[redacted]

From: Lawson, Catherine R. L. <catherinelawson@parkerpoe.com>
Sent: Thursday, December 19, 2019 2:34 PM
To: DOJ: Consumer Protection Bureau
Cc: Hutchins, Sarah Fulton
Subject: Data breach notification
Attachments: Zenith Ad r1prf.pdf

To whom it may concern:

My firm serves as counsel to Zenith Global Logistics, a North Carolina based company that provides freight, warehousing, and trucking services in the home furnishings industry. On October 24, 2019, Zenith became aware that an employee's email account was compromised around October 16, 2019, also compromising a second employee's email account. Those accounts were secured on October 24, 2019. A secondary vulnerability related to one of the previously identified accounts was discovered on November 18, 2019, and resolved the same day.

Zenith engaged outside parties to prevent further incidents and review the scope of any unauthorized access. Zenith hired Parker Poe, a law firm with which it works, and Elliot Davis, a cybersecurity consulting firm, to oversee an investigation into how the potential breach occurred, what was its scope, who was affected, and to assist with forensic analysis of the impacted environment and other assets.

Zenith has identified 1,483 affected individuals, including 1 resident of New Hampshire. The information that may have been exposed by the breach includes certain employees' or benefit recipients' names and social security numbers. For certain individuals, bank account numbers, passport numbers, tax ID numbers, or drivers' license numbers may also have been exposed.

Zenith has engaged Kroll, a leading global provider of risk solutions, to support Zenith in providing notification and comprehensive identity monitoring services to the affected individuals, along with call center support to affected individuals. Zenith will also be introducing additional cybersecurity measures, such as requiring two-factor authentication for Office 365 accounts, more widespread use of encryption, increased personnel training on cybersecurity best practices, and other more powerful security measures.

Notification letters are being sent to the affected individuals starting on December 19, 2019. A copy of the notification letter is attached to this email. Zenith is committed to assisting affected individuals to mitigate any potential harm associated with this incident. If there are any follow up questions or concerns, you can reach out to Sarah Hutchins through email, sarahhutchins@parkerpoe.com, or phone, 704.335.6639.

Sincerely,
Catherine Lawson

Catherine Lawson
Associate

Parker Poe

PNC Plaza | 301 Fayetteville Street | Suite 1400 | Raleigh, NC 27601
Office: 919.835.4640 | Fax: 919.834.4564 | vcard | map

Visit our website at
www.parkerpoe.com

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Zenith Global Logistics is writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

We are investigating a suspected data breach. On Thursday, October 24, 2019, we first discovered that an employee's Office 365 account appeared to have been infiltrated by an unknown actor. We later discovered suspected access to a second employee's account. We secured vendors to help us close off the improper access and assess the impact of any potential data breach. While we are still investigating, it is possible that over 1,500 individuals may have been affected by the incident, which includes current employees and former employees. Based on the information regularly collected by our Human Resources Department, we do not believe that employees' dependent personal information is at risk, however, if you believe that you have emailed such information to us, such as for purposes of benefit enrollment, please contact us right away using the contact information in this notice.

What information was involved?

While we are still reviewing potentially impacted information, the information that may have been exposed includes certain employees' names and Social Security numbers, and for certain individuals, bank account numbers, passport numbers, tax ID numbers, and/or drivers' license numbers may also have been exposed.

What we are doing.

After we discovered the incident, we engaged in internal measures to cut off the infiltration and we contacted a cybersecurity consulting firm, Elliott Davis, to oversee an investigation into how the potential breach occurred, what was its scope, and who was affected. Elliott Davis is a consulting firm that has the capabilities to assist with forensic analysis of the impacted environment as well as assist our team with the investigation of other assets to make sure they were not impacted. Along with contacting Elliott Davis, we engaged Parker Poe, which is a law firm we work with.

We believe we have cut off the threat to the infected account. To mitigate the risk of future cyber incidents, we plan to introduce other protective measures, such as requiring two-factor authentication for Office 365 accounts, more widespread use of encryption, increased personnel training on cybersecurity best practices, and other more powerful security measures.

To help relieve concerns and restore confidence following this incident, we have secured the services of 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, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

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

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Jack Hawn
President & CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

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, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) 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).

Fraud Alert. You may place a fraud alert in 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

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 credit report 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.

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, DC 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.

Reporting of identity theft and obtaining 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.

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

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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 Chrome, Firefox, Safari and Edge.
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.