

**THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION**

DANIEL HAYES and KATRINA NASH,

on behalf of themselves and all others
similarly situated,

Plaintiffs,

v.

AUTOMATION PERSONNEL SERVICES,
INC.,
an Alabama corporation,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Daniel Hayes and Katrina Nash (“Plaintiffs”), individually and on behalf of all others similarly situated (“Class Members”), bring this Class Action Complaint against Automation Personnel Services, Inc. (“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 sensitive information of individuals who obtained temporary employment through Defendant (collectively, “Class Members”), including, without limitation, name, Social Security number, and financial account information (collectively, “personally identifiable information” or “PII”).

2. According to its website, Defendant “specializes in connecting highly qualified individuals with employers in a wide range of industries nationwide” and “has 36 branch offices

in 10 states.”¹

3. On or before November 17, 2020, Defendant “discovered suspicious activity impacting the operability of certain systems” (the “Data Breach”).²

4. At the time of the Data Breach, these “systems” stored the PII of more than 299,000 individuals that obtained temporary employment through Defendant.

5. On or around December 24, 2020, reports began surfacing on the Internet that an archive of 440 GB of data that belong to Defendant had been “leaked on a popular hacker platform” after Defendant refused to pay a ransom to cybercriminals and that “[s]ince the data was made freely available in the final week of November, it’s safe to assume that multiple users of the hacker forum where it was posted had access to the data.”³

6. On or around March 16, 2021, approximately four months after it learned of the Data Breach, Defendant began notifying various states Attorneys General of the Data Breach.

7. On or around March 17, 2021, approximately four months after it learned of the Data Breach, Defendant began notifying Plaintiffs and Class Members 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 to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII exposed to “unauthorized activity” included names, Social Security numbers, and financial account information.

¹ See <https://www.apstemps.com/about-us/> (last visited June 22, 2021); <https://www.apstemps.com/about-us/locations/> (last visited June 22, 2021).

² Ex. 1 (sample *Notice of Data Breach* filed with Maine Attorney General).

³ Cybernews - 440GB of data from US-based temporary staffing agency leaked on hacker forum), *available at* <https://cybernews.com/security/440gb-of-data-from-us-based-temporary-staffing-agency-leaked-on-hacker-forum/> (last visited June 22, 2021).

9. The exposed PII of Plaintiffs and Class Members 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 now 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 the PII of Plaintiffs and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited approximately four months to report it to the states' Attorneys General and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

11. As a result of this delayed response, 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 (iv) the continued and certainly 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.

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 PII of Plaintiffs and Class Members 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 a 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 Daniel Hayes ("Hayes") is a Citizen of Alabama residing in Bibb County, Alabama.

16. Plaintiff Katrina Nash ("Nash") is a Citizen of Mississippi residing in Leake County, Mississippi.

17. Defendant Automation Personnel Services, Inc. is a corporation organized under the laws of Alabama, headquartered at 3500 Colonnade Parkway, Birmingham, Alabama with its principal place of business in Birmingham, Alabama.

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 its 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 Northern District of Alabama 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 Alabama and this District through its headquarters, offices, parents, and affiliates.

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. Defendant provides temporary staffing solutions to employers in a variety of industries, including light industrial, technical, contact center, manufacturing, skilled labor, and

automotive.

24. Plaintiffs and Class Members entrusted Defendant with sensitive and confidential information, including name, Social Security number, and financial account information, which include information that is static, does not change, and can be used to commit myriad financial crimes.

25. Plaintiffs and Class Members, as individuals who obtained temporary employment through Defendant, relied on this sophisticated 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. Plaintiffs and Class Members demand security to safeguard their PII.

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

The Data Breach

27. On or about May 17, 2021, Defendant sent Plaintiffs and Class Members a *Notice of Data Breach*.⁴ Defendant informed Plaintiffs and Class Members as follows:

What Happened? On November 17, 2020, APS discovered suspicious activity impacting the operability of certain systems. We quickly launched an investigation to determine the nature and scope of this incident, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed by the unknown actor. We completed a thorough and lengthy review to determine whether sensitive information was present in the impacted files and folders. On February 3, 2021, it was confirmed that some of your personal information was present in the files and folders that may have been accessed. We then worked to locate address information for those whose personal information was accessible within the files and just completed that effort.

