BenefitMall

January 3, 2019

Via: Certified Mail

Office of the Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: ***Notice of Data Breach***

Dear Sir or Madam:

We are writing to inform you that Centerstone Insurance and Financial Services, d/b/a BenefitMall (the "Company") was the target of a data security incident that may have exposed certain personal information of 45 New Hampshire residents.

On October 11, 2018, the Company discovered it was the target of an email phishing scam in which unknown actors were able to obtain and use the email login credentials for some of the Company's employees. The dates of potential unauthorized access to Company email accounts vary, but generally occurred between June 2018 and the discovery date. At this point, we are not aware of any fraud or misuse of any personal information as a result of this incident.

Emails in the affected mailboxes may have included names, addresses, social security numbers, dates of birth, bank account numbers, and information relating to payment of insurance premiums.

The Company retained a leading cybersecurity forensics firm to help conduct a thorough investigation of the incident. The investigation allowed the Company to identify the cause of the incident and contain it. To help prevent a similar type of incident from occurring in the future, the Company implemented additional security measures designed to protect employee email accounts and insured information, including two-factor authentication for access to the Company's email system. It has also undertaken a further employee education initiative to inform employees about phishing scams and how to guard against them and will continue to deliver additional employee training about email safety and recognizing phishing emails. We have also reported the incident to law enforcement and will continue to cooperate with any investigation.

We will notify affected New Hampshire residents by mail on January 4, 2019 and will be offering them 24 months of complimentary credit monitoring and fraud protection services. A copy of the notice letter is attached.

If you have any questions or need further information regarding this incident, please contact our legal counsel, David Kessler, Partner, Norton Rose Fulbright US LLP, at 212-318-3382.

Sincerely,

Stephanie Bowman

Chief Financial Officer

BenefitMall

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
R836504

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

January 4, 2019

Dear John Sample,

Notice of Data Breach

We are writing to inform you of a data security incident that may have exposed some of your personal information. Based on our current review, we have no indication that any information has been used inappropriately. However, out of an abundance of caution, we wanted to provide information on the incident and provide recommendations on steps you can take to help protect your information.

What Happened

On October 11, 2018, we became aware that Centerstone Insurance and Financial Services, d/b/a BenefitMall, (the "Company") was the target of an email phishing attack that exposed employee email login credentials. Our investigation revealed that unauthorized access to the compromised employee mailboxes may have exposed some of your personal information. While the dates of the unauthorized access vary, the issue generally occurred between June 2018 and the discovery date.

Who Is BenefitMall

We are a company that helps employers deliver workplace solutions such as administering payroll and employee benefits. Given the nature of this work, we would have access to your personal information because of services we provide to your employer and/or health plan.

What Information Was Involved

Emails in the affected mailboxes may have included your name, address, Social Security number, date of birth, bank account number, and information relating to payment of your insurance premiums.

What We Are Doing

We take the privacy and security of your personal information very seriously. Once we learned of this incident, we immediately initiated an internal review. We also retained a top computer forensics firm to help us conduct a thorough investigation of the incident and remediate our systems. We have reported the incident to law enforcement and will continue to work closely with them during their review.

To help prevent a similar type of incident from occurring in the future, we have implemented additional security measures designed to protect employee email accounts and your information, including two-factor authentication for access to our email system. We have also undertaken an employee education initiative to inform employees about phishing scams and how to guard against them and will continue to deliver additional employee training about email safety and recognizing phishing emails. We will continue to cooperate with your insurance provider and state regulators as appropriate.

What You Can Do

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-861-4016 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-861-4016 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Review of Financial Accounts and Credit Reports. You should carefully review your account statements and credit reports for suspicious activity, accounts you did not open, or inquiries from creditors you did not initiate. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand on your credit report, call the credit agency immediately. If you find any suspicious activity on your statements or credit reports, call your local police or sheriff's office, file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.

Information About Identity Theft Protection Guide. Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

For More Information

We sincerely apologize that this incident occurred and for any concern it may cause you. For more information, or if you have questions or need additional information, please contact AllClear ID at 1-855-861-4016, Monday through Saturday, 8:00 a.m. – 8:00 p.m. Central Time, or write to me at 12404 Park Central Drive, Suite 400s, Dallas, Texas 75251.

Sincerely,

Robert C. Love
President, Benefits Division

ATENCIÓN: Este documento incluye una notificación de importancia. Si no puede leer el mensaje adjunto, ofrecemos servicios de asistencia en otros idiomas sin costo para usted. Por favor, llame al 1-855-861-4016 para obtener ayuda con la traducción.

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
1-800-685-111 P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	1-888-397-3742 P.O. Box 4500, Allen, TX 75013 www.experian.com	1-800-916-8800 P.O. Box 2000 Chester, PA 19016 www.transunion.com

The following information reflects recommendations from the Federal Trade Commission regarding identity theft protection.

Free Credit Report. We remind you to be 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. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348-5281.

> **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont Residents:** You may obtain one or more additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Medical Privacy. We recommend that you regularly review the explanation of benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

> **For California residents:** We also suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alert. You may place a fraud alert on your file by calling one of the three nationwide credit reporting agencies above. 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. Pursuant to the Economic Growth, Regulatory Relief, and Consumer Protection Act, you may place a fraud alert on your file free of charge.

> **For Colorado and Illinois residents:** You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Security Freeze. You have the ability to place a security freeze on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above.

The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.