IN THE DISTRICT COURT OF OKLAHOMA COUNTY
WITHIN AND FOR THE STATE OF OKLAHOMA

CARMEN JOHNSON, on behalf of herself and her minor children **A.J.** and **H.J.**, **AMY KELLER**, on behalf of herself and her minor children **V.K. (1)** and **V.K. (2)**, **SARA LOVELESS,** on behalf of her minor children **S.L.** and **N.L.,** and **SARAH OSGOOD**, on behalf of herself and her minor child **S.O.,** together on behalf of themselves and all other similarly situated individuals,

Plaintiffs,

v.

PAYCOM PAYROLL, LLC,

Defendant.

Case No. CJ-2023-4763

Judge: Honorable Judge Brent Dishman

JURY TRIAL DEMANDED

SECOND AMENDED CLASS ACTION PETITION

Plaintiffs **Carmen Johnson**, on behalf of herself and her minor children **A.J.** and **H.J.**, **Amy Keller**, on behalf of herself and her minor children **V.K. (1)** and **V.K. (2)**, **Sara Loveless**, on behalf of her minor children **S.L.** and **N.L.**, and **Sarah Osgood**, on behalf of herself and her minor child **S.O.**, together on behalf of all other similarly situated individuals (collectively, "Plaintiffs"), upon personal knowledge of facts pertaining to them and upon information and belief as to all other matters, by and through their undersigned counsel, hereby bring this Second Amended Class Action Petition against Defendant **Paycom Payroll, LLC** ("Paycom" or "Defendant"), and allege as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action lawsuit against Paycom for its failure to

protect the personally identifiable information ("PII") of Plaintiffs and other individuals (the "Class" or "Class Members"), including their first and last names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

2. As a result of Paycom's failure to implement adequate data security and privacy measures in its use of the MOVEit software, well-known ransomware cybergang, Cl0p ("Clop") easily accessed and ***stole*** the PII of Plaintiffs and the Class in a massive and preventable data incident (the "Data Incident" or "Incident"). During the Data Incident, Clop accessed and exfiltrated Plaintiffs' PII. Now, Plaintiffs' and the Class's confidential PII is in the hands of cybercriminals who have already posted it for sale on the dark web and have begun to use it for nefarious purposes.

3. According to Paycom, it learned that Plaintiffs' PII was accessed and stolen by unauthorized cybercriminals between May 28, 2023, through June 2, 2023. Thus, for six (6) days the unauthorized actors had unfettered access to Plaintiffs' and the Class's PII.

4. After the Incident, Defendant initiated an investigation and determined that cybercriminals had "***accessed and downloaded***" the sensitive PII of Plaintiffs and the Class during the Data Incident.

5. Regrettably, Clop has already exploited the PII stolen in the Data Incident, including Plaintiffs' PII. Clop posted data obtained in the Incident on its dark web data leak site.[1]

---

[1] *See* https://www.resecurity.com/blog/article/cl0p-ups-the-ante-with-massive-moveit-transfer-supply-chain-exploit.

6. Further, Clop has not only stolen Plaintiffs' and Class Members' PII, but it has also conducted multiple private sales of Plaintiffs' and Class Members' data on forums since July of 2023. As a result, Plaintiffs' and Class Members' PII continues to be sold and resold on the dark web.

7. None of this should have happened because the Data Incident was entirely preventable.

8. Indeed, MOVEit users, such as Paycom, are each ***separately responsible*** for deciding what kinds of files to transfer using MOVEit, and for configuring the application to operate in a secure manner in their independent environments.

9. However, Paycom was negligent and utterly failed to configure the application to operate in a secure manner in its independent environment.

10. On or around July 31, 2023, Paycom sent a letter titled "Notice of Progress' MOVEit Incident" ("Notice Letter") to those impacted by the Data Incident, informing them that their PII was stolen in the Data Incident and was now at risk of misuse.

11. The PII compromised in the Data Incident included highly sensitive data that represents a gold mine for data thieves. Armed with the PII accessed in the Data Incident, data thieves can immediately commit a variety of sordid crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. Paycom willingly accepted the responsibility to adequately secure, safeguard, protect, and maintain the PII of Plaintiffs and the Class.

13. There has been no assurance offered by Paycom that Paycom has adequately enhanced its data security practices within its own environment since the Data Incident sufficiently to avoid a similar data incident in the future.

14. Similarly, Paycom has not terminated its use of the MOVEit software.

15. Therefore, Plaintiffs and Class Members have already suffered and are at an imminent, immediate, and continuing increased risk of continuing to suffer additional ascertainable losses from identity theft and other fraudulent misuse of their PII, including incurring out-of-pocket expenses to remedy or mitigate the effects of the Data Incident, and have suffered lost value of their time to reasonably remedy or mitigate the effects of the Data Incident.

16. The unauthorized access and theft of Plaintiffs' and Class Members' PII was a known risk to Defendant.

17. Specifically, Paycom knew or was negligent to not know that if it did not individually implement appropriate security measures with its use of the MOVEit software, that a data incident would occur and Plaintiffs' and the Class's PII would be unlawfully exposed and at risk.

18. Upon information and belief, Defendant failed to properly monitor its networks and systems, failed to properly implement adequate data security practices, procedures, infrastructure, and protocols, and failed to encrypt data. Had Defendant properly monitored and secured its computerized digital environment, the Data Incident would not

have happened and Plaintiffs' and Class Members' PII would not be on the dark web.

19. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct as the PII that Defendant collected and maintained is now on the dark web and is in the hands of data thieves and other unauthorized third parties. There is no question that well-known cybergang, Clop, has stolen Plaintiffs' and the Class's PII and is actively misusing such PII.

II. PARTIES

20. Plaintiff **Carmen Johnson**, on behalf of herself and her minor children **A.J.** and **H.J.**, is, and at all times mentioned herein was, an individual citizen of Tulsa, Oklahoma. Plaintiff Carmen Johnson received a Notice Letter from Defendant advising her that her PII and her minor children's PII was stolen in the Data Incident.[2]

21. Plaintiff **Amy Keller**, on behalf of herself and her minor children **V.K. (1) and V.K. (2)**, is, and at all times mentioned herein was, an individual citizen of Edmond, Oklahoma. Plaintiff Amy Keller received a Notice Letter from Defendant advising her that her PII and her minor children's PII was stolen in the Data Incident.[3]

22. Plaintiff **Sara Loveless**, on behalf of her minor children **S.L.** and **N.L.**, is, and at all times mentioned herein was, an individual citizen of Piedmont, Oklahoma. Plaintiff Sara Loveless received a Notice Letter from Defendant advising her that her minor children's PII was stolen in the Data Incident.[4]

23. Plaintiff **Sara Osgood**, on behalf of herself and her minor child **S.O.**, is, and

[2] *See* **Exhibit 1**
[3] *See* **Exhibit 2**
[4] *See* **Exhibit 3**

at all times mentioned herein was, an individual citizen of Dayton, Ohio. Plaintiff Sara Osgood, and S.O. both received a Notice Letter from Defendant advising them that their PII was stolen in the Data Incident.[5]

24. Defendant **Paycom Payroll, LLC** is a Delaware limited liability company registered in the State of Oklahoma with the Oklahoma Secretary of State. Paycom's corporate headquarters is located at 7501 W. Memorial Road, Oklahoma City, OK 73142.

III. JURISDICTION AND VENUE

25. This action arises under the authority vested in this Court by virtue of 12 O.S. §2004(F).

26. Venue is proper in this Court under 12 O.S. § 134, because Paycom has its principal place of business in Oklahoma County, Oklahoma, and the causes of action herein arose in this county.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Businesses and the Collection of Plaintiffs' and Class Members' PII.*

27. Paycom, established in 1998, is a human resources service provider whose vision is to "automate and streamline the highly complex payroll process through a single HR software."[6]

28. As a condition to employment and receipt of elective benefits from Paycom or a customer of Paycom, Plaintiffs and Class Members were required to provide Paycom with their PII.

---

[5] *See* **Exhibit 4**

[6] https://www.paycom.com/about/.

29. Paycom used the MOVEit application to store and/or transfer Plaintiffs' and the Class's PII.

30. Because of the highly sensitive and personal nature of the information Paycom acquired and stored, Defendant promised to, among other things: keep Plaintiffs' and the Class's PII private; comply with industry standards related to data security; only use and release highly sensitive information stored for reasons that relate to the services they provide; and provide adequate notice to individuals if their PII is disclosed without authorization.

