<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

As you may know, Capitol Administrators Inc. ("Capitol") processes the claims under the <<ClientDef1 (Lucent Client)>> Group Health Plan (the Plan) and understands the importance of protecting the information it maintains. Capitol is a third party administrator hired by companies to provide benefits administration. To accomplish this function, our clients, medical providers and others provide us with data about Plan participants, including certain types of personal and medical information. Regrettably, this letter is to inform you of a recent incident that may have involved your personal information, which was provided to Capitol in connection with processing claims and related services for the Plan. This notice describes the incident, outlines the measures we have taken in response, and advises you on steps you can take to further protect your information.

What Happened

On March 30, Capitol learned through a forensic investigation of a phishing email incident that certain emails and attachments had been accessed by an unauthorized person. Upon first learning of the phishing incident, Capitol took immediate steps to secure the account, conduct an internal investigation, and enhance the security of its system. Capitol also engaged a leading cyber security firm to perform an investigation. That investigation determined that an unauthorized individual accessed certain emails and attachments in a small number of Capitol employees' email accounts.

What Information Was Involved

The emails and attachments contained your name and personal data, including <<ClientDef2 (variable elements.)>> While the investigation could not determine if the attachments to the emails had been opened by the unauthorized person that possibility could not be ruled out.

What We Are Doing

In addition to providing you notice of the incident, Capitol has taken various steps to enhance its existing network and email security, including implementing multi-factor authentication and upgrading its security center, as well as providing education and training to its employees to help prevent a similar incident from happening in the future.

What You Can Do

We encourage you to remain vigilant by reviewing your account statements for any unauthorized activity. You should also review the additional information on the following pages on ways to protect yourself. We have arranged for Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention and Kroll Identity Monitoring, please see the page that follows this letter.

Visit **kroll.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **August 9, 2018** to activate your identity monitoring services.*

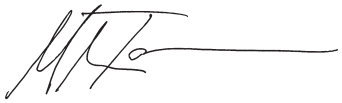
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-833-219-9090. Additional information describing your services is included with this letter.

For More Information

Capitol regrets that this incident occurred. If you have questions about this matter or the recommended next steps, please call 1-833-219-9090, Monday through Friday between 6 a.m. – 3 p.m., Pacific Time.

Sincerely,



Michael Tate
General Manager and Sr. Vice President
Capitol Administrators, Inc.

CC: Group Health Plan

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

Even if you choose not to take advantage of this complimentary credit monitoring service, we remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft, as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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