Exhibit 1

**THE UNITED STATES DISTRICY COURT**
**FOR THE DISTRICT OF NEW JERSEY**

| | |
|---|---|
| CARLOS GAMEZ<br><br>and<br><br>ROBERTO QUINONEZ, as parent and general guardian of C.L.Q-B, a minor,<br><br>on behalf of themselves and all others similarly situated,<br><br>Plaintiffs,<br><br>vs.<br><br>PCS REVENUE CONTROL SYSTEMS, INC.,<br><br>a New Jersey corporation,<br><br>Defendant. | Case No.:<br><br>**CLASS ACTION COMPLAINT**<br><br>DEMAND FOR JURY TRIAL |

Plaintiffs Carlos Gamez and Roberto Quinonez, as parent and general guardian of C.L.Q-B, a minor (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Class Action Complaint against PCS Revenue Control Systems, Inc. ("PCS" or "Defendant"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

## I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information about more than 800,000 current and former K-12 students whose schools (the "Schools") entrusted their information to "Advanced Business Technologies" ("ABT") to obtain its food and nutrition technology. Defendant subsequently acquired ABT, thereby gaining possession, custody, and control of the students' information, including, without limitation, their names, student identification numbers, dates of birth, and/or

Social Security numbers (collectively, "personal identifiable information" or "PII"). Defendant then allowed the information to remain accessible from the internet for more than three years, notwithstanding that Defendant never had a relationship with some of the Schools and many of Plaintiffs and Class Members no longer attended the Schools.

2. Prior to its acquisition by Defendant, ABT provided food and nutrition technology to schools throughout the United States. In order to obtain this technology, the Schools entrusted and provided ABT with an extensive amount of PII for K-12 students.

3. In 2016, Defendant acquired ABT, thereby gaining possession, custody, and control of a computer server (the "Server") that included the PII of more than 800,000 K-12 students who attended the Schools, including schools in Pelham, Alabama; Alachua County, Florida; Polk County, Florida; DeKalb County, Georgia; and the Austin (Texas) Independent School District.

4. For approximately three years after Defendant took possession, custody, and control of the Server, the PII of K-12 students remained on the Server, which was accessible from the internet, notwithstanding that (a) some of the Schools never had a relationship with PCS and ended their relationships with ABT in or before 2016 and (b) some of the K-12 students had stopped attending the Schools, including those students who had changed schools or graduated.

5. On or around December 19, 2019, Defendant determined that an unauthorized actor obtained access to the Server, and the students' PII thereon, via the internet (the "Data Breach").

6. At the time it learned of the Data Breach, Defendant knew or should have known that the Server contained the PII of more than 800,000 current or former K-12 students, including Plaintiffs and Class Members.

7. Nonetheless, Defendant waited **more than a year** to notify the affected current or former K-12 students, or their parents or guardians, of the Data Breach.

8. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals. Defendant admits that the unencrypted PII exposed to "unauthorized activity" included names, student identification numbers, dates of birth, and/or Social Security numbers.

9. The exposed PII of the current or former K-12 students can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

10. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of the students.

11. Until notified of the breach, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

12. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII, and at the very least , are entitled to nominal damages.

14. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the students' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## II. PARTIES

15. Plaintiff Carlos Gamez is a citizen of Florida residing in Polk County, Florida. Mr. Gamez received Defendant's letter notifying him of the Data Breach, dated March 11, 2021, on or about that date.[1] Mr. Gamez's parents received Defendant's letter notifying them of the Data Breach, dated March 12, 2021, on or about that date.[2]

16. Plaintiff Roberto Quinonez is the parent and general guardian of C.L.Q-B, who

[1] Ex. 1.
[2] Ex. 2.

resides in Alachua County, Florida. Mr. Quinonez received Defendant's letter notifying him of the Data Breach, dated March 12, 2021, on or about that date.[3]

17. Defendant PCS Revenue Control Systems, Inc. is a corporation organized under the laws of New Jersey, headquartered at 560 Sylvan Avenue, Englewood Cliffs, New Jersey, with its principal place of business in Englewood Cliffs, New Jersey.

18. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

19. All of Plaintiffs' claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

20. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

21. The District of New Jersey has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conduct substantial business in New Jersey and this District through its headquarters, offices, parents, and affiliates.

[3] Ex. 3.

22. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

## IV. FACTUAL ALLEGATIONS

***Background***

23. According to its website, Defendant is "[a] nationwide provider of school food and nutrition technology providing products."

24. In 2016, Defendant acquired ABT.

25. Prior to Defendant's acquisition of ABT, schools were required to provide ABT some of the most sensitive and confidential information of Plaintiffs and Class Members, including names, student identification numbers, dates of birth, and Social Security numbers. This information is static, does not change, and can be used to commit myriad financial crimes.

26. Plaintiffs and Class Members relied on ABT, and Defendant once it acquired ABT, to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

27. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

***The Data Breach***

28. Beginning on or about March 11, 2021, Defendant sent Plaintiffs and Class Members, and/or their parents and guardians, letters notifying them of the Data Breach.[4] Defendant informed the recipients of the notice that:

> We are writing to advise you of an incident involving potential

[4] Ex. 4 (sample *Notice of Data Breach* filed with California Attorney General).

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.[5]

[5] Ex. 4, p. 1.

29. Defendant admitted that unauthorized third persons accessed files that contained sensitive information about Plaintiffs and Class Members, including names, student identification numbers, dates of birth, and Social Security numbers.

30. Defendant admitted that it knew about the Data Breach for more than a year before it notified Plaintiffs and Class Members of the Data Breach.

31. In response to the Data Breach, Defendant claims that it "immediately acted to secure its network, and third-party forensics experts were engaged to investigate the situation"[6]

32. Plaintiffs' and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

33. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing their PII to be exposed.

***Defendant Acquires, Collects and Stores the PII of Plaintiffs and Class Members.***

34. ABT acquired, collected, and stored the PII of Plaintiffs and Class Members.

35. Defendant gained possession, custody, and control of the PII of Plaintiffs and Class Members through the acquisition of ABT, which required that schools entrust the highly confidential PII to ABT.

36. By acquiring, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII of Plaintiffs and Class Members from disclosure.

[6] Ex. 4, p. 1.

37. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***Securing PII and Preventing Breaches***

38. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiffs and Class Members, or Defendant could have destroyed the data, especially old data that Defendant had no legal right to retain.

39. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

40. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

41. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[8]

42. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security

[7] 17 C.F.R. § 248.201 (2013).
[8] *Id.*

numbers, fraudulent use of that information and damage to victims may continue for years.

***Value of Personal Identifiable Information and Protected Health Information***

43. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

44. Social Security numbers, for example, are among the mot sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

---

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2021).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2021).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Jan. 26, 2021).

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2021).

45. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

46. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

47. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, address, date of birth, and Social Security number.

48. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[14]

49. Among other forms of fraud, identity thieves may obtain driver's licenses,

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 26, 2021).

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2021).

government benefits, medical services, and housing or even give false information to police.

50. The PII of Plaintiffs and Class Members was taken by hackers to engage in identity theft or and or to sell it to others criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

51. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

52. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

53. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

54. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially hundreds of thousands of individuals' detailed, personal information and thus, the significant number of

[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Apr. 1, 2021).

individuals who would be harmed by the exposure of the unencrypted data.

55. To date, Defendant has offered Plaintiffs and Class Members only one year of identity monitoring services through a single provider, Kroll. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

56. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

***Plaintiff Carlos Gamez's Experience***

57. In and before 2016, Plaintiff Carlos Gamez, then a minor, attended one or more of the Schools in Polk County, Florida. As a condition for attending school, he was required to provide and entrust his PII to the school, including, but not limited to, his name, student identification number, date of birth, and Social Security number.

58. Mr. Gamez received Defendant's letter notifying him of the Data Breach, dated March 11, 2021, on or about that date.[16]

59. Mr. Gamez's parents received Defendant's letter notifying them of the Data Breach, dated March 12, 2021, on or about that date.[17]

60. As a result of the letters notifying him and his parents of the Data Breach, Mr. Gamez spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the letter, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Defendant, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

[16] Ex. 1.
[17] Ex. 2.