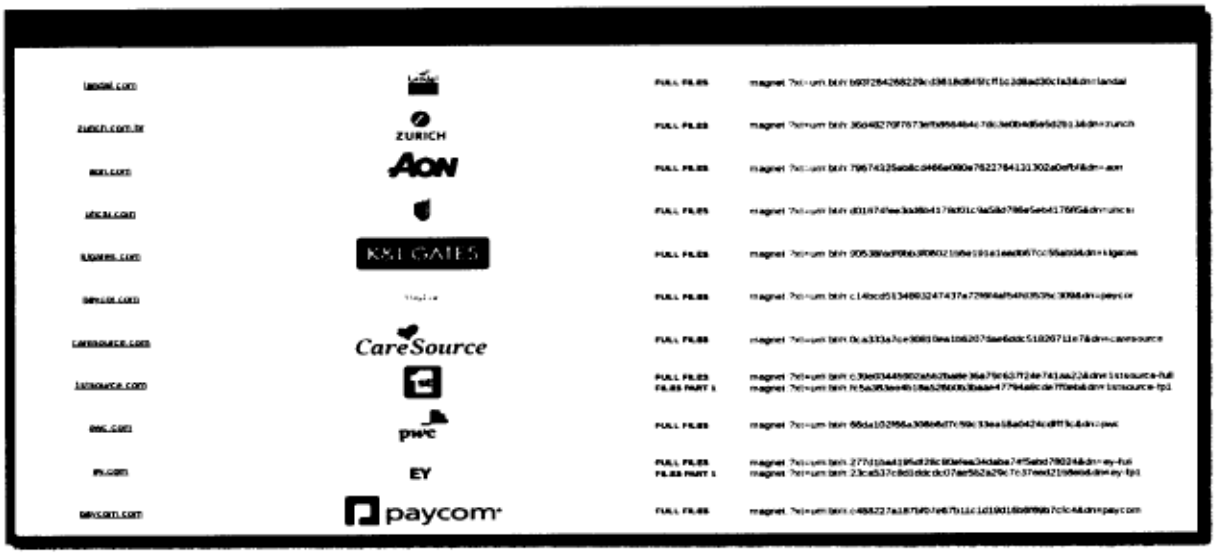
31. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that they each were individually responsible for protecting Plaintiffs' and Class Members' PII to ensure it was not subject to unauthorized disclosure and exfiltration.

32. Plaintiffs and Class Members relied on Defendant to keep their PII confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

B. *The Data Incident and Defendant's Inadequate Notice to Plaintiffs and Class Members*

33. On or around June 1, 2023, Paycom learned that that the file transfer application it used, and failed to adequately secure, MOVEit, was infiltrated by notorious cybercriminal gang, Clop, in a massive and preventable data incident. The Data Incident is confirmed by looking at Clop's own dark net website:

[IMAGE ON NEXT PAGE]



34. As a result of the Data Incident, Clop had access to Plaintiffs' and Class Members' PII from May 28, 2023, through June 2, 2023.

35. Despite the Data Incident occurring in May of 2023, Plaintiffs and Class Members did not begin receiving Notice Letters until more than two (2) months later.

36. Defendant has not provided an adequate explanation as to why it did not timely advise Plaintiffs and the Class of the Incident.

37. After receiving the notice letter, it is reasonable for recipients, including Plaintiffs and Class Members, to believe that the risk of future harm (including identity theft and fraud) is substantial and imminent. This is especially true considering multiple Plaintiffs' PII has already been misused and found on the dark web.

38. Paycom explicitly recognized the concrete and substantial risks of harm Plaintiffs and the Class now face. The Notice Letters disseminated by Paycom specifically advise Plaintiffs and the Class to "remain vigilant against incidents of identity theft and fraud

by monitoring your financial account statements and reviewing your credit reports for suspicious activity."[7]

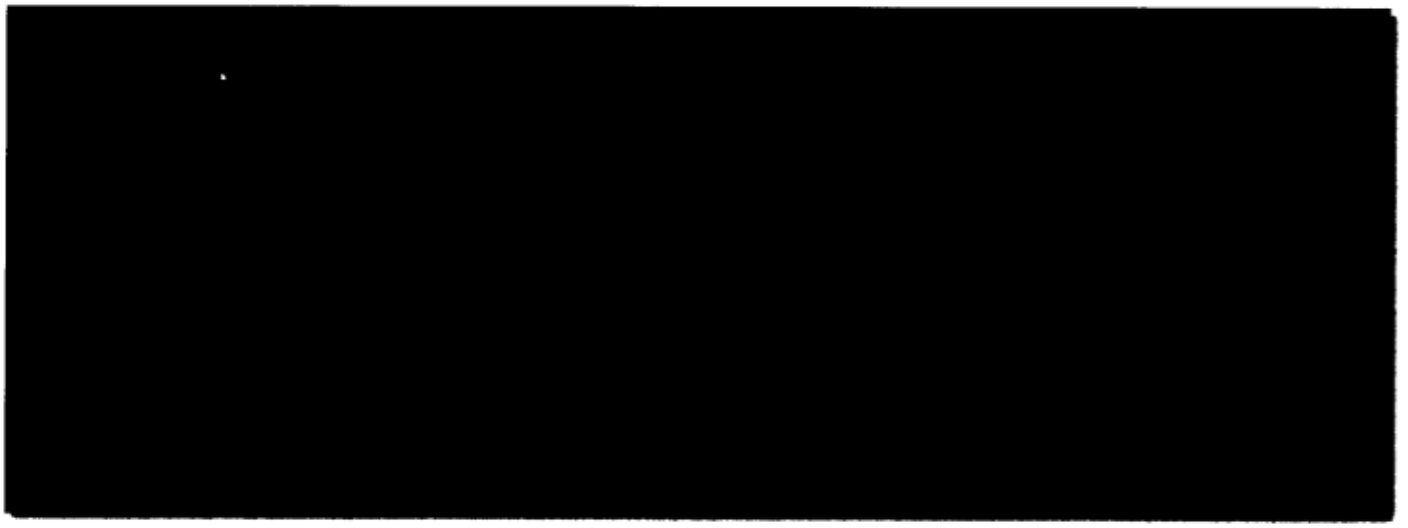
39. In further recognition of the risk of harm Plaintiffs and the Class now face, Paycom made an offering of 24 months of free credit monitoring services. There would be no need for such an offering if Plaintiffs and the Class were not at an imminent risk of future identity theft and harm. Nevertheless, this offer is wholly inadequate considering Plaintiffs and the Class will be at risk of identity theft and fraud for the rest of their lives.

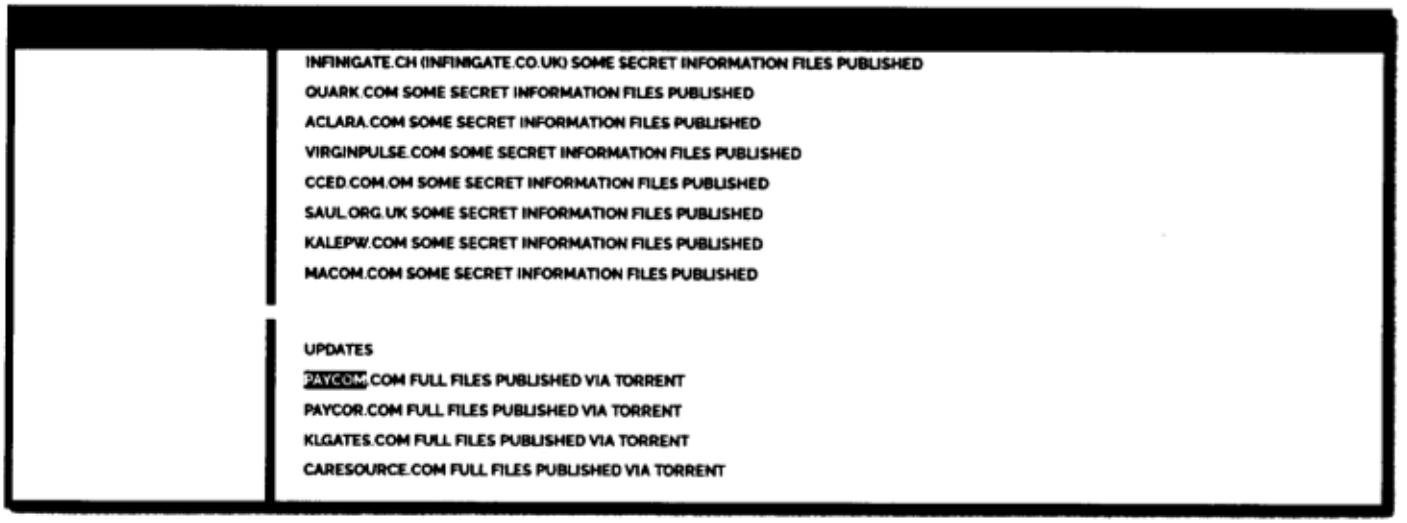
40. Upon information and belief, the cybercriminals gained access to the PII of Plaintiffs and the Class with the intent of misusing their PII, including marketing and selling Plaintiffs' and Class Members' PII on the dark web. In fact, multiple Plaintiffs have already experienced specific instances of actual misuse of their PII.

