Appendix

PASCO recently completed an investigation that involved a ransomware infection that affected its network. Upon detecting the unauthorized access to the network on August 24, 2020, PASCO took steps to secure the network and began an investigation with the assistance of a cybersecurity firm. PASCO also notified law enforcement and worked to support the investigation.

The investigation determined that the unauthorized person accessed PASCO's network on August 24, 2020 and accessed certain files and folders that contained personal information of some current and former employees and affiliates. PASCO conducted a thorough review of the data contained in those files and folders to identify potentially affected individuals. On October 7, 2020, PASCO identified information pertaining to one Maine resident, including her name and Social Security number.

Beginning on January 7, 2021, PASCO is mailing a notification letter via United States Postal Service First Class Mail to these residents in accordance with Me. Rev. Stat. Tit. 10, §1348.[1] PASCO is offering a one-year membership in complimentary credit monitoring and identity theft protection services through Kroll. PASCO is also providing a toll-free number that individuals can call with questions about the incident or enrolling in credit monitoring.

To reduce the risk of a similar incident occurring in the future, PASCO is implementing additional measures to enhance existing security protocols.

[1] This report does not waive PASCO's objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.

PASCO

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

PASCO scientific understands the importance of protecting our employees' personal information. We are writing to inform you of a recent security incident that may have involved some of your information. This notice explains the incident, measures we have taken and some steps you can take in response.

On August 24, 2020, we detected malicious software code that was introduced into our computer network. Upon discovery, we immediately took steps to secure our systems, remove the malware, and conduct an investigation to determine how this happened and what information may have been involved. Our investigation determined that the malware allowed remote access to computer systems where some confidential information was stored, including your name, Social Security number and driver's license number or other government identification number.

We have no evidence that any of your personal information was stolen, targeted, or compromised by this incident. Nevertheless, as a precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll provides risk mitigation and response, and their team has 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.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **March 28, 2021** to activate your identity monitoring services.*

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

We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. For more information on Kroll's services, as well as some additional steps you can take to help protect yourself, please see the additional information provided with this letter.

We sincerely regret any concern or inconvenience caused by this incident. In response to the incident, and to help prevent a reoccurrence of a similar incident, we have installed on all computers software designed to monitor and isolate this type of malware, implemented a more stringent password policy, closed potential vulnerabilities in our network firewall, and store sensitive data on portable drives not directly connected to the company network. If you have any questions, please call 1-833-971-3334 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Sincerely,

Richard Briscoe
President
10101 Foothills Blvd,
Roseville, CA 95747
1-916-786-3800

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

1. 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

2. 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.

3. 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable 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. Contact information for the three nationwide credit reporting companies is as follows:

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

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov