Exhibit A

UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
NORTHERN DIVISION

In re Kelly Benefits Data Breach Litigation	Case No. 1:25-cv-01304-SAG **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Dhymonique Alexander, Jasmine Anderson, Jacob Dohrman, Jaesyn Evans, Chasten Law, Anne O'Brien, Brittany Parks, and Kimberly Rose (collectively, "Plaintiffs") bring this Consolidated Class Action Complaint ("Complaint"), individually and on behalf of all others similarly situated, against Defendant Kelly & Associates Insurance Group, Inc. d/b/a Kelly Benefits ("Kelly Benefits" or "Defendant"), and allege, upon personal knowledge as to their own actions and upon information and belief based on their counsel's investigation and public records as to all other matters, as follows:

NATURE OF THE ACTION

1. This "hub-and-spoke" class action arises out of a data breach in which unauthorized third parties extracted and copied the sensitive Personally Identifiable Information ("PII"), including Social Security numbers, financial account information, tax ID information, medical data, and insurance information (collectively, "Private Information"), of more than 553,000 Class Members, including named Plaintiffs, from the computer network of Kelly Benefits between December 12, 2024 and December 17, 2024 (the "Data Breach").[1]

[1] Steve Alder, *Kelly Benefits Data Breach Update: More Than 553,000 Individuals Affected*, THE HIPAA J. (JULY 2, 2025), https://www.hipaajournal.com/kelly-benefits-data-breach/ (last visited Feb. 5, 2026).

2. The hub in this case is Kelly Benefits—one of the nation's largest providers of benefits administration and technology, broker and consulting services, and payroll solutions. During the ordinary course of its business, Kelly Benefits stores an enormous amount of Private Information collected from its clients (the "spokes") and their customers.

3. Defendant Kelly Benefits' clients used its services and software, and in doing so, entrusted Kelly Benefits with the most sensitive of Private Information of their employees. The volume of Private Information stored by Defendant on Kelly Benefits' systems and platform was enormous and, according to Kelly Benefits' Data Breach Notice, included a broad array of sensitive Private Information, including Social Security numbers, tax ID numbers, dates of birth, medical information, health insurance information, financial account information, and other sensitive, identifying information – information that is regularly used for identity theft and fraud.[2]

4. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the Private Information that it collected and maintained as part of its regular business practices.

5. Upon information and belief, current and former employees of Kelly Benefits' clients were and are required to entrust their employers with sensitive, non-public Private Information, including that of their family members ("Benefits Recipients"), which was then shared with Kelly Benefits. Without receiving this information from Plaintiffs' and Class Members' current and former employers, Defendant could not perform its regular business activities, in order to obtain and facilitate employment benefits programs. Defendant retains this information for many years and even after the employee-employer or client-benefits management relationship has ended.

[2] A compilation of the "Notice Letters" Plaintiffs received is attached hereto as ***Exhibit A***.

6. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect Benefits Recipients' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk of identity theft and fraud to victims of the Data Breach will remain for their respective lifetimes.

8. In breaching its duties to properly safeguard Plaintiffs' and Class Members' Private Information and give them timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and recklessness and violates federal and state laws.

9. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; (iii) secure its systems containing the Private Information using reasonable and effective security procedures; (iv) ensure that its staff, agents, and companies with whom it shared the Private Information utilized reasonable data security practices; and (v) promptly and adequately notify Plaintiffs and Class Members that their Private Information was impacted in the Data Breach.

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

11. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of the Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) emotional distress associated with the loss of control over their highly sensitive Private Information; (viii) nominal damages; and (ix) the continued and certainly impending increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information.

12. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose Private Information was

compromised and stolen as a result of the Data Breach and who have been harmed and remain at serious risk of harm due to Defendant's inadequate data security practices.

PARTIES

13. Plaintiff Dhymonique Alexander is a resident of Rockingham County, North Carolina, who is a Benefits Recipient who entrusted Kelly Benefits with her Private Information.

14. Plaintiff Jasmine Anderson is a resident of Kaufman County, Texas, who is a Benefits Recipient who entrusted Kelly Benefits with her Private Information.

15. Plaintiff Jacob Dohrman is a resident of Harford County, Maryland, who is a Benefits Recipient who entrusted Kelly Benefits with his Private Information.

16. Plaintiff Jaesyn Evans is a resident of Washington County, Maryland, who is a Benefits Recipient who entrusted Kelly Benefits with his Private Information.

17. Plaintiff Chasten Law is a resident of Alameda County, California, who is a Benefits Recipient who entrusted Kelly Benefits with his Private Information.

18. Plaintiff Anne O'Brien is a resident of Baltimore County, Maryland, who is a Benefits Recipient who entrusted Kelly Benefits with her Private Information.

19. Plaintiff Brittany Parks is a resident of Harford County, Maryland, who is a Benefits Recipient who entrusted Kelly Benefits with her Private Information.

20. Plaintiff Kimberly Rose is a resident of Dallas County, Texas, who is a Benefits Recipient who entrusted Kelly Benefits with her Private Information.

21. Defendant Kelly Benefits is a privately held insurance company with its headquarters and principal place of business in Baltimore County, Maryland. Kelly Benefits is organized and incorporated under its parent company, Kelly Services, Inc., under the laws of the

State of Delaware. Because Kelly Benefits has its headquarters and principal place of business in the State of Maryland, Kelly Benefits is a citizen of the States of both Maryland and Delaware.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 putative class members, and at least one Class Member is a citizen of a state that is diverse from any Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

23. This Court has personal jurisdiction over Defendant Kelly Benefits because it maintains its principal place of business in Maryland and regularly conducts substantial business in this District. Defendant has engaged in the conduct at issue in this District, and/or otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because: (a) a substantial part of the events or omissions giving rise to these claims occurred in this District, (b) Kelly Benefits maintains substantial operations in this District, (c) the conduct relevant to this action occurred in part within this District, and (d) Defendant has harmed Class members residing in this District.

FACTUAL ALLEGATIONS

Background on Defendant.

25. Kelly Benefits is a company that provides wide-ranging employee-benefit management services to its clients.

26. Plaintiffs and Class Members are current and former Benefits Recipients whose Private Information was provided to Kelly Benefits by their employers, all of whom are Kelly

Benefits' clients. Plaintiffs did not contract with Kelly Benefits directly but are third party beneficiaries of any such contracts.

27. Kelly Benefits touts its ability to seamlessly connect its clients' "current systems with Kelly Benefits' Total Benefits Solution® technology" to provide "a full suite of integrated business solutions."[3]

28. Kelly Benefits' proprietary Total Benefits Solution® technology ("KTBSonline") "offers a single point of entry for brokers, employers and employees" and "was designed by brokers and consultants with hundreds of years of combined experience in understanding the complexity and challenges of employee benefits management."[4]

29. Each of Kelly Benefits' clients stores the Private Information of their customers and/or employees on Kelly Benefits' platform through the use of Kelly Benefits' offered services and software.

30. Kelly Benefits' marketing demonstrates that it is well aware that data security is a key component of the services it provides to its customers. The following examples illustrate how Kelly Benefits markets and highlights the strength of its data security practices to entice customers to use Kelly Benefits' products and services, as well as Kelly Benefits' awareness of industry guidance and regulations that set standards for effective data security practices:

a. Kelly Benefits claims to "***maintain[] a robust information security program to ensure the protection and availability of our customers' sensitive data***. We have full-time Security Engineers on-staff and maintain relationships with a number of industry-leading security partners. With

[3] https://www.KellyBenefits.com/ (Last visited Jan. 6, 2026).
[4] *KTBSonline*, KELLY BENEFITS, https://kellybenefits.com/resources/ktbsonline/#:~:text=KTBSonline%2C%20Kelly%20Benefits%27%20proprietary%20Total%20Benefits%20Solution%C2%AE,complexity%20and%20challenges%20of%20employee%20benefits%20management.&text=Client%20Database%20and%20Eligibility%20Management%20System:%20Benefit,secure%20electronic%20billing%20payment%20and%20management%20options (Last visited Jan. 6, 2026).

these partners, we conduct a comprehensive annual assessment and penetration test of our systems."[5]

b. Kelly Benefits also claims that "[o]ur development environments only contain sanitized non-identifiable data, and our developers code against common attacks such as SQL injection."[6]

c. Kelly Benefits also advertises several industry protocols it purports to support, maintain and be accredited in, including SOC1 Type II, SOC2 Type II, and the NIST 800-53 standards.[7]

d. At the time of the Data Breach, Kelly Benefits' Privacy Policy represented its "firm commitment to protecting user privacy and sensitive user information."[8]

e. At the time of the Data Breach, Kelly Benefits' Privacy Policy also represented that "[w]e use reasonable care to protect your data from loss, misuse, unauthorized access, disclosure, alteration and untimely destruction…***Please be assured that the Site is equipped with security measures to protect the information you provide us***. Kelly Benefits processes user information in a proper method and takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of personal identifiable information."[9]

f. In the aftermath of the Data Breach, specifically last week, Kelly Benefits revised its Privacy Policy to, inter alia, remove language referencing its "firm commitment" to protect Personal Information.[10]

31. During the ordinary course of its business (primarily through the operation of its cloud-based databases and KTBSonline), Kelly Benefits receives the Private Information of individuals, such as Plaintiffs and the Class, from Kelly Benefits' clients. The Plaintiffs and Class have no say in what is provided to Kelly Benefits and how that access occurs.

---

[5] *Security*, KELLY BENEFITS, https://kellybenefits.com/resources/ktbsonline/security/ (Last visited Jan. 6, 2026).
[6] *Id.*
[7] *Id.*
[8] *Privacy Policy*, KELLY BENEFITS, https://kellybenefits.com/privacy-policy/ (Last visited Feb. 7, 2026).
[9] *Id.* (emphasis added).
[10] *Revised Privacy Policy*, KELLY BENEFITS, https://privacy.cptn.co/privacy-policy/a2240183-6850-499b-8cc5-d1eb033e4132 (Last visited Feb. 7, 2026).

32. Because cloud-based databases and software applications like KTBSonline are prime targets for cybercriminals due to the sheer volume of sensitive data they house and transfer, Kelly Benefits knew of the risks of a potential data breach. One recent report has highlighted the risks presented specifically by cloud storage as follows:[11]

> It is estimated that more than 60% of the world's corporate data is stored in the cloud. ***That makes the cloud a very attractive target for hackers. In 2023, over 80% of data breaches involved data stored in the cloud***. That is not just because the cloud is an attractive target. In many cases, ***it is also an easy target due to cloud misconfiguration*** – that is, companies unintentionally misuse the cloud, such as allowing excessively permissive cloud access, having unrestricted ports, and use unsecured backups.

33. In order to apply to obtain certain employment-related benefits with Defendant, Plaintiffs and Class Members were required to provide Defendant with their sensitive and confidential Private Information, including their names, dates of birth, and Social Security numbers.

34. The information held by Kelly Benefits in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

35. Upon information and belief, Defendant made promises and representations to Plaintiffs and Class Members, through their employers, that the Private Information collected from them as a condition of being Benefits Recipients would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it. Plaintiffs were third party beneficiaries of such promises.

36. Plaintiffs and Class Members provided their Private Information to Defendant through their employers with the reasonable expectation and on the mutual understanding that

[11] Stuart Madnick, *Why Data Breaches Spiked in 2023*, HARVARD BUS. REV. (FEB. 19, 2024), https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 (Last visited Jan. 6, 2026).

Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

37. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

38. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its clients', employees' and beneficiaries' Private Information safe and confidential.

39. Defendant had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiffs' and Class Members' employers, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

40. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

41. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

The Data Breach.

42. Starting on or about April 9, 2025, Kelly Benefits began sending Plaintiffs and other victims of the Data Breach a letter (the "Notice Letter"), informing them as follows:

> **What Happened?** Kelly Benefits recently learned of suspicious activity within our environment. . . . Our investigation determined our environment was subject to unauthorized access between December 12, 2024 and December 17, 2024 and certain files were copied and taken. . . . You are receiving this letter because, on March 3, 2025 we completed this review and determined that your information was present in one or more of the impacted files. . . .
>
> **What Information Was Involved?** Kelly Benefits determined that the following information related to you was present on the impacted files: your name and Social Security number, health or insurance group ID number. [12]

43. The occurrence of the Data Breach has resulted in numerous injuries suffered by Plaintiffs and the Class, which were exacerbated by several deficiencies in Kelly Benefits' Data Breach notification letter, including: (1) Kelly Benefits waited ***four months*** to provide notice to Plaintiffs and Class members of the Data Breach; (2) Kelly Benefits failed to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Kelly Benefits continues to maintain is secure; and (3) Kelly Benefits failed to provide details concerning how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in the Data Breach.

44. Furthermore, Defendant's delay in notifying Plaintiffs and Class Members of the Data Breach is in direct violation of Defendant's responsibilities under the data breach notification statute in Maryland, *see* Md. Code Com. Law § 14-3504 (b)(3), which requires that the disclosure notification be made "as soon as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach". Defendant missed this deadline by over 70 days.

[12] *See* ***Exhibit A***.

45. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

46. The attacker targeted, accessed, and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiffs and Class Members, including their names, Social Security numbers, tax ID, and insurance ID information. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

47. Plaintiffs' Private Information from this breach was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type. Moreover, several Plaintiffs allege below that they have already been notified that their Private Information was found on the dark web following the Data Breach despite assurances from Kelly Benefits that no such disclosure had occurred.

Data Breaches Are Preventable.

48. Defendant could have prevented this Data Breach by, among other things, properly encrypting files containing the Private Information, protecting its equipment and networks with adequate firewalls, requiring multifactor authentication to access networks containing Private Information, training and monitoring their staff to ensure compliance with adequate data security measures.

49. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[13]

[13] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

50. To prevent and detect cyber-attacks, Defendant could and should have implemented a number of measures as recommended by the United States Government.[14]

51. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented measures recommended by the Microsoft Threat Protection Intelligence Team, including securing internet facing assets, including IT pros in security discussions, and applying the principle of least-privilege.[15]

52. Given that Defendant was storing the sensitive Private Information of its clients' Benefits Recipients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

53. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, hundreds of thousands of individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Benefits Recipients' Private Information

54. As a condition of being Benefits Recipients, Plaintiffs and Class Members were required to give their sensitive and confidential Private Information to Defendant.

55. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its services.

[14] *E.g. Id.* at 3-4.
[15] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

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

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

58. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

Defendant Knew or Should Have Known of the Risk Because Employee-Benefit Management Companies in Possession of Private Information are Particularly Susceptible to Cyber Attacks.

59. Data thieves regularly target companies like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

60. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store Private Information and other sensitive information, like Defendant, preceding the date of the breach.

61. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[16] Of the 3,205 recorded data compromises, 809 of them, or

[16] *See 2023 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024);

25.2%, were in the medical or healthcare industry.[17] The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points.[18] The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.[19]

62. Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

63. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

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

65. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to hundreds of thousands of individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data[20].

---

https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf .

[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/047b774f-2e79-4a04-9f4c-4dd7a8b2ee8d.html(last visited April 15, 2025).

66. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft or financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' Private Information. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

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

68. As an employee-benefit management company in possession of Benefits Recipients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendant Fail to Comply with FTC Guidelines.

69. 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.