61. Additionally, Mr. Gamez is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

62. Mr. Gamez stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

63. Mr. Gamez suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Gamez entrusted to Defendant, which was compromised in and as a result of the Data Breach.

64. Mr. Gamez suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

65. Mr. Gamez has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name and date of birth, being placed in the hands of unauthorized third-parties and possibly criminals.

66. Mr. Gamez has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

***C.L.Q-B's Experience***

67. In and before 2016, C.L.Q-B, then and now a minor, attended one or more of the Schools in Alachua County, Florida. As a condition for obtaining food and nutrition from his school, he was required to provide and entrust his PII to the school, including, but not limited to, his name, student identification number, date of birth, and Social Security number.

68. C.L.Q-B's parent, Plaintiff Roberto Quinonez, received Defendant's letter

notifying him of the Data Breach, dated March 12, 2021, on or about that date.[18]

69. As a result of the letter notifying him of the Data Breach, Mr. Quinonez, on behalf of C.L.Q-B, spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the letter, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Defendant, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

70. Additionally, Mr. Quinonez, on behalf of C.L.Q-B, is very careful about sharing C.L.Q-B's PII. He has never knowingly transmitted C.L.Q-B's unencrypted PII over the internet or any other unsecured source.

71. Mr. Quinonez, on behalf of C.L.Q-B, stores any documents containing C.L.Q-B's PII in a safe and secure location or destroys the documents.

72. C.L.Q-B suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that C.L.Q-B entrusted to Defendant, which was compromised in and as a result of the Data Breach.

73. Mr. Quinonez, on behalf of C.L.Q-B, suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of C.L.Q-B's privacy.

74. C.L.Q-B has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name and date of birth, being placed in the hands of unauthorized third-parties and possibly criminals.

75. C.L.Q-B has a continuing interest in ensuring that his PII, which, upon information

[18] Ex. 3.

and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

## V. CLASS ALLEGATIONS

76. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

77. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All United States residents whose PII was compromised in the data breach refenced in Defendant's letter to Plaintiff Carlos Gamez dated March 11, 2021 (the "Nationwide Class").

78. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate statewide subclass, defined as follows:

> All Florida residents whose PII was compromised in the data breach refenced in Defendant's letter to Plaintiff Carlos Gamez dated March 11, 2021 (the "Florida Class").

79. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

80. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

81. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of current or former K-12 students whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised Maine Attorney General Frey that the Data Breach affected 867,209 individuals.

82. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in

the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

83. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

84. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

85. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that

would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

86. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

87. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause

of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

88. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

89. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

90. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

91. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

92. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to

exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

**COUNT I**
**Negligence**
**(On Behalf of Plaintiffs and the Nationwide Class)**

93. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

94. Plaintiffs and the Nationwide Class, as current and former K-12 students, entrusted their PII, including their names, student identification numbers, dates of birth, and Social Security numbers, to their schools, which in turn entrusted this PII to ABT, which Defendant later acquired,

thereby gaining possession, custody, and control of this PII.

95. Plaintiffs and the Nationwide Class understood that Defendant would safeguard their PII, use their PII for business purposes only, not disclose their PII to unauthorized third parties, and promptly and properly dispose of their PII in the absence of any need or legal obligation to retain it.

96. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

97. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

98. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

99. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain pursuant to regulations.

100. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

101. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special

relationship arose because Plaintiffs and the Nationwide Class entrusted Defendant with their confidential PII.

102. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

103. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

104. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

105. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

106. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

107. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

108. Defendant had and continues to have a duty to adequately disclose that the PII of

Plaintiffs and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

109. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

110. Defendant has admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

111. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendant's possession or control.

112. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII.

115. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII it was no longer required to retain pursuant to regulations.

116. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

117. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

118. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

119. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

120. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Nationwide Class.

121. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

122. Plaintiffs and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

123. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Nationwide Class.

124. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

125. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury

and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

126. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

**COUNT II**
**Violation of the Florida Deceptive and Unfair Trade Practices Act,**
**(Fla. Stat. §§ 501.201, *et seq.*)**
**(On Behalf of Plaintiffs and the Florida Class)**

127. Plaintiffs and the Florida Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

128. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained the PII of Plaintiffs and the Florida Class through its acquisition of ABT, which in turn obtained the PII through advertising, soliciting, providing, offering, and/or distributing goods and services to schools that served Plaintiffs and the Florida Class and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

129. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard PII;

b. failure to make only authorized disclosures of the PII of Plaintiffs and the Florida Class;

c. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft; and

d. failure to timely and accurately disclose the Data Breach to Plaintiffs and the Florida Class.

130. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Plaintiffs and the Florida Class.

131. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Plaintiffs and the Florida Class that it did not follow industry best practices for the collection, use, and storage of PII.

132. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Florida Class have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

133. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs and the Florida Class have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

134. Also as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and the Florida Class are entitled to damages as well as injunctive relief, including, but not limited to:

e. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

f. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

g. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

h. Ordering that Defendant segment PII by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

i. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner PII not necessary for its provisions of services;

j. Ordering that Defendant conduct regular database scanning and securing checks;

k. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

l. Ordering Defendant to meaningfully educate Plaintiffs and the Florida Class about the threats they face as a result of the loss of their PII to third parties, as well as the steps Plaintiffs and the Florida Class must take to protect themselves.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Florida Class and appointing Plaintiffs and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information

when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as

well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2

Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand that this matter be tried before a jury.

Date: April 12, 2021

Respectfully Submitted,

*/s/ James A. Barry*

JAMES A. BARRY
**LOCKS LAW FIRM, LLC**
801 N. Kings Highway
Cherry Hill, NJ 08034
(856)663-8200
jbarry@lockslaw.com

and

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN D. MAXEY
(*Pro Hac Vice application forthcoming*)
**MORGAN & MORGAN COMPLEX LITIGATION GROUP**
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

pcs
Revenue Control Systems

79 1 29082 **********AUTO**5-DIGIT 33809
CARLOS D GAMEZ
[redacted]

March 11, 2021

**Notice of Data Breach**

Dear Carlos D Gamez,

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 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.*

[redacted]

Additional information describing your services is included with this letter.

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

pcs
Revenue Control Systems

222 1 83203 ********** AUTO**5-DIGIT 33809
Parent or Guardian of
CARLOS GAMEZ
[redacted]

March 12, 2021

**Notice of Data Breach**

Dear Parent or Guardian of Carlos Gamez,

We are writing to advise you of an incident involving potential exposure of your minor child's 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 child's 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 concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration 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.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your Minor Identity Monitoring services.

*You have until **June 15, 2021** to activate your Minor Identity Monitoring services.*

[redacted]

Additional information describing your services is included with this letter. *If your child is no longer a minor, he/she may be eligible for Adult identity monitoring services instead. Please email pcsnotifications@kroll.com for more information before activating the Minor Identity Monitoring services offered in 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 child's information.

For More Information

We regret any inconvenience or concern created by this matter. If you have any questions, please call our dedicated call center 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

PCS
Revenue Control Systems

122 1 46212 **********AUTO**5-DIGIT 32607
Parent or Guardian of
C[redacted] L Q[redacted]-B[redacted]

March 12, 2021

**Notice of Data Breach**

Dear Parent or Guardian of [redacted]

We are writing to advise you of an incident involving potential exposure of your minor child's 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 child's 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 concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration 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.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your Minor Identity Monitoring services.

*You have until **June 15, 2021** to activate your Minor Identity Monitoring services.*

[redacted]

Additional information describing your services is included with this letter. *If your child is no longer a minor, he/she may be eligible for Adult identity monitoring services instead. Please email pcsnotifications@kroll.com for more information before activating the Minor Identity Monitoring services offered in 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 child's information.

For More Information

We regret any inconvenience or concern created by this matter. If you have any questions, please call our dedicated call center 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:

**Minor Identity Monitoring**

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

**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.

PCS Revenue Control Systems

<<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.