41. Further, Clop has claimed responsibility for publishing 360 GB of Plaintiffs' and Class Members' PII stolen from the Data Incident to its torrent site on August 17, 2023. Upon information and belief, the PII of Plaintiffs and Class Members remains available on Clop's torrent site. On ransomlook.io, Clop confirms the publishing of the data on its torrent site:

[IMAGES ON NEXT PAGE]

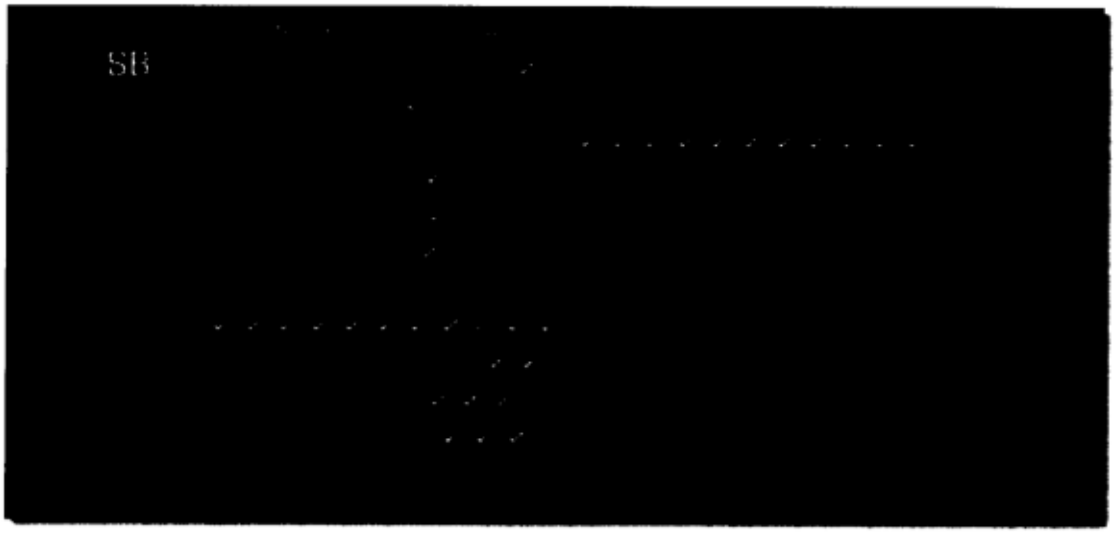
[7]https://apps.web.maine.gov/online/aeviewer/ME/40/0a6431a1-1278-41df-85d6-73ed0fc0dd8c/96030da1-c584-4394-98aa-e674790dd426/document.html





42. In addition, Plaintiffs' and Class Members' PII has specifically been identified as being sold and re-sold in private sales on dark web forums since July of 2023. For example, the Telegram forums and groups "Loaders and Carders(w SSN)" and the group Mad Hackers (handle represented as "MAD-HACKERS") listed the following by threat actor Cyb3r H3xagon and threat actor, "Only The", reposted by Steve Brandon (fake name):

[redacted]



43. Therefore, it is clear that the PII stolen in the Data Incident is not only at an increased risk of future misuse but is ***actively*** being sold to nefarious actors across the dark web.

44. Despite the severity of the Data Incident, Defendant has done very little to protect Plaintiffs and the Class. For example, and as previously stated, Defendant only provided 24 months of identity theft and credit monitoring protection to victims of the Data Incident. This complimentary service is a token gesture that does little if anything to remedy the harm Defendant's misconduct caused. This does not and will not fully protect Plaintiffs and the Class from cybercriminals and is largely ineffective against protecting data after it has been stolen. Cybercriminals are fully aware of the well-publicized preventative measures

taken by entities after data incidents. Therefore, cybercriminals oftentimes hold onto the stolen data and will not use it until after the complimentary service is no longer active and victim concerns and preventative steps have diminished. Moreover, these services do not prevent fraud, but only alert the individual of the fraud once the fraud has already occurred.

45. In effect, Defendant is shirking its responsibility for the harm and increased risk of harm it has caused Plaintiffs and members of the Class, including the distress and financial burdens the Data Incident has placed on Data Incident victims.

46. The Notice Letter fails to provide the consolation Plaintiffs and Class Members seek and certainly falls far short of eliminating the substantial risk of fraud and identity theft Plaintiffs and the Class now face and continue to experience. Paycom never once states it will remedy its negligent data retention/deletion policies, practices, procedures, and protocols.

47. As a result of Paycom's negligence in retaining Plaintiffs' and the Class's data far past the point of reasonable necessity, Plaintiffs' and Class Members' information has been misused and has been found on the dark web.

48. Further, "[Clop] also threatened that the exfiltrated data will be posted on the clear web which will enable all the users to see the exposed data without using specialized tools that are required for dark web surfing."[8]

49. There is no question Plaintiffs' and the Class's PII was stolen in the Data Incident as it has already been misused and has been found on the dark web involved in

[8] *See* https://thecyberexpress.com/clop-leaks-victim-data-moveit-hack-clear-web/; *see also* https://www.resecurity.com/blog/article/cl0p-ups-the-ante-with-massive-moveit-transfer-supply-chain-exploit.

multiple private sales.

50. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

51. Plaintiffs and Class Members provided their PII to Paycom with the reasonable expectation and mutual understanding that Paycom would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

52. Plaintiffs and the Class also provided their PII to Paycom with the reasonable expectation and mutual understanding that Paycom would take appropriate measures to ensure the applications it used, such as MOVEit, were secure.

53. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same Russian cybergang, Clop.[9]

54. Thus, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

C. *Paycom has Independent Responsibility for the Data Incident and Could Have Prevented the Data Incident.*

55. Paycom was independently responsible for securing its installation of the

---

[9] *See* https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/; *see also* https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/.

MOVEit transfer software and could have prevented the Data Incident if it had taken this responsibility seriously.

56. Paycom has a network infrastructure specific to its organization and had the sole responsibility of designing and developing its security network.

57. It is up to Paycom to employ software and practices to control and monitor access to its data and systems.

58. Paycom was separately responsible for deciding what kinds of files to transfer using MOVEit and configuring the product to operate in a secure manner in its environments.

59. In sum, Paycom had the sole responsibility to determine:

a) How to protect and configure the environments in which MOVEit was operating;

b) What kind of data was transferred and stored via MOVEit;

c) Whether and how to encrypt that data; and

d) Whether to monitor or respond to early indicators that hackers were taking steps to access and exfiltrate that data.

60. The creator of MOVEit (Progress Software Corporation ("PSC")) acknowledges this and publishes detailed recommendations for users, such as Paycom, regarding the configuration of the MOVEit software:

> Updates, settings, accounts, and policies should be reviewed on a regular cadence to ensure the configuration is meeting current compliance frameworks and to review for unexpected activity or behavior that needs to be addressed. It is recommended that MOVEit administrators perform a regular security audit with their corporate security and compliance teams. Many teams perform this monthly or quarterly. This document is intended to provide MOVEit administrators with a starting point to create their own security checklist that can be used for regular reviews.

> The list is not exhaustive and not all recommendations will apply to all MOVEit installations.[10]

61. PSC gives a detailed installation and configuration manual so that MOVEit users are in control of the security features offered in the software. Paycom disregarded these directives and failed to employ any security features in the software.

62. PSC also provides an administrator guide and a security best practices guide to aid in configuring and securing the MOVEit Transfer application. However, Paycom disregarded these directives.

63. MOVEit is also dependent on other software such as Windows Server, Microsoft SQL Server (MSSQL) or MySQL, and IIS, which Paycom failed to secure.

64. Additionally, other software and hardware solutions are involved such as routers, firewalls, and mail servers which could have provided access to the MOVEit server to those who should not have it like Clop. Those other software solutions and systems are not produced or maintained by PSC and are not the responsibility of PSC to secure. It is the responsibility of Paycom.

65. The data is hosted, maintained, and secured by Paycom, not PSC.

66. Paycom was responsible for securing its installation of the MOVEit Transfer software and designing and securing the network infrastructure. However, Paycom negligently failed to do so.

67. This is evidenced by the fact that not all MOVEit users were impacted.

68. Indeed, some MOVEit users had appropriate monitoring and other security

[10] https://community.progress.com/s/article/MOVEit-Security-Best-Practices-Guide.

measures in place and, as a result, were able to detect and thwart efforts to exploit the MOVEit vulnerability on their systems.

69. For instance, on May 27, 2023, Akamai, a managed detection and response service that corporations can hire to monitor their data systems, detected the attack and prevented it. "Akamai researchers detected exploitation attempts against one of Akamai's financial customers — an attack that was blocked by the Akamai Adaptive Security Engine."[11]

70. For this particular vulnerability with the MOVEit application, Paycom exercising some basic security practices would have mitigated the vulnerability, to gain access, which would have prevented the Incident.

71. Clop used the ATT&CK Techniques for Enterprise.

72. Clop simply exploited a weakness in MOVEit to write a file to the web server which was a Remote Access Tool.

73. Security measures to prevent unauthenticated users from Russian IP addresses accessing the server would have stopped the Incident in its tracks. However, Paycom did not have these security measures in place.

74. A deny all default approach to security would have prevented the Incident. However, Paycom did not have this in place.

75. Any one of the following security measures, if employed by Paycom, could have stopped the Data Incident from occurring:

a) **Denying write access to all but local account used for writing**

[11] *See* https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware.

to the web directory. There is no reason to grant unauthenticated user access and all user access to a file or directory that does not need write access. Additionally, there are solutions with MOVEit and third-party solutions to provide an email or SMS notification in the event files are accessed, created, or modified.

b) **A firewall dropping all packets originating from IP addresses outside of the organization.** By dropping all packets from foreign IP addresses, this would have prevented Clop the ability to connect to perform the SQL injection.

c) **Placing the server in a DMZ.** This would have prevented Clop from delivering the TrueBot malware stopping the Data Incident. Publicly facing web servers can provide an attacker access inside the organization where they can traverse systems on the inside of any perimeter firewalls. A DMZ would help mitigate that vulnerability.

76. Unfortunately for Plaintiffs and the Class, Paycom negligently failed to implement any of the above measures prior to the Data Incident.

