Linda K. Gardner
Sr Attorney & Chief Privacy Officer
600 New Century Parkway
New Century, KS 66031
linda.gardner@centurylink.com

February 24, 2017

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

I am writing to inform you of a recent incident involving the potential breach of personal information of two (2) New Hampshire residents. Pursuant to N.H. Rev. Stat. Ann. § 359-C:20 et seq., the attached is a sample copy of the letter to be mailed on February 27, 2017 to those involved.

As the attached letter describes, on February 1, 2017, CenturyLink's Corporate Security detected and began an investigation into a potentially compromised email account that was being used to generate SPAM. As part of the investigation, we determined that the compromise could have occurred as early as January 30, 2017 when an employee provided account credentials in response to a phishing attack. While there is no indication that the phishing attack was designed for anything other than to compromise an email account in order to send SPAM, the method used may have allowed remote access to the employee's emails which included sensitive personally identifiable information, such as name, address, SSN, and date of birth. No credit card or banking information was involved.

Within a short time of the security alert, the SPAM was stopped and several actions were taken to prevent any further potential unauthorized access. We are also providing additional training to those involved and examining procedures to minimize the risk of reoccurrence.

Although there is no evidence of misuse of the information or that the compromising activity was designed for the purpose of capturing such information, we have arranged for a complimentary one-year membership in a credit monitoring service for all involved. The details regarding that service and how to enroll, as well as information on other resources concerning identity theft and fraud are included with the letter. In addition, we have notified the major credit reporting agencies.

Please do not hesitate to contact me if there are any questions.

Sincerely,

Linda Gardner

Linda K. Gardner
Sr Attorney & Chief Privacy Officer
600 New Century Parkway
New Century, KS 66031
linda.gardner@centurylink.com

February XX, 2017

Name
Address
City, State, Zip

NOTICE OF BREACH

Dear <Employee Name>,

The security and privacy of your personal information is of utmost importance to CenturyLink and we take significant measures to protect it. Unfortunately, we recently discovered that an employee's email account was compromised which may have inadvertently exposed some of your personal information. It is important to note that there is no evidence of misuse of the information or that the compromising activity was designed for the purpose of capturing such information. Nonetheless, it is important to notify you of this incident so that you are aware of the situation and can monitor your accounts.

WHAT HAPPENED?

On February 1, 2017, Corporate Security detected and began an investigation into a potentially compromised email account that was being used to generate SPAM. As part of the investigation, we determined that the compromise could have occurred as early as January 30, 2017 when an employee provided account credentials in response to a phishing attack. While there is no indication that the phishing attack was designed for anything other than to compromise an email account in order to send SPAM, the method used may have allowed remote access to the employee's emails which included sensitive personally identifiable information.

WHAT INFORMATION WAS INVOLVED?

The information potentially exposed varied by individual but could have included, among other things:

- Your name and address
- Your Social Security Number
- Your date of birth

The information did *not* include credit card or other banking information.

WHAT WE ARE DOING:

Within a short time of the security alert, the SPAM was stopped and several actions were taken to prevent any further potential unauthorized access. We are also providing additional training and examining procedures to minimize the risk of reoccurrence.

While we do not have any evidence that your sensitive, personal information has been misused, we do want you to be aware of the situation so you can monitor your accounts.

To support you, we are offering a complimentary one-year membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. For additional details about ProtectMyID, please see the last page of this letter. ProtectMyID is completely free to you and enrolling will not hurt your credit score. A credit card is not required to enroll.

Activate ProtectMyID Now in Three Easy Steps:

1. ENSURE That You **Enroll By: May 31, 2017** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll:** www.protectmyid.com/redeem
3. PROVIDE **Your Activation Code:** <insert code>

If you have questions or need an alternative to enrolling online, please call **877-288-8057** and provide engagement **#PC[redacted]**.

WHAT YOU CAN DO:

It is important for you to remain vigilant for incidents of fraud and identity theft by reviewing your credit card account statements and monitoring your credit report for unauthorized account activity. If you suspect identity theft, you are advised to report it to local law enforcement, to the Attorney General, and/or to the Federal Trade Commission.

You may obtain a free copy of your credit report once every 12 months. To order, go to www.annualcreditreport.com, or call toll-free 1-877-322-8228, or you may complete the Annual Credit Report Request Form available on the website noted and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

You may also purchase a copy of your credit report by contacting any of the three national credit reporting agencies listed below. They can also provide you with information about fraud alerts and security/credit freezes. Credit freeze procedures and costs vary from state to state. For more information, see the last page of this letter or you may also contact the following:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 4500	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-493-2392
www.equifax.com	www.experian.com	www.transunion.com

For further information about steps you can take to avoid identity theft, including more on fraud alerts or security freezes and what those options provide, please contact:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

We understand this incident may be concerning to you, as it is to us. We sincerely apologize for any inconvenience this may cause and we encourage you to take advantage of the services we have arranged for you. I would like to reiterate that CenturyLink takes the security of your information seriously and we are working on ways to further secure your information in light of this incident.

If you have any questions or concerns about this notification, please do not hesitate to contact us at notification.inquiries@centurylink.com or by contacting Philip [redacted] at [redacted].

Sincerely,

Linda Gardner

ADDITIONAL DETAILS REGARDING YOUR COMPLIMENTARY ONE YEAR PROTECTMYID MEMBERSHIP:

Once your ProtectMyID membership is activated, you will receive the following:

- **Free copy of your Experian credit report.**
- **Surveillance Alerts for Daily Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCare:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
    - It is recognized that identify theft can happen long after a data breach. To offer added protection, you will receive ExtendCare™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

*** 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 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.**

INFORMATION REGARDING FRAUD ALERTS:

An initial 90 day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should be denied. Contact a credit reporting company listed above for assistance in setting up an alert.

INFORMATION REGARDING SECURITY FREEZES:

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with new credit applications, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies listed in the letter above.

TOOLS FROM CREDIT PROVIDERS:

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.