70. In 2016, the FTC updated their publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines

note that businesses should protect the personal employee 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.[21]

71. 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 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.[22]

72. The FTC further recommends that companies not maintain Private Information 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 for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

73. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect employee data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[21] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[22] *Id.*

74. These FTC enforcement actions include actions against employee-benefit management companies, like Defendant.

75. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

76. Defendant failed to properly implement basic data security practices.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information in its possession, and was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails to Comply with Industry Standards.

79. As noted above, experts studying cybersecurity routinely identify employee-benefit management companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

80. Several best practices have been identified that, at a minimum, should be implemented by employee-benefit management companies in possession of Private Information,

like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

81. Other best cybersecurity practices that are standard for employee-benefit management companies include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points. On information and belief, Defendant failed to follow these cybersecurity best practices, including failure to train staff.

82. On information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

83. These foregoing frameworks are existing and applicable industry standards for employee-benefit management companies safeguarding their employees' data, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

84. In addition to the general data security standards described above, numerous authorities have issued guidance specific to cloud data storage, defining the roles and responsibilities of cloud service providers like Kelly Benefits.

i. Governmental Authorities

85. In June 2020, the FTC published an article titled, *Six steps toward more secure cloud computing.* The article warned, "[a]s cloud computing has become business as usual for many businesses, frequent news reports about data breaches and other missteps should make companies think carefully about how they secure their data." The article expressly highlighted the importance of MFA in protecting consumer data stored on cloud services, recommending businesses: "Require multi-factor authentication and strong passwords to protect against the risk of unauthorized access."[23]

86. In March 2023, the FTC issued a Request for Information seeking public comment on "Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security."[24] After reviewing over 100 public comments on the issue, the FTC published a report in November 2023 titled, *Cloud Computing RFI: What we heard and learned.* The report expressly flagged the room for improvement in cloud security as follows: "[A] a number of commenters argued there is a great deal of room for improvement in cloud security; that default security configurations could be better; and that the "shared responsibility" model for cloud security often

[23] Elisa Jillson & Andy Hasty, *Six steps toward more secure cloud computing*, FED. TRADE COMM'N (JUNE 15, 2020), https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing (Last visited Jan. 6, 2026).

[24] *FTC Seeks Comment on Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security*, FED. TRADE COMM'N (MAR. 22, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-seeks-comment-business-practices-cloud-computing-providers-could-impact-competition-data (Last visited Jan. 6, 2026).

lacks clarity, which can lead to situations where neither the cloud provider nor the cloud customer implements necessary safeguards."[25]

87. In March 2024, the U.S. National Security Agency and Cybersecurity & Infrastructure Agency issued a joint publication titled, *Use Secure Cloud Identity and Access Management Practices.* The publication warned, "[a]s organizations continue to migrate to using cloud environments, these environments are becoming increasingly valuable targets for malicious cyber actors[.]" The publication made numerous recommendations relevant to MFA, rotating credentials, and restricting allow lists to ensure only necessary privileges are granted to users:

> a. **Multifactor authentication.** Single-factor authentication (e.g., password or PIN only) based account access is susceptible to credential theft, forgery, and reuse across multiple systems. Cloud accounts are generally globally accessible; thus they are more susceptible to certain types of single-factor authentication weaknesses. Multifactor authentication (MFA) boosts account security, better resisting compromise by enhancing user verification methods. MFA requires two or more factors for login: something the user knows, has, or is. Typically this is implemented using a password and a second factor usually based on a randomly seeded numeric token, a biometric option (such as a fingerprint or facial recognition), or a physical token (unique hardware-based identifier: smartcard, Common Access Card, etc.).
>
> b. Periodically audit IAM configurations to confirm only necessary privileges are granted to users. Many CSPs [Cloud Service Providers] offer services that will track unused privileges to help admins tailor accounts to the least privileges users need to accomplish their day-to-day responsibilities.