D. *Paycom Failed to Comply with FTC Guidelines*

77. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

78. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep,

properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

79. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

81. As evidenced by the Data Incident, Paycom negligently failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

82. Defendant was at all times fully aware of its obligations to protect the PII of

Plaintiffs and Class Members yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

83. Further, Defendant knew, or should have known, that Plaintiffs and the Class were relying on it to protect their PII that Defendant required from each of them.

84. Some industry best practices that should be implemented by businesses like Defendant include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Incident, Paycom failed to follow some or all these industry best practices.

85. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff and customers regarding these points. As evidenced by the Data Incident, Paycom failed to follow these cybersecurity best practices.

86. Paycom failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

87. Paycom failed to comply with these accepted standards, thereby permitting the Data Incident to occur.

E. *Paycom Breached its Duties to Safeguard Plaintiffs' and Class Members' PII.*

88. In addition to their obligations under federal and state laws, Paycom owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, transferring, storing, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

89. Paycom owed a duty to Plaintiffs and Class Members to provide reasonable data security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, software, networks, and protocols adequately protected the PII of Class Members.

90. Defendant breached its duties and obligations owed to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Plaintiffs' and the Class's PII. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. failing to configure the MOVEit application to operate in a secure manner in its independent environment;

c. failing to adequately protect customers' PII;

d. failing to properly monitor its own data security systems for existing intrusions;

e. failing to properly oversee and monitor the MOVEit software;

f. failing to sufficiently train its employees regarding the proper handling of its customers' files containing the PII;

g. failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

h. failing to adhere to industry standards for cybersecurity as discussed above; and

i. otherwise breaching duties and obligations to protect Plaintiffs' and Class Members' PII.

91. Paycom negligently and unlawfully failed to implement adequate data security and privacy measures in its use of the MOVEit software.

92. Had Paycom remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems through the MOVEit software, and ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

93. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed because of the Data Incident and now face instances of identity theft, fraud, and are the victims of having their PII continuously sold across the dark web. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

F. *Defendant Should Have Known that Cybercriminals Target PII to Carry Out Fraud and Identity Theft*

94. The FTC hosted a workshop to discuss "informational injuries," which are

injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[12]

95. Exposure of highly sensitive personal information that a consumer wants to keep private may cause harm to the consumer, such as the ability to obtain or keep employment.

96. A victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market (i.e., dark net or dark web) to identity thieves who can then extort and harass victims or to take over victims' identities to engage in illegal financial transactions under the victims' names.

97. Indeed, Plaintiffs' PII has already been found and sold on the dark web, and multiple Plaintiffs have experienced instances of actual misuse of their PII in the form of identity theft and fraud.

98. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login

---

[12] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff- perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls, text messages, or phishing emails.

99. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

100. Thus, even if certain information was not purportedly involved in the Data Incident, the unauthorized parties could use Plaintiffs' and Class Members' PII to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

101. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[13] However, these steps do

---

[13] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps.

not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

102. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

103. PII can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond a doubt that PII has considerable market value.

104. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[14] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

---

[14] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr announces-indictment-fourmembers-china-s-military.

105. The PII of consumers 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, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[16]

106. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[17]

107. The Dark Web Price Index of 2022, published by PrivacyAffairs[18] shows how valuable just email addresses alone can be, even when not associated with a financial account:

---

[15] *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/.

[16] *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/.

[17] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/.

[18] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/.

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

108. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

109. Likewise, the value of PII is increasingly evident in our digital economy. Many companies collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and share it with third parties for similar purposes.[19]

110. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[20]

111. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

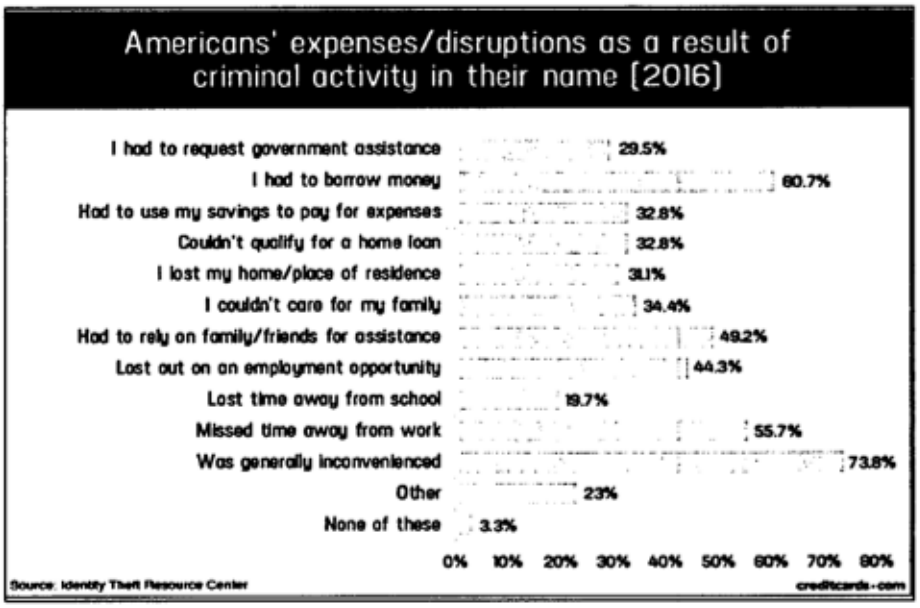
112. A consumer's ability to use their PII is encumbered when their identity or

[19] *See* https://robinhood.com/us/en/support/articles/privacy-policy/.
[20] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Incident led to a diminution in value of the PII.

113. Data incidents, like at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

114. A study by the Identity Theft Resource Center[21] shows the multitude of harms caused by fraudulent use of PII:



[21] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (image no longer available).

115. It must also be noted that there ***may*** be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[22]

> [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.

116. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

117. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. *Plaintiffs' Individual Experiences*

Plaintiff Carmen Johnson on Behalf of Herself and her Minor Children A.J. and H.J.

118. Plaintiff Carmen Johnson provided her PII, and the PII of her minor children, A.J. and H.J., including names, Social Security numbers, dates of birth, passport information,

---

[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html.

and employment authorization card information to Defendant in connection with her husband's employment with Defendant.

119. On or around July 31, 2023, Plaintiff Carmen Johnson received Notice Letters from Paycom notifying her that her PII, and the PII of her minor children, including names, Social Security numbers, dates of birth, passport information, and employment authorization card information were compromised as a result of the Data Incident.

120. As a direct and traceable result of the Data Incident, Carmen Johnson has spent countless hours researching the Data Incident, reviewing and monitoring her accounts for fraudulent activity, and reviewing credit reports for fraudulent activity. However, this is not the end. Plaintiff Carmen Johnson and the Class will now be forced to expend additional time to review their credit reports and monitor their accounts for the rest of their lives. This is time spent at Defendant's direction, which has been lost forever and cannot be recaptured.

121. Plaintiff Carmen Johnson places significant value in the security of her PII and the PII of her minor children. Plaintiff Carmen Johnson entrusted her personal PII and the PII of her minor children to Defendant with the understanding that Defendant would keep their information secure, and that Defendant would employ reasonable and adequate security measures to ensure that their PII would not be compromised.

122. As a direct and traceable result of the Data Incident, Plaintiff Carmen Johnson and her minor children A.J. and H.J. suffered actual damages such as: (i) theft of their PII; (ii) lost time related to monitoring their accounts for fraudulent activity; (iii) loss of privacy due to their PII being exfiltrated by cybercriminals; (iv) loss of the benefit of the bargain because Defendant did not adequately protect their PII; (v) severe emotional distress because

identity thieves now possess their PII; (vi) exposure to an increased and imminent risk of fraud and identity theft now that their PII has been stolen; (vii) loss in value of their PII due to their PII being in the hands of cybercriminals who can use it at their leisure; and (viii) other economic and non-economic harm.

123. As a direct and traceable result of the Data Incident, Plaintiff Carmen Johnson and her minor children A.J. and H.J. have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Incident.

124. Paycom acknowledged the increased risk of future harm Plaintiffs and the Class now face by paying for credit monitoring services to Plaintiffs and the Class. Such an offer is woefully inadequate as it will not prevent identity theft and fraud but will only alert Plaintiffs once it has already occurred. Paycom's measly two (2) year offering of monitoring services completely ignores the fact that Plaintiffs and the Class will be at a significant and imminent risk of future harm for the rest of their lives.

125. Knowing that thieves intentionally targeted and stole their PII, including their Social Security numbers, and knowing that Clop has already released data obtained in the Incident for sale on the dark web, Plaintiff Carmen Johnson and her minor children A.J. and H.J have great anxiety beyond mere worry. Specifically, Plaintiff Carmen Johnson has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her PII and the PII of her minor children has been compromised as a result of the Data Incident.

126. Plaintiff Carmen Johnson has a continuing interest in ensuring that her PII, and the PII of A.J. and H.J., which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data incidents.

127. As a direct and traceable result of the Data Incident, Plaintiff Carmen Johnson and her minor children A.J. and H.J. will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of their life to protect their PII.

