PCS REVENUE CONTROL SYSTEMS

560 Sylvan Avenue
Englewood Cliffs, NJ 07632
800-247-3061
www.pcsrcs.com

Office of the Attorney General
Attn: Security Breach Notification
1125 Washington St. SE
Olympia, WA 98504
SecurityBreach@atg.wa.gov

March 17, 2021

To Whom It May Concern:

We are writing to advise of an incident involving potential exposure of personal information which involved Washington residents. Below, we outline the details of the data security incident, and steps PCS Revenue Control Systems ("PCS") has taken since discovering the incident.

On December 20, 2019, PCS (a provider of food, nutrition and other technology products and services serving educational institutions throughout the United States) identified a potential threat for unauthorized access to some of its data. Third-party forensics experts were engaged to investigate the situation. After a complex and exhaustive investigation, it was determined that there was unauthorized access to a server that belonged to an entity acquired by PCS. This server included files and records related to certain school lunch and meal programs. The impacted server was immediately taken offline. As part of this investigation, PCS also became aware that an email account on its network had been improperly accessed. PCS immediately acted to secure its network.

Working with third-party experts, PCS conducted a thorough review of its systems and processes. Based on this review, PCS acted to further strengthen existing security systems and processes to help prevent a similar situation from occurring in the future. PCS mitigation activities include (1) conducting vulnerability scans, (2) patching systems, (3) resetting passwords, (4) reviewing access privileges, and (5) employee training.

On March 16, 2021, it was determined that 11,807 Washington residents were potentially impacted by this incident. Results from the investigation show that improperly accessed data primarily included names and student identification numbers for the vast majority of affected individuals whose data was on this server. In a sub-set of cases, Social Security numbers and/or dates of birth may have been accessible. We have seen no evidence to date that any personal information has been used for malicious purposes.

PCS is notifying impacted individuals of these events even though, again, there has been no evidence to date that any personal information has been used for malicious purposes. PCS is also offering 12 months of complimentary credit monitoring and identity theft protection

services to impacted Washington individuals in an abundance of caution. Notifications to the potentially impacted Washington residents will be mailed over the dates of March 17 – March 23, 2021.

PCS is cooperating with law enforcement regarding their investigations and is complying with all relevant reporting and notification obligations. In addition to providing complimentary identity theft protection and credit monitoring services to all possibly affected Washington residents, PCS has established a dedicated member support hotline to help address any further questions about the incident.

Please do not hesitate to contact us with any questions or comments.

MENDES & MOUNT, LLP (on behalf of PCS Revenue Control Systems)

Margaret A. Reetz
Margaret.Reetz@mendes.com
212-261-8726

Gregory Mantych
Gregory.Mantych@mendes.com
212-261-8091

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

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

Notice of Data Breach

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

We are writing to advise you of an incident involving potential exposure of your personal information. PCS Revenue Control Systems, Inc. ("PCS") is a provider of food, nutrition and other technology products and services serving K-12 educational institutions throughout the United States.

Below are details regarding the incident, steps PCS has taken since discovering the incident, and guidance for protecting your personal information going forward.

What Happened

On December 19, 2019, PCS identified unauthorized access to a server that belonged to an entity called Advanced Business Technologies ("ABT"), which was acquired by PCS in 2016. This server included files and records related to certain school lunch and meal programs.

PCS immediately acted to secure its network, and third-party forensics experts were engaged to investigate the situation. We have seen no evidence to date that any personal information has been used for malicious purposes. However, in an abundance of caution, we are providing notice to individuals identified as potentially affected.

What Information Was Involved

The information included names plus school student identification numbers, while some of the relevant data may have also included Social Security numbers and/or dates of birth.

What We Are Doing

Working with third-party experts, we conducted a thorough review of PCS systems and processes. Based on this review, we have acted to further strengthen existing security systems and processes to help prevent a similar situation from occurring in the future.

To help relieve any concerns 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, Fraud Consultation, and Identity Theft Restoration.

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

*You have until **June 15, 2021** to activate your identity monitoring services.*

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

Additional information describing your services is included with this letter.

Please note that PCS no longer accepts Social Security numbers as part of its administration of programs on behalf of its institutional customers.

What You Can Do

In addition to activating the services described above, please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to help protect your information.

For More Information

We regret any inconvenience or concern created by this matter. If you have any questions, please call 1-855-761-1064, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Sincerely,

Customer Relations
PCS Revenue Control Systems

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

Fraud Alert

You may consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. There shall be no charge for a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above. The contact information for the Federal Trade Commission is as follows:

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

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 New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

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.

Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

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:

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 will be able to help you determine if it is 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 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.