⁴ Ex. 1 (Sample *Notice of Data Breach* filed with Maine Attorney General).

What Information Was Involved? The investigation determined that the following types of your personal information were present in the potentially accessed files and folders at the time of the incident: <<b2b_text_1(Impacted Data)>>.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the potentially accessed files and folders to determine whether they contained protected information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.⁵

28. On or about March 16, 2021, Defendant notified various state Attorneys General of the Data Breach. Defendant also provided the Attorneys General with letters and/or “sample” notices of the Data Breach that reaffirm the information that could have been subjected to unauthorized access included name, Social Security number, and financial account information.⁶

29. Defendant admitted in the *Notice of Data Breach*, the letters to the Attorneys General, and the “sample” notices of the Data Breach that unauthorized third persons accessed files that contained sensitive information about Plaintiffs and Class Members, including names, Social Security numbers, and financial account information.

30. In response to the Data Breach, Defendant claims that it “moved quickly to investigate and respond to this incident, assess the security of relevant systems, and notify

⁵ *Id.* at 4.

⁶ Ex. 2 (Letter and sample *Notice of Data Breach* filed with New Hampshire Attorney General)

potentially affected individuals.”⁷ However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

31. The unencrypted PII of Plaintiffs and Class Members 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.

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for more than 299,000 individuals.

33. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁸

34. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

⁷ Exhibits 1, 2.

⁸ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited June 15, 2021).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁹

35. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems

⁹ *Id.* at 3-4.

(OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....¹⁰

36. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management

¹⁰ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited June 15, 2021).

- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹¹

37. Given that Defendant was storing the PII of more than 299,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

38. The occurrence of the Data Breach indicates that Defendant failed to adequately

¹¹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited June 15, 2021).

implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of more than 299,000 individuals, including Plaintiffs and Class Members.

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

39. Defendant acquired, collected, and stored the PII of Plaintiffs and Class Members at least from 2006 to 2020.

40. As a condition of obtaining employment through Defendant, Defendant requires that those obtaining such employment entrust Defendant with highly confidential PII.

41. By obtaining, 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 from disclosure.

42. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and 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

43. Defendant could have prevented this Data Breach by properly securing and encrypting the private cloud containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially decade-old data from those who obtained employment through Defendant years ago.

44. 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.

45. 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.

46. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹² 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.”¹³

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

Value of Personally Identifiable Information

48. 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 \$200.¹⁴ Experian reports that a stolen credit or debit

¹² 17 C.F.R. § 248.201 (2013).

¹³ *Id.*

¹⁴ *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 June 22, 2021).

card number can sell for \$5 to \$110 on the dark web.¹⁵ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁶

49. Social Security numbers, for example, are among the worst 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.¹⁷

50. 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.

51. Even then, a new Social Security number may not be effective. According to Julie

¹⁵ *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 June 22, 2021).

¹⁶ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed June 22, 2021).

¹⁷ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed June 22, 2021).

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.”¹⁸

52. 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—Social Security number and name.

53. 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.”¹⁹

54. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

55. The fraudulent activity resulting from the Data Breach may not come to light for years.

56. 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

¹⁸ 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 June 21, 2021).

¹⁹ 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 June 21, 2021).

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.²⁰

57. 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 financial account information, 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.

58. 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.

59. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s private cloud, amounting to potentially hundreds of thousands of individuals’ detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

60. To date, Defendant has not offered Plaintiffs and Class Members any identity theft detection or similar service, and instead merely suggested that Plaintiffs and Class Members monitor their account statements, explanation(s) of benefits, and credit bureau reports. The failure to offer such service is highly unusual and reflects an indifference to the seriousness of the exposure, which includes Social Security numbers. Defendant’s paltry recommendation to self-

²⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed June 15, 2021).

monitor 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.

61. 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 Daniel Hayes' Experience

62. In or around 2006, Plaintiff Hayes obtained employment through Defendant. As a condition of obtaining such employment, Defendant required that he provide his PII, including but not limited to his name and Social Security number.

63. Mr. Hayes received Defendant's Notice of Data Breach, dated March 17, 2021, on or about that date. The notice stated that Plaintiff Hayes' Social Security number was "present in the potentially accessed files and folders at the time of the incident."