Plaintiff Amy Keller on Behalf of Herself and Her Minor Children V.K. (1) and V.K. (2)

128. Plaintiff Amy Keller, on behalf of herself and her minor children V.K. (1) and V.K. (2), provided their PII, including their names, Social Security numbers, dates of birth, passport information, and employment authorization card information to Defendant in connection with her husband's employment with Defendant.

129. On or around July 31, 2023, Plaintiff Keller began receiving Notice Letters from Paycom on behalf of herself and her minor children notifying her that their names, Social Security numbers, dates of birth, passport information, and employment authorization card information were compromised in the Data Incident.

130. The PII Paycom failed to protect and that was subsequently compromised by cybercriminals has already been misused for nefarious purposes following the Data Incident.

131. Specifically, after the Data Incident , on October 4, 2023, Plaintiff Keller received a CreditWise alert that her Social Security number was compromised and found on the dark web. Further, on October 5, 2023, Plaintiff Keller's husband, a former employee of Paycom, received a CreditWise alert that his Social Security number was also compromised

and found on the dark web. Upon information and belief, Plaintiff Keller's husband's PII was also compromised in the Data Incident and is now on the dark web.

132. Plaintiff Keller reasonably believes the misuse she has experienced following the Data Incident is a direct result of her PII being stolen in the Data Incident. Specifically, because the PII that was stolen (Social Security numbers) is the same type of PII found on the dark web, and considering Clop has already confirmed the publishing of PII on the dark web in connection with the Data Incident, the publishing of Plaintiff Keller's PII is fairly traceable to the Data Incident. It is particularly troublesome to Plaintiff Keller that Paycom retained her and her minor children's PII long after her husband terminated his employment relationship with Paycom.

133. As a direct and traceable result of the Data Incident and considering her PII has been found on the dark web, Plaintiff Keller has spent countless hours researching the Data Incident, reviewing and monitoring her accounts for fraudulent activity, and reviewing credit reports for fraudulent activity. However, this is not the end. Plaintiffs and the Class will now be forced to expend additional time to review their credit reports and monitor their accounts for the rest of their lives. This is time spent at Defendant's direction, which has been lost forever and cannot be recaptured.

134. As a result of the Data Incident, Plaintiff Keller has also received numerous phishing emails and text messages since the Data Incident occurred, requiring her to spend additional time verifying the legitimacy of such messages. Specifically, Plaintiff Keller has received subscription renewal notifications from unknown websites, emails purporting to be geek squad support, and a substantial increase in unsolicited advertisements.

135. Plaintiff Keller places significant value in the security of the PII of her and her children. Plaintiff Keller entrusted her PII and the PII of her minor children to Defendant with the understanding that Defendant would keep their information secure, and that Defendant would employ reasonable and adequate security measures to ensure that their PII would not be compromised.

136. As a direct and traceable result of the Data Incident, Plaintiff Keller and her minor children, V.K. (1) and V.K. (2), suffered actual damages such as: (i) theft of their PII; (ii) Plaintiff Keller's PII being disseminated on the dark web; (iii) lost time related to monitoring their accounts for fraudulent activity; (iv) loss of privacy due to their PII being exfiltrated by cybercriminals and published on the dark web; (v) loss of the benefit of the bargain because Defendant did not adequately protect their PII; (vi) severe emotional distress because identity thieves now possess their PII; (vii) exposure to an increased and imminent risk of fraud and identity theft now that their PII has been stolen; (viii) loss in value of their PII due to their PII being in the hands of cybercriminals who can use it at their leisure; and (ix) other economic and non-economic harm.

137. As a direct and traceable result of the Data Incident, Plaintiff Keller and her minor children, V.K. (1) and V.K. (2), have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. Such a risk is certainly real and impending, and is not speculative, especially given the highly sensitive nature of the PII compromised by the Data Incident and the presence of Plaintiff Keller's PII on the dark web.

138. Knowing that thieves intentionally targeted and stole their PII, including Social

Security numbers, and knowing that Plaintiff Keller's PII is on the dark web has caused Plaintiff Keller great anxiety beyond mere worry. Specifically, Plaintiff Keller has lost hours of sleep, is in a constant state of stress for her minor children's PII, is very frustrated, and is in a state of persistent worry now that her PII has been located on the dark web.

139. Plaintiff Keller and her minor children, V.K. (1) and V.K. (2), have a continuing interest in ensuring that their PII which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

140. As a direct and traceable result of the Data Incident, and considering Plaintiff Keller's PII has already been found on the dark web, Plaintiff Keller and her minor children, V.K. (1) and V.K. (2), will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of their life to protect their PII.

Plaintiff Sara Loveless on Behalf of Her Minor Children S.L. and N.L.

141. Plaintiff Sara Loveless is a former employee of Paycom. Plaintiff Loveless worked for Defendant from approximately 2016 through July 2021 as a Team Lead for the IT Governance, Risk and Privacy/Data Governance teams. Plaintiff Loveless provided her PII and her minor children's PII to receive employment and elective benefits stemming therefrom.

142. Plaintiff Loveless received two Notice Letters from Defendant dated July 31, 2023, informing her that her minor children's information was exposed in the Data Incident. Consequently, Plaintiff Loveless reasonably believes her PII was also exposed in the Data Incident.

143. It is particularly troublesome to Plaintiff Loveless that Paycom retained her and her minor children's PII long after she terminated her employment relationship with Paycom, approximately two years ago.

144. As a direct and traceable result of the Data Incident, Plaintiff Loveless has been forced to spend time dealing with and responding to the direct consequences of the Data Incident, which includes researching the Data Incident and reviewing her credit report. This is time that has been lost forever and cannot be recaptured.

145. Plaintiff Loveless is very careful about sharing her PII and the PII of her minor children. Plaintiff Loveless and her minor children have never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Moreover, Plaintiff Loveless stores all documents containing her PII and her minor children's PII in a safe and secure location.

146. Plaintiff Loveless and her minor children have suffered actual, concrete injury in the form of damages to, and diminution in, the value of their PII – a form of intangible property that Plaintiff Loveless entrusted to Defendant for the purpose of her employment.

147. Plaintiff Loveless has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Incident, and has stress, anxiety, and increased concerns due to the loss of her and her minor children's privacy and the substantial risk of fraud and identity theft they now face. Plaintiff Loveless is especially concerned that cybercriminals obtained S.L. and N.L.'s PII because they are only minors. She worries about the negative impact this will have on their futures. Needless to say, knowing that thieves stole her PII and the PII of

her minor children, including Social Security numbers, and knowing that their PII will be sold on the dark web by Clop has caused Plaintiff Loveless great anxiety.

148. Plaintiff Loveless and her minor children have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of their PII. Especially since her minor children's Social Security numbers, in combination with their names, are now in the hands of cybercriminals.

149. Plaintiff Loveless has a continuing interest in ensuring that her and her minor children's PII which, upon information and belief, remains in the possession of Defendant, is protected or purged from Paycom's systems.

150. As a direct and traceable result of the Data Incident, Plaintiff Loveless and her children will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of their lives to protect their exposed PII.

Plaintiff Sarah Osgood on Behalf of Herself and Her Minor Child S.O.

151. Plaintiff Sarah Osgood's husband is a former employee of Paycom. Plaintiff Osgood's husband worked for Defendant from approximately December of 2017 through May of 2021. Plaintiff Sarah Osgood provided her PII, and the PII of her minor child, S.O, to receive elective benefits stemming from her husband's employment with Paycom.

152. Plaintiff Sarah Osgood received two Notice Letters from Defendant dated July 31, 2023, informing her that her and her minor child's information was exposed in the Data Incident.

153. It is particularly troublesome to Plaintiff Sarah Osgood that Paycom retained

her and her minor child's PII long after her husband terminated his employment relationship with Paycom over two years ago.

154. As a direct and traceable result of the Data Incident, Plaintiff Sarah Osgood has been forced to spend time dealing with and responding to the direct consequences of the Data Incident, which includes researching the Data Incident and reviewing her credit report. This is time that has been lost forever and cannot be recaptured.

155. Further, as a direct and traceable result of the Data Incident, Plaintiff Sarah Osgood has also experienced actual misuse of her PII. Specifically, since the Data Incident, Plaintiff Osgood has received multiple text messages informing her and her husband that a "USPS" package ordered in their name has arrived at a warehouse but cannot be delivered. Plaintiff Osgood is completely unaware of the package the message is referring to. Therefore, an unauthorized individual is placing orders in Plaintiff Sarah Osgood's name.

156. Plaintiff Sarah Osgood is very careful about sharing her and her minor child's PII. Plaintiff Osgood and her minor child, S.O., have never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Moreover, Plaintiff Sarah Osgood stores all documents containing her PII and her minor child's PII in a safe and secure location.

157. Plaintiff Osgood and her minor child have suffered actual, concrete injury in the form of damages to, and diminution in, the value of their PII – a form of intangible property that Plaintiff Osgood entrusted to Defendant for the purpose of receiving benefits.

158. Plaintiff Sarah Osgood has also suffered actual, concrete injury in the form of actual misuse, lost time and opportunity costs, annoyance, interference, and inconvenience

as a direct and traceable result of the Data Incident, and has stress, anxiety, and increased concerns due to the loss of her and her minor children's privacy and the substantial risk of fraud and identity theft which she and her children now face. Plaintiff Osgood is especially concerned that cybercriminals obtained S.O.'s PII because he is a minor. She worries about the negative impact this will have on his future. Needless to say, knowing that thieves stole her and her minor child's PII, including their Social Security numbers, and knowing that Clop will sell their PII on the dark web, has caused Plaintiff Osgood great anxiety.

