personal information.

What Happened?

In the fall of 2017 Lonza employees were exposed to several phishing attempts, some of which resulted in hackers accessing a small number of employees' credentials. On December 29, 2017 Lonza became aware that certain employees' WorkDay accounts were accessed by an unauthorized entity sometime in November or December of 2017. As a result, the hackers were able to view an account holder's personal information.

What Information Was Involved?

While we cannot confirm exactly what information was viewed, this incident potentially provided access to any and all of your personal information that is stored on this WorkDay platform.

What We Are Doing.

Lonza values your privacy, and upon learning about the unauthorized access of certain employees' WorkDay accounts, Lonza immediately launched an internal investigation. We have completed the investigation of this incident as it relates to your WorkDay account, and Lonza has begun enhancing security measures to prevent future breaches. At this time, Lonza has already implemented new security measures to protect employees' WorkDay accounts, including requiring an additional approval step before changing payment elections in a WorkDay account.

In addition to taking steps to enhance our data protection measures, Lonza is now offering you and the other employees impacted by this data breach two years of free credit monitoring. Please review the enclosed "Steps You Can Take to Further Protect Your Information" and the attached letter for additional instructions on enrolling for this service.

Lonza

What You Can Do.

Please also review the enclosed "Steps You Can Take to Further Protect Your Information" for further information on steps that you can take to protect your personal information and instructions on how to receive free credit monitoring services for two years.

Other Important Information.

In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with your ability to apply for a new credit card or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift, or remove the security freeze.

For More Information.

For more information and further assistance, please contact Lorraine Mercede at 201 683-2919 or via email at Lorraine.mercede@lonza.com.

Sincerely,

Walter Fux
Data Privacy Officer

Lorraine Mercede
Head of HR Service Center-Americas

Lonza

Steps You Can Take to Further Protect Your Information

1. Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

2. Credit Report Monitoring

In addition, Lonza has arranged with Experian to provide you with credit monitoring services for two years, at no cost to you. The attached letter provides you with a summary of the benefits as well as instructions for enrolling in the service. To take advantage of this offer, you must enroll by **April 30, 2018**.

3. Credit Reporting Services

For your reference, contact information for the three national credit reporting agencies is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

4. Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

5. Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

Lonza

[Letter Regarding Credit Monitoring Services]

Lonza

90 Boroline Road
Allendale, NJ 07401 USA

201 683 2919 Phone
lorraine.mercede@lonza.com

Employee Name
Address
City/State/Zip

Experian *Identity Restoration and Fraud Detection Monitoring*

Dear Employee Name:

As indicated in the letter from _____, in addition to taking steps to enhance our data protection measures, Lonza is now offering you and the other employees impacted by this data breach two years of free Identity Restoration and fraud detection monitoring.

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 two-years 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 SM as a complimentary two-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: April 30, 2018** (Your code will not work after this date).
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/3bplus**
- Provide your **activation code**: **[each person has a different activation code]**

Lonza

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **April 30, 2018.** Be prepared to provide engagement number **DB05001** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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 to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 201-683-2919 or via email at lorraine.mercede@lonza.com

Sincerely,

Lorraine S. Mercede

cc: HRBP at Location

* Offline members will be eligible to call for additional reports quarterly after enrolling
** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not

Lonza

include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.