88. Also in March 2024, NSA separately issued a publication titled, *NSA's Top Ten Cloud Security Mitigation Strategies.* The publication emphasized the importance of MFA,

[25] Nick Jones, *Cloud Computing RFI: What we heard and learned*, FED. TRADE COMM'N (NOV. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/cloud-computing-rfi-what-we-heard-learned (Last visited Jan. 6, 2026).

credential rotation, and restricted allow lists as follows for customers using cloud data services as follows:[26]

> Proper identity and access management (IAM) are critical to securing cloud resources. Malicious actors can compromise accounts using phishing techniques, exposed credentials, or weak authentication practices to gain initial access into cloud tenants. They can also exploit overly broad access control policies to penetrate further into the environment, gaining access to sensitive resources. To prevent this, cloud users should use secure authentication methods such as phishing-resistant multifactor authentication (MFA) and properly managed temporary credentials. Access control policies should be carefully configured to ensure users are granted the least privileges necessary. Separation of duties should be implemented to protect especially sensitive operations and resources.

ii. **Industry Standards**

89. The PCI Data Security Council has issued an April 2018 supplement to the PCI DSS titled, *Cloud Computing Guidelines.*[27] The PCI Cloud Computing Guidelines again emphasize the importance of MFA, providing: "PCI DSS Requirement 8.2.2 requires multi-factor authentication for all remote network access to the CDE [cardholder data environment], and when public cloud services are part of a Customer's CDE, all such access will be considered remote access and will require multi-factor authentication.

90. The PCI Cloud Computing Guidelines includes a section titled *Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)*, which provides: "As the Customer's access to network level data can be severely restricted in cloud environments, the responsibility for tracking intrusions at the network layer will often reside with the Provider, as the only entity that has sufficient privileges to do this across the underlying infrastructure." The guidelines go on to note

[26] *NSA's Top Ten Cloud Security Mitigation Strategies*, NATL SEC'Y AGENCY, https://media.defense.gov/2024/Mar/07/2003407860/-1/-1/0/CSI-CloudTop10-Mitigation-Strategies.PDF (Last visited Jan. 6, 2026).
[27] *Information Supplement: PCI SSC Cloud Computing Guidelines*, https://listings.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf (Last visited Jan. 6, 2026).

that for SaaS providers such as Kelly Benefits: "Since customer access to low level network traffic is impossible, it must rely on Providers for IDS/IPS, monitoring and alerting."[28]

91. The Center for Internet Security ("CIS") is a non-profit organization that develops globally recognized best practices for securing IT systems and data. In March 2022, CIS issued a publication entitled *CIS Controls Cloud Companion Guide* that provided guidance on security best practices for customers using cloud services. The guidance made the following recommendations emphasizing the importance of MFA and revoking access to stale credentials:

a. **Disable Dormant Accounts.** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

b. **Establish an Access Revoking Process.** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

c. **Require MFA for Administrative Access.** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

92. ISO/IEC 27017 is an international standard that "provides controls and implementation guidance for both cloud service providers and cloud service customers."[29] Control 9.2.3 specifically highlights that cloud service providers (like Kelly Benefits) should provide MFA capabilities as follows:

Cloud service provider
The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the

[28] *Id.*

[29] *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027017-2015.pdf (Last visited Jan. 6, 2026).

> administrative capabilities of a cloud service, according to the identified risks. For example, the cloud service provider can provide multi-factor authentication capabilities or enable the use of third-party multi-factor authentication mechanisms.

a. Defendant Owed a Duty of Care to Plaintiff and Class Members and Breached that Duty.

93. The Private Information of Plaintiff and Class Members was stored on Defendant's platforms, networks, systems or products at the time of the Data Breach.

94. Defendant owed common law duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendant's possession from being compromised, accessed, stolen, or misused by unauthorized parties.

95. Defendant Kelly Benefits' duty of reasonable care is established due to the nature of its business, which is to provide *secure* human resources and benefits administration via its proprietary KTBSonline software to customers, and store massive amounts of data, including Plaintiffs' and Class Members' Private Information. In offering and undertaking these services to customers, Kelly Benefits had a duty to exercise reasonable care to safeguard Plaintiffs' and Class Members' Private Information because it was foreseeable that failure to do so would cause them injury.