159. Plaintiff Osgood and her minor child have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of their PII. Especially since her and her minor child's Social Security numbers, in combination with their names, are now in the hands of cybercriminals.

160. Plaintiff Osgood has a continuing interest in ensuring that her and her minor child's PII which, upon information and belief, remains in the possession of Defendant, is protected or purged from Paycom's systems.

161. As a direct and traceable result of the Data Incident, Plaintiff Osgood and her child will continue to be at heightened risk for financial fraud, additional instances of identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of their lives to protect their exposed PII.

H. *Plaintiffs' and Class Members' Damages*

162. Plaintiffs would not have provided their PII to Paycom had Paycom disclosed it lacked adequate data security.

163. Additionally, Plaintiffs would not have permitted their PII to be transmitted

and/or stored via the MOVEit software had Paycom disclosed it took no measures to secure it.

164. Plaintiffs have suffered actual injury in the form of time spent dealing with the Data Incident and the increased risk of fraud resulting from the Data Incident.

165. Plaintiffs suffered actual injury in the form of having their PII stolen, published on the dark web, and sold across the dark web by unauthorized vendors to nefarious actors as a result of the Data Incident.

166. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII – a form of intangible property that Plaintiffs entrusted to Paycom.

167. Plaintiffs suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their PII now being sold and being placed in the hands of criminals.

168. Plaintiffs and the Class have a continuing interest in ensuring that their PII, which remains in Defendant's possession and stored within MOVEit, is protected, and safeguarded from future breaches.

169. Plaintiffs also suffered actual injury as a result of the Data Incident in the form of (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from them; (b) violation of their privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud they now face.

170. As a result of the Data Incident, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the

Data Incident.

171. In sum, Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Incident.

172. Plaintiffs' PII was compromised as a direct and proximate result of the Data Incident, which resulted from Paycom's failure to ensure it employed adequate data security with the use of the MOVEit software.

173. As a direct and proximate result of Defendant's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of fraud and identity theft.

174. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their PII, since potential fraudsters will likely use such PII to carry out such targeted schemes against Plaintiffs and Class Members.

175. The PII maintained by and stolen from Defendant, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

176. Additionally, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the Data Incident on their everyday lives, including placing "freezes"

and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and/or closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

177. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Incident.

178. Plaintiffs and Class Members also suffered a loss of value of their PII when it was accessed, viewed, and acquired by Clop in the Data Incident. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for PII also exists, as is evidenced by the multiple private sales of Plaintiffs' and Class Members' PII.[23] In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[24] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[25]

179. As a result of the Data Incident, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its theft and acquisition by cybercriminals. This transfer of valuable

---

[23] *See* Data Coup, https://datacoup.com/.
[24] *What is digi.me?, DIGI.ME,* https://digi.me/what-is-digime/.
[25] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is apparently readily available to others. As a result, the rarity of the PII has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

180. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Incident in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Incident. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

181. Moreover, Plaintiffs and Class Members have a continuing interest in ensuring that their PII, which is believed to still be in the possession of Defendant, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

182. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

183. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to 12 O.S. § 2023(A) and (B).

184. Specifically, Plaintiffs proposes the following Nationwide Class (referred to herein as the "Class" or "Class Members"), subject to amendment as appropriate:

> All living individuals residing in the United States whose personal information was accessed or acquired in the Data Incident.

185. Excluded from the Class is Defendant and its parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

186. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class and Oklahoma Subclass, as well as add subclasses, before the Court determines whether certification is appropriate.

187. Numerosity. There are over 21,000 members of the Class, thus they are too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

188. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Paycom engaged in the conduct alleged herein;

b. When Paycom learned of the Data Incident;

c. Whether Paycom's response to the Data Incident was adequate;

d. Whether Paycom unlawfully lost or disclosed Plaintiffs' and Class Members' PII;

e. Whether Paycom failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Incident;

f. Whether Paycom failed to implement adequate data security and privacy measures in its use of the MOVEit software;

g. Whether Paycom failed to employ appropriate data security measures within MOVEit;

h. Whether Paycom failed to oversee and monitor MOVEit;

i. Whether Paycom's data security practices related to MOVEit prior to and during the Data Incident complied with applicable data security laws and regulations;

j. Whether Paycom owed a duty to Class Members to safeguard their PII;

k. Whether Paycom breached it duties to Class Members to safeguard their PII;

l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Incident to Plaintiffs and the Class Members;

m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Incident to Plaintiffs and Class Members;

n. Whether Paycom knew or should have known that its data security systems and monitoring processes as it relates to MOVEit were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

p. Whether Defendant's conduct was negligent;

q. Whether Defendant's conduct was *per se* negligent;

r. Whether Defendant's were unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiffs and Class Members are entitled to credit or identity monitoring and monetary relief; and

u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

189. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Incident.

190. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

191. Predominance. Paycom has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and was unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

192. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

193. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

194. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names, addresses, and/or email addresses of Class Members affected by the Data Incident.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE

195. Plaintiffs restate and reallege the allegations stated above as if fully set forth herein.

196. Paycom knowingly collected, acquired, and stored Plaintiffs' and Class Members' PII, and had a duty to exercise reasonable care in safeguarding and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

197. To fulfill this duty of care, Paycom was required to ensure it maintained adequate data security, procedures, systems, infrastructure, and protocols and implemented such across its entire network environment.

198. Paycom was also required to oversee, monitor, and adequately protect all software it utilized to store and transfer Plaintiffs' and the Class's PII.

199. Paycom's duty also included a responsibility to implement processes by which it could detect and analyze a vulnerability quickly and to give prompt notice to those affected in the case of a cyberattack.

200. Paycom knew or should have known of the risks inherent in collecting the PII of Plaintiffs and Class Members and the importance of adequate data security.

201. Paycom was on notice because, on information and belief, it knew or should have known of the substantial increase in cyberattacks in recent years, including recent similar attacks against Accellion and Fortra carried out by the same Russian cyber gang, Clop.

202. After all, PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, transferring, and storing the PII of Plaintiffs and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to it.

203. Paycom owed a duty of care to Plaintiffs and Class Members to provide data

security consistent with industry standards and other requirements discussed herein, and to ensure that its systems, software, and networks, and the personnel responsible for them, adequately protected the PII in its possession.

204. Paycom breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. And but for Paycom's negligence, Plaintiffs and Class Members would not have been injured. The specific negligent acts and omissions committed by Paycom include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to employe adequate security measures in its use of the MOVEit software;

c. Failing to adequately monitor and oversee the security of the MOVEit software;

d. Failing to ensure that the MOVEit software had security in place to maintain reasonable data security;

e. Failing to intelligently decide what kinds of files to transfer using the MOVEit software and configure the software to operate in Paycom's independent environment;

f. Failing to comply with—and thus violating—FTC Act and its regulations;

g. Failing to have in place mitigation policies and procedures;

h. Allowing unauthorized access to Class Members' PII;

i. Failing to detect in a timely manner that Class Members' PII had been compromised; and

j. Failing to timely notify Class Members about the Data Incident so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

205. Under the Federal Trade Commission Act, Defendant had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data. Plaintiffs and the Class are precisely the class of individuals the FTCA was designed to protect.

206. Moreover, Plaintiffs and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

207. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

208. Defendant owed Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Incident. This duty is necessary for Plaintiffs and Class Members to

take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of Defendant's Data Incident.

209. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the PII of Plaintiffs and Class Members.

210. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

211. Simply put, Defendant's negligence actually and proximately caused Plaintiffs and Class Members' actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, actual misuse of their PII, the publishing and sale of their PII on the dark web, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Incident that resulted from and were caused by Defendant's negligence. Moreover, multiple Plaintiffs have already suffered injuries-in-fact and damages are ongoing, imminent, and immediate.

212. Plaintiffs and Class Members are entitled to compensatory and consequential

damages suffered because of the Data Incident.

213. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strengthen its data security systems and monitoring procedures regarding the MOVEit software; (2) submit to future annual audits of those systems and monitoring procedures; and (3) to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT

214. Plaintiffs restate and reallege the allegations stated above as if fully set forth herein.

215. Plaintiffs and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect their PII and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

216. Plaintiffs and the Class were required to, and delivered, their PII to Defendant as a condition to employment or receipt of elective benefits stemming therefrom.

217. Plaintiffs and Class Members conferred a monetary benefit on Defendant in that Plaintiffs paid money to Defendant in exchange for services. Part of this monetary benefit was to be used to provide a reasonable level of data security to protect Plaintiffs' and the Class's PII.

218. Defendant accepted possession of Plaintiffs' and Class Members' PII for the purpose of providing services.

219. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under state and federal regulations. The additional

consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

220. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

221. Based on the implicit understanding, Plaintiffs and Class Members accepted Defendant's offers for services and provided Defendant with their PII.

222. Plaintiffs and Class Members would not have permitted their PII to be collected and stored by Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

223. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

224. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Incident.

225. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Paycom's breach of its implied contracts with

Plaintiffs and Class Members.