64. After the Data Breach, Mr. Hayes's credit report showed a hospital visit that he did not make and a telephone number that is not his.

65. As a result of the Data Breach notice, Mr. Hayes spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

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

67. Mr. Hayes stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and

passwords for his various online accounts.

68. Mr. Hayes suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Hayes entrusted to Defendant for the purpose of obtaining employment through Defendant, which was compromised in and as a result of the Data Breach.

69. Mr. Hayes 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.

70. Mr. Hayes 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, being placed in the hands of unauthorized third parties and possibly criminals.

71. Mr. Hayes 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.

Plaintiff Katrina Nash's Experience

72. In or around 2016, Plaintiff Nash obtained employment through Defendant. As a condition of obtaining such employment, Defendant required that she provide her PII, including but not limited to her name, Social Security number, and financial account information.

73. Ms. Nash received Defendant's Notice of Data Breach, dated March 17, 2021, on or about that date. The notice stated that Plaintiff Nash's Social Security number and financial account information were "present in the potentially accessed files and folders at the time of the incident."

74. As a result of the Data Breach notice, Ms. Nash spent time dealing with the

consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

75. Additionally, Ms. Nash is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

76. Ms. Nash stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

77. Ms. Nash suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Nash entrusted to Defendant for the purpose of obtaining employment through Defendant, which was compromised in and as a result of the Data Breach.

78. Ms. Nash suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

79. Ms. Nash has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and possibly criminals.

80. Ms. Nash has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

81. 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.

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

All individuals whose PII was accessed during the incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 17, 2021 (the “Nationwide Class”).

83. Excluded from the Nationwide Class 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.

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

85. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class is so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of individuals who obtained employment through Defendant and 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 299,251 individuals.

86. 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 and when Defendant actually learned that the PII of Plaintiffs and Class Members had been potentially or actually accessed and/or compromised;
- g. Whether Defendant adequately, accurately, and timely informed Plaintiffs and Class Members that their PII had been potentially or actually accessed and/or compromised;
- h. Whether Defendant violated the law by failing to timely notify Plaintiffs and Class Members that their PII had been potentially or actually accessed and/or compromised;
- i. 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;
- j. Whether Defendant adequately addressed and fixed the vulnerabilities which

permitted the Data Breach to occur;

- k. Whether Plaintiffs and Class Members are entitled to actual, consequential, 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.

87. 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.

88. 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 Nationwide Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Nationwide 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.

89. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Nationwide Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Nationwide 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.

90. 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.

91. 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 was exposed is representative of that experienced by the Nationwide 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.

92. 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.

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

94. 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.

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

96. 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 implied contracts 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 implied contracts with Plaintiffs and Class Members;
 - f. Whether Defendant adequately, accurately, and timely informed Plaintiffs and Class Members that their PII had been potentially or actually accessed and/or 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 Plaintiffs and Class Members are entitled to actual, consequential, and/or 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)

97. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 96.

98. As a condition of obtaining employment through Defendant, Plaintiffs and the Nationwide Class were obligated to provide Defendant with certain PII, including names, Social Security numbers, and financial account information.

99. Plaintiffs and the Nationwide Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

100. 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.

101. 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.

102. 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.

103. Defendant also had a duty to exercise appropriate clearinghouse practices to remove the PII of Plaintiffs and Class Members it was no longer required to retain pursuant to regulations.

104. 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.

105. 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, a necessary part of obtaining employment through Defendant.

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

107. 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.

108. 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.

109. 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.

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

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

112. 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.

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

114. 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.

115. 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.

116. 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.

117. 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.

118. 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.

119. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove the PII of Plaintiffs and the Nationwide Class it was no longer required to retain pursuant to regulations.

120. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately, accurately, and timely disclose to Plaintiffs and the Nationwide Class that their PII had been potentially or actually accessed and/or compromised.

121. 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.

122. 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.

123. 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.

124. 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.

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

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

127. 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.

128. 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.

129. 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.

130. 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.

131. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

132. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

133. Defendant required Plaintiffs and the Nationwide Class to provide their personal information, including names, Social Security numbers, and financial account information.