COUNT III
INVASION OF PRIVACY

226. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

227. Plaintiffs and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access and publication of their PII to criminal actors, as occurred with the Data Incident. The PII of Plaintiffs and Class Members contain intimate details of a highly personal nature, individually and in the aggregate.

228. Plaintiffs and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

229. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party.

230. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

231. This invasion of privacy resulted from Defendant's intentional failure to adequately implement, maintain, monitor and oversee the security of the MOVEit software, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data, which has been misused and sold across the dark web.

232. Plaintiffs and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs', and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

233. The disclosure of Plaintiffs' and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

234. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and Class Members' intimate and sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

235. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

236. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT IV
UNJUST ENRICHMENT

237. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

238. This Count is pleaded in the alternative to Count II.

239. Plaintiffs and Class Members conferred a benefit on Defendant by surrendering their PII to Paycom.

240. Paycom derived profits from Plaintiffs' and the Class's PII because it allowed them to provide services and derive revenue therefrom.

241. As such, a portion of the payments made to Paycom, which payments would not be possible without Plaintiffs and Class Members turning over their PII, was to be used to provide a reasonable and adequate level of data security that was in compliance with applicable state and federal regulations and industry standards. However, Paycom did not do this. Rather, Paycom retained the benefits of its unlawful conduct, including the amounts of payment received that should have been used for adequate cybersecurity practices that it

failed to provide.

242. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures, which would have secured Plaintiffs' and Class Members' PII and prevented the Data Incident.

243. If Plaintiffs and Class Members had known that Defendant would not adequately secure their PII, they would not have agreed to provide such PII.

244. Due to Defendant's conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendant to be permitted to retain the benefits of their wrongful conduct.

245. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered actual injury in the form of actual misuse of their PII and/or are at a substantial and continuous risk of suffering injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and theft of their PII now on sale across the dark web; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, 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 Incident, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains 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 their continued possession; and (vii) 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 Incident for the remainder of the lives of Plaintiffs and Class Members.

246. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

247. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF

248. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

249. This count is brought pursuant to 12 O.S. §§1651, *et seq.* on behalf of the Plaintiffs and the Oklahoma Subclass.

250. As previously alleged, Defendant owes duties of care to Plaintiff and the Class Members that require it to adequately secure and delete their PII.

251. Defendant still possesses the PII of Plaintiff and Class Members.

252. Defendant has not satisfied its obligations and legal duties to Plaintiff and the

Class Members.

253. Upon information and belief, Defendant is taking some steps to increase its data security but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Data Incident, and to once again place profits above protection.

254. Plaintiffs, therefore, seek a declaration that (1) Defendant's existing security measures and data retention/deletion policies do not comply with its contractual obligations and duties of care and (2) to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to stop its use of the MOVEit software;

b. Ordering Defendant to implement adequate data security and privacy measures in its use and selection of future service providers who receive customers' PII;

c. Ordering Defendant to significantly increase its spending on cybersecurity, including software, systems and personnel;

d. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring on future service providers used by Defendant;

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

f. Ordering that Defendant require future service providers to purge, delete, and destroy in a reasonably secure manner any PII not necessary

for its provision of services;

g. Ordering that Defendant require future service providers to conduct regular software scanning and security checks;

h. Ordering Defendant to guarantee future service providers are routinely and continually conducting internal training and education to inform their internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendant to require future service providers to implement and enforce adequate retention policies for PII, including destroying PII as soon as it is no longer necessary for it to be retained;

j. Ordering Defendant to meaningfully educate its employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves; and

k. Ordering that Defendant require future service providers to remove former customers' PII from any hard drive or server that has external (Internet) access.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action, defining the Class as

requested herein, and finding that Plaintiffs are proper representatives of the Nationwide Class and Oklahoma Subclass requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Date: July 2, 2024

Respectfully Submitted,

/s/: William B. Federman
William B. Federman, OBA #2853
Kennedy M. Brian, OBA # 34617
FEDERMAN & SHERWOOD
10205 N. Pennsylvania
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
kpb@federmanlaw.com

Attorneys for Plaintiffs and the Class

Exhibit 1

Return Mail Processing
PO Box 999
Suwanee, GA 30024

2 1 771 ********** AUTO**MIXED AADC **
CARMEN JOHNSON
[redacted]

July 31, 2023

Re: Notice of Progress' MOVEit Incident

Dear Carmen Johnson:

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To protect your identity, we are offering a complimentary 24-month membership of Experian®'s IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

[redacted]

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks

- **Experian credit report at signup:** See what information is associated with your credit file Daily credit reports are available for online members only [1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.[2]

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus, and assisting you with contacting government agencies to help restore your identity to its proper condition)

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 888-397-0091 toll-free Monday through Friday from 8 a.m. to 10 p.m Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S holidays). Be prepared to provide your engagement number B100009

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

[redacted]

[1] Offline members will be eligible to call for additional reports quarterly after enrolling

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company Please refer to the actual policies for terms, conditions, and exclusions of coverage Coverage may not be available in all jurisdictions

Steps You Can Take to Further Protect Your Information

Complimentary Identity Monitoring Services: We encourage you to activate the fraud detection and credit monitoring tools through Experian®'s IdentityWorks℠, which are provided as a complimentary 24-month membership. To start monitoring your personal information, please follow the steps above.

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
888-378-4329	888-397-3742	800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes), (2) Social Security number, (3) date of birth, (4) current address and previous addresses for the past five years, (5) proof of current address, such as a current utility bill, bank statement, or insurance statement, (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.), (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

Additional Information: You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Suite 110 South, Washington, D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

Maryland Residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

Massachusetts Residents: Under Massachusetts law, Massachusetts residents have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

[redacted]

New York Residents: New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information: the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583, 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina Residents: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/, or at: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400.

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 event. There is 1 Rhode Island resident impacted by this event.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, 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 violators. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

[redacted]

Return Mail Processing
PO Box 999
Suwanee, GA 30024

[redacted]

July 31, 2023

Re: Notice of Progress' MOVEit Incident

To the Parent or Guardian of A[redacted] J[redacted]

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To help protect your minor's identity, we are offering a complimentary 24-month membership of Experian®'s IdentityWorks℠. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

[redacted]

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts, assisting you in placing a freeze on your credit file with the three major credit bureaus, and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 888-397-0091 toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number [redacted].

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

[redacted]

Steps You Can Take to Further Protect Your Information

Complimentary Identity Monitoring Services: We encourage you to activate the fraud detection and credit monitoring tools through Experian®'s IdentityWorks℠, which are provided as a complimentary 24-month membership To start monitoring your personal information, please follow the steps above

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements and monitor your credit reports for suspicious activity Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U S law, you are entitled to one free credit report annually from each of the three major credit bureaus To obtain a free annual credit report, go to www annualcreditreport com or call 1-877-322-8228 You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months

Equifax
P O Box 740241
Atlanta, GA 30348
888-378-4329
www equifax com

Experian
P O Box 2002
Allen, TX 75013
888-397-3742
www experian com

TransUnion
P O Box 2000
Chester, PA 19022
800-916-8800
www transunion com

You should also know that you have the right to file a police report if you ever experience identity fraud Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim A police report is often required to dispute fraudulent items You can report suspected incidents of identity theft to local law enforcement or to the Attorney General

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization However please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail In order to request a security freeze, you will need to provide the following information (1) full name (including middle initial and any suffixes), (2) Social Security number; (3) date of birth, (4) current address and previous addresses for the past five years, (5) proof of current address, such as a current utility bill, bank statement, or insurance statement, (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc), (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles

You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes

Additional Information You can obtain additional information about the steps you can take to avoid identity theft from the following agencies The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www consumer gov/idtheft, 1-877-IDTHEFT (438-4338), TTY 1-866-653-4261

District of Columbia Residents You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D C 20001, https //www oag dc gov/, 1-202-727-3400

Maryland Residents You may contact the Office of the Maryland Attorney General, 200 St Paul Place, Baltimore, MD 21202, http //www marylandattorneygeneral gov, 1-888-743-0023 The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft

Massachusetts Residents Under Massachusetts law, Massachusetts residents have the right to obtain any police report filed in regard to this incident If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it

[redacted]

New York Residents New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany NY 12231-0001 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection, and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Residents North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400

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 event. There is 1 Rhode Island resident impacted by this event

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

New Mexico Residents You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, 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 FCRA not summarized here Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA We encourage you to review your rights pursuant to the FCRA by visiting https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf

[redacted]

Return Mail Processing
[redacted]
Suwanee GA [redacted]

[redacted]

July 31 2023

Re Notice of Progress' MOVEit Incident

To the Parent or Guardian of H[redacted] J[redacted]

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To help protect your minor's identity, we are offering a complimentary 24-month membership of Experian®'s IdentityWorks℠. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

[redacted]

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number on the Experian credit report
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts, assisting you in placing a freeze on your credit file with the three major credit bureaus, and assisting you with contacting government agencies to help restore your identity to its proper condition)

Please note that this Identity Restoration support is available to your minor for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 888-397-0091 toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number B100010

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

[redacted]

Steps You Can Take to Further Protect Your Information

Complimentary Identity Monitoring Services: We encourage you to activate the fraud detection and credit monitoring tools through Experian®'s IdentityWorks℠, which are provided as a complimentary 24-month membership To start monitoring your personal information, please follow the steps above

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission Under U S law, you are entitled to one free credit report annually from each of the three major credit bureaus To obtain a free annual credit report, go to www annualcreditreport com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months

Equifax
P O Box 740241
Atlanta, GA 30348
888-378-4329
www equifax com

Experian
P O Box 2002
Allen, TX 75013
888-397-3742
www experian com

TransUnion
P O Box 2000
Chester, PA 19022
800-916-8800
www transunion com

You should also know that you have the right to file a police report if you ever experience identity fraud Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim A police report is often required to dispute fraudulent items You can report suspected incidents of identity theft to local law enforcement or to the Attorney General

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail In order to request a security freeze, you will need to provide the following information (1) full name (including middle initial and any suffixes), (2) Social Security number, (3) date of birth, (4) current address and previous addresses for the past five years, (5) proof of current address, such as a current utility bill, bank statement, or insurance statement, (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc), (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles

You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes

Additional Information You can obtain additional information about the steps you can take to avoid identity theft from the following agencies The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580. www consumer gov/idtheft, 1-877-IDTHEFT (438-4338), TTY 1-866-653-4261

District of Columbia Residents You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D C 20001 https //www oag dc gov/, 1-202-727-3400

Maryland Residents You may contact the Office of the Maryland Attorney General, 200 St Paul Place, Baltimore, MD 21202, http //www marylandattorneygeneral gov 1-888-743-0023 The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft

Massachusetts Residents Under Massachusetts law, Massachusetts residents have the right to obtain any police report filed in regard to this incident If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it

[redacted]

New York Residents New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave, Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220 http://www.dos.ny.gov/consumerprotection, and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Residents North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400

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 event. There is 1 Rhode Island resident impacted by this event

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

New Mexico Residents You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, 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 FCRA not summarized here Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA We encourage you to review your rights pursuant to the FCRA by visiting https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf

[redacted]

Exhibit 2

[redacted]

AMY KELLER
[redacted]

July 31, 2023

Re Notice of Progress MOVEit Incident

Dear Amy Keller

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To protect your identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Engagement # [redacted]

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts, assisting you in placing a freeze on your credit file with the three major credit bureaus, and assisting you with contacting government agencies to help restore your identity to its proper condition).

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 888-397-0091 toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number B100009.

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You Can Take to Further Protect Your Information

Complimentary Identity Monitoring Services: We encourage you to enroll in free identity protection services by calling [redacted]. Experian's IdentityWorks℠, which are provided at no cost to you. For more information about these services, please follow the steps above.

Reviewing credit reports: It is recommended by state laws that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free annual credit report, please visit www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive free reports from one of the three credit bureaus every four months.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
888-378-4329	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: At no charge you can also have these credit bureaus place a 'fraud alert' on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two bureaus and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is designed to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) Full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement or insurance statement; (6) a legible photocopy of a government-issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

Additional Information: You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington DC, 20001, https://oag.dc.gov, 1-202-727-3400.

Maryland Residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

Massachusetts Residents: Under Massachusetts law, Massachusetts residents have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information: the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave, Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina Residents: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400.

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 event. There is 1 Rhode Island resident impacted by this event.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, 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 FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

[redacted]

July 31, 2023

Re: Notice of Progress' MOVEit Incident

To the Parent or Guardian of [redacted]

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's IdentityWorks℠. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll [redacted]
- Provide your **activation code**: [redacted]
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Engagement # [redacted]

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor.

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts, assisting you in placing a freeze on your credit file with the three major credit bureaus, and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 888-397-0091 toll-free Monday through Friday from 8 a.m. to 10 p.m. Central or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number B100010.

We regret any inconvenience caused by this incident.

Sincerely,

Payconn

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You Can Take to Further Protect Your Information

Complimentary Identity Monitoring Services: We encourage you to activate the fraud detection and credit monitoring tools through Experian®'s IdentityWorks℠, which are provided as a complimentary 24-month membership. To start monitoring your personal information, please follow the steps above.

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
888-378-4329	888-397-3742	800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

Additional Information You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

Maryland Residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

Massachusetts Residents: Under Massachusetts law, Massachusetts residents have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Engagement # [redacted]

New York Residents: New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information: the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina Residents: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/, or at: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400.

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 event. There are [illegible] Rhode Island resident impacted by this event.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, 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 "pre-screened" 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 FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Engagement # [redacted]

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

[redacted]

July 31, 2023

Re Notice of Progress' MOVEit Incident

To the Parent or Guardian of [redacted]

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To help protect your minor's identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Engagement # [redacted]

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 888-397-0091 toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number B100010.

We regret any inconvenience caused by this incident.

Sincerely,

[redacted]

dentity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant y. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all ions

Steps You Can Take to Further Protect Your Information

Complimentary Identity Monitoring Services: We encourage you to activate the fraud detection and credit monitoring tools through Experian's IdentityWorks℠, which are provided as a complimentary 24-month membership. To start monitoring your personal information, please follow the steps above.

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Equifax
P.O. Box 740241
Atlanta, GA 30348
888-378-4329
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-916-8800
www.transunion.com

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes), (2) Social Security number, (3) date of birth, (4) current address and previous addresses for the past five years, (5) proof of current address, such as a current utility bill, bank statement or insurance statement, (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.), (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

Additional Information: You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

Maryland Residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

Massachusetts Residents: Under Massachusetts law, Massachusetts residents have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information: the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583, 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina Residents: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/, or at: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400.

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 event. There is 1 Rhode Island resident impacted by this event.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, 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 violators. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Exhibit 3

Return Mail Processing
PO Box 999
Suwanee, GA 30024

[redacted]

July 31, 2023

Re: Notice of Progress' MOVEit Incident

To the Parent or Guardian of [redacted]

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To help protect your minor's identity, we are offering a complimentary 24-month membership of Experian®'s IdentityWorks℠. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Engagement # [redacted]

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at [redacted] toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number [redacted]

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

---

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You Can Take to Further Protect Your Information

Complimentary Identity Monitoring Services: We encourage you to activate the fraud detection and credit monitoring tools through Experian®'s IdentityWorks℠, which are provided as a complimentary 24-month membership. To start monitoring your personal information, please follow the steps above.

Reviewing credit reports: It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Equifax
P.O. Box 740241
Atlanta, GA 30348
888-378-4329
www equifax com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-916-8800
www.transunion.com

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Fraud Alerts: At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report at no cost to you. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) Social Security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

Additional Information. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

Maryland Residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

Massachusetts Residents: Under Massachusetts law, Massachusetts residents have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information: the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina Residents: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400.

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 event. There is 1 Rhode Island resident impacted by this event.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA, 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 FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Return Mail Processing
PO Box 999
Suwanee, GA 30024

[redacted]

July 31, 2023

Re: Notice of Progress' MOVEit Incident

To the Parent or Guardian of [redacted]

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To help protect your minor's identity, we are offering a complimentary 24-month membership of Experian®'s IdentityWorks℠. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Engagement # [redacted]

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at [redacted] toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number [redacted]

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

---

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Exhibit 4

Return Mail Processing
PO Box 999
Suwanee, GA 30024

11370 **********AUTO**MIXED AADC 300
SARAH OSGOOD
[redacted]

July 31, 2023

Re: Notice of Progress' MOVEit Incident

Dear Sarah Osgood:

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To protect your identity, we are offering a complimentary 24-month membership of Experian®'s IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your **activation code** [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0091 by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Engagement # B[redacted]

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.[2]

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 888-[redacted] toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number[redacted]

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.
[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Return Mail Processing
PO Box 999
Suwanee GA 30024

[redacted]

July 31, 2023

Re: Notice of Progress' MOVEit Incident

To the Parent or Guardian of [redacted]

Paycom values the privacy and confidentiality of our employees' and their dependents' personal information and takes the protection of that information very seriously. As you may have seen in the news, threat actors exploited a vulnerability in Progress Software Corporation's ("Progress") MOVEit software. Unfortunately, this recent data security incident involved some of our current and former employees' and their dependents' personal information.

What Happened? Progress announced a previously unknown zero-day vulnerability in its MOVEit software, a file transfer platform that allowed an unauthenticated attacker to gain access to MOVEit databases.

It has been widely publicized that threat actors exploited that vulnerability in Progress' MOVEit software, gaining unauthorized access to sensitive data stored on servers for numerous organizations, U.S. government agencies and others around the world that host the MOVEit software.

We recently learned the MOVEit server had been accessed by unauthorized attackers in connection with the MOVEit incident between May 28, 2023 and June 2, 2023.

What Information Was Involved? Depending on individual circumstances, the compromised files may have contained names, Social Security numbers, dates of birth, passport information, and employment authorization card information.

What We Are Doing. Paycom takes the privacy of your information seriously, and we are taking steps to prevent a similar occurrence. To help protect your minor's identity, we are offering a complimentary 24-month membership of Experian®'s IdentityWorks℠. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/minorplus**
- Provide your **activation code**: [redacted]
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by **November 30, 2023.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Engagement # [redacted]

ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0091. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by monitoring your financial account statements and reviewing your credit reports for suspicious activity.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 888-[redacted] toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Be prepared to provide your engagement number [redacted].

We regret any inconvenience caused by this incident.

Sincerely,

Paycom

---

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.