134. As a condition of their treatment with Defendant, Plaintiffs and the Nationwide Class provided their personal and financial information. In so doing, Plaintiffs and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to adequately, accurately, and timely notify Plaintiffs and the Nationwide Class if their data had been actually or potentially accessed and/or compromised.

135. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

136. Defendant breached the implied contracts it made with Plaintiffs and the Nationwide Class by failing to safeguard and protect their personal and financial information and by failing to provide adequate, accurate, and timely notice to them that personal and financial information was potentially or actually accessed and/or compromised as a result of the data breach.

137. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

138. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

139. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

140. Plaintiffs and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

141. Defendant owed a duty to Plaintiffs and the Nationwide Class to keep their PII confidential.

142. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and the Nationwide Class.

143. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and the Nationwide Class, by way of Defendant's failure to protect the PII.

144. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and the Nationwide Class is highly offensive to a reasonable person.

145. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Nationwide Class disclosed their PII to Defendant as part of obtaining employment through Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

146. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

147. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

148. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Nationwide Class.

149. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and the Nationwide Class was disclosed to third parties without authorization, causing

Plaintiffs and the Nationwide Class to suffer damages.

150. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Nationwide Class.

151. As a direct and proximate result of Defendant's invasion of privacy, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class)

152. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

153. At all times during Plaintiffs' and the Nationwide Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Nationwide Class's PII that Plaintiffs and the Nationwide Class provided to Defendant.

154. As alleged herein and above, Defendant's relationship with Plaintiffs and the Nationwide Class was governed by terms and expectations that Plaintiffs' and the Nationwide Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

155. Plaintiffs and the Nationwide Class provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

156. Plaintiffs and the Nationwide Class also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

157. Defendant voluntarily received in confidence Plaintiffs' and the Nationwide Class's PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

158. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and the Nationwide Class's PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Nationwide Class's confidence, and without their express permission.

159. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and the Nationwide Class have suffered damages.

160. But for Defendant's disclosure of Plaintiffs' and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Nationwide Class's PII as well as the resulting damages.

161. The injury and harm Plaintiffs and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Nationwide Class's PII. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and the Nationwide Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Nationwide Class's PII.

162. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Nationwide Class, 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 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.

163. As a direct and proximate result of Defendant's breaches of confidence, 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.

164. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

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 appointing Plaintiffs and their Counsel to represent 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 adequate, accurate, and timely disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiff, 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, consequential, and nominal 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: June 23, 2021

Respectfully Submitted,

s/Jay Aughtman
Joseph "Jay" H. Aughtman (ASB-8081-A43J)
AUGHTMAN LAW FIRM, LLC
1772 Platt Place
Montgomery, AL 36117
Tel: 334-215-9873
Fax: 334-213-5663
jay@aughtmanlaw.com

Erby J. Fischer, II
MORGAN & MORGAN ALABAMA, PLLC
2317 3rd Avenue North, Suite 102
Birmingham, AL 35203
(659) 204-6364
efischer@forthepeople.com

John A. Yanchunis*
Ryan D. Maxey*
**MORGAN & MORGAN COMPLEX
BUSINESS DIVISION**
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

**pro hac vice to be filed*

Attorneys for Plaintiffs and the Proposed Class

DEFENDANT TO BE SERVED BY THE COURT BY CERTIFIED MAIL AS FOLLOWS:

Automation Personnel Services, Inc.
c/o Randy Watts
3500 Colonnade Parkway Suite 500
Birmingham, Al 35243

EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Automation Personnel Services (“APS”) does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

APS discovered suspicious activity impacting the operability of certain systems. APS quickly launched an investigation to determine the nature and scope of this incident, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed by the unknown actor. APS completed a thorough and lengthy review to determine whether sensitive information was present in the impacted files and folders. On February 3, 2020, it was confirmed that a Maine resident’s personal information was present in the files and folders that may have been accessed. APS then worked to locate address information for those whose personal information was accessible within the files and just completed that effort.

The information that could have been subject to unauthorized access includes name, Social Security number, and financial account information.

Notice to Maine Residents

Beginning on March 16, 2021, APS provided written notice of this incident to affected individuals, which includes approximately five (5) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, APS moved quickly to investigate and respond to the incident, assess the security of APS systems, and notify potentially affected individuals. APS is also working to implement additional safeguards and training to its employees.

Additionally, APS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. APS is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state and territory Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A



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

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

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Automation Personnel Services, Inc. (“APS”) writes to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On November 17, 2020, APS discovered suspicious activity impacting the operability of certain systems. We quickly launched an investigation to determine the nature and scope of this incident, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed by the unknown actor. We completed a thorough and lengthy review to determine whether sensitive information was present in the impacted files and folders. On February 3, 2021, it was confirmed that some of your personal information was present in the files and folders that may have been accessed. We then worked to locate address information for those whose personal information was accessible within the files and just completed that effort.

What Information Was Involved? The investigation determined that the following types of your personal information were present in the potentially accessed files and folders at the time of the incident: <<b2b_text_1(Impacted Data)>>.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the potentially accessed files and folders to determine whether they contained protected information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

APS notified law enforcement of this incident and is notifying relevant state and federal regulators.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 1-855-515-1650, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also write to APS at: 3500 Colonnade Parkway, Suite 500, Birmingham, AL 35243.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink, appearing to read 'David Soileau', with a long horizontal flourish extending to the right.

David Soileau
Vice President of Administration
Automation Personnel Services, Inc.

Steps You Can Take to Help Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. APS is located at 3500 Colonnade Parkway, Suite 500, Birmingham, AL 35243.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are ten (10) Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED
MAR 22 2021
CONSUMER PROTECTION

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 16, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Automation Personnel Services (“APS”), located at 3500 Colonnade Parkway, Suite 500, Birmingham, Alabama 35243, and are writing to notify your office of an incident that may affect the security of some personal information relating to approximately seven (7) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, APS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

APS discovered suspicious activity impacting the operability of certain systems. APS quickly launched an investigation to determine the nature and scope of this incident, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed by the unknown actor. APS completed a thorough and lengthy review to determine whether sensitive information was present in the impacted files and folders. On February 3, 2020, it was confirmed that some New Hampshire residents’ personal information was present in the files and folders that may have been accessed. APS then worked to locate address information for those whose personal information was accessible within the files and just completed that effort.

Mullen.law

Office of the New Hampshire Attorney General
March 16, 2021
Page 2

The information that could have been subject to unauthorized access includes name, Social Security number, and financial account information.

Notice to New Hampshire Residents

Beginning on March 16, 2021, APS provided written notice of this incident to affected individuals, which includes approximately seven (7) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, APS moved quickly to investigate and respond to the incident, assess the security of APS systems, and notify potentially affected individuals. APS is also working to implement additional safeguards and training to its employees.

Additionally, APS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. APS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state and territory Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4554.

Very truly yours,



Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT:kjc

EXHIBIT A



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

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

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Automation Personnel Services, Inc. ("APS") writes to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On November 17, 2020, APS discovered suspicious activity impacting the operability of certain systems. We quickly launched an investigation to determine the nature and scope of this incident, working with industry-leading computer forensics specialists to determine what happened and what information may have been affected. The investigation identified a limited number of files and folders as potentially accessed by the unknown actor. We completed a thorough and lengthy review to determine whether sensitive information was present in the impacted files and folders. On February 3, 2021, it was confirmed that some of your personal information was present in the files and folders that may have been accessed. We then worked to locate address information for those whose personal information was accessible within the files and just completed that effort.

What Information Was Involved? The investigation determined that the following types of your personal information were present in the potentially accessed files and folders at the time of the incident: <<b2b_text_1(Impacted Data)>>.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the potentially accessed files and folders to determine whether they contained protected information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

APS notified law enforcement of this incident and is notifying relevant state and federal regulators.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 1-855-515-1650, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also write to APS at: 3500 Colonnade Parkway, Suite 500, Birmingham, AL 35243.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink, appearing to read 'David Soileau', with a long horizontal flourish extending to the right.

David Soileau
Vice President of Administration
Automation Personnel Services, Inc.

Steps You Can Take to Help Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. APS is located at 3500 Colonnade Parkway, Suite 500, Birmingham, AL 35243.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are ten (10) Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Automation Personnel Services Hit with Class Action Over Nov. 2020 Data Breach](#)