96. Kelly Benefits' duty of reasonable care is established by governmental regulations and industry guidance establishing industry standards for data security to safeguard the Private Information it stored.

97. Kelly Benefits' duty of reasonable care is also established by its own marketing statements and Privacy Policy, which hold out its secure provision of services.

98. Kelly Benefits' duty of reasonable care is also established by relevant common law.

99. Kelly Benefits breached its duties to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information by failing to implement adequate data security practices, which caused the Data Breach.

100. Kelly Benefits was negligent and breached its duty of care to Plaintiffs and Class Members to protect their Private Information from exploitation via customers' use of KTBSonline.

101. Kelly Benefits' breach of its duty of care caused the Data Breach, because if Kelly Benefits had maintained adequate data security, the Data Breach could have been prevented.

102. Kelly Benefits' data security failings also constitute an unfair trade practice. As discussed above, the FTC's enforcement actions have established that a company's failure to maintain reasonable and appropriate data security of PII violates the FTC Act's prohibition on "unfair and deceptive acts."

103. Kelly Benefits' breach of its duty of care and engagement in unfair trade practices caused injury to Plaintiffs and Class Members.

104. Kelly Benefits is liable for the injuries suffered by Plaintiffs and Class Members by virtue of its role as the proprietary owner and administrator of KTBSonline, which was used to facilitate the transfer of and store the data of its affected customers, including Defendant.

The Data Breach Increases Victims' Risk of Identity Theft.

105. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

106. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs

and Class Members. Simply put, unauthorized individuals can now easily access the Private Information of Plaintiffs and Class Members.

107. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

108. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

109. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[30]

110. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into

[30] *See* N.C. Gen. Stat. § 132-1.10(1).

their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[31]

111. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[32] Accordingly, because Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[33]

112. The exposure of Social Security numbers is not the sole risk Plaintiffs and Class Members are now exposed to. When combined with other publicly available data, any PII element can be used to build full identity profiles, known as "Fullz" packages, which are frequently exploited in financial fraud schemes. "Fullz" is fraudster-speak for data that includes a victim's information, including name, address, SSN, date of birth, and more.

113. With Fullz packages, cybercriminals can cross-reference two (or more) sources of PII to marry unregulated data available elsewhere (e.g., address or phone number) to criminally stolen data to assemble shockingly accurate and complete dossiers on individuals.

114. Compromised PII, whether alone or as part of a Fullz package, is highly valuable to cybercriminals, who can use it to engage in a wide range of fraudulent activities, including

---

[31] *See* Hussayn Kassai, *BankThink Banks need to stop relying on Social Security numbers*, AM. BANKER (NOV. 12, 2018), https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers (last visited Feb. 5, 2026).

[32] *See* Ann Carns, *Just 5 Banks Prohibit Use of Social Security Numbers*, N.Y. TIMES (MAR. 20, 2013), https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/ (last visited Feb. 5, 2026).

[33] *See What Can Someone Do With Your Social Security Number?*, CREDIT.COM (OCT. 19, 2023), https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Feb. 5, 2026).

committing unemployment insurance fraud, opening unauthorized financial accounts, and applying for government benefits.

115. This type of identity theft renders any compromised data—including seemingly innocuous PII, such as name and contact information—valuable. In the wrong hands, up-to-date names, addresses, phone numbers, and email addresses can be used to update, validate, and verify Fullz packages, which can then be used for nefarious purposes.

116. For example, a criminal actor can use an up-to-date Fullz package to bypass identity verification tools—which are often used in financial transactions (like loan applications), background checks, etc.—without detection. In a typical identity verification system, a user submits their PII, like their name, addresses, or date of birth. That customer-submitted PII is then cross-checked against "a trusted data set," including those from "credit bureaus, official government documents or mobile operator databases."

117. Thus, with an up-to-date Fullz package—which might include seemingly harmless information, like the identity theft victim's name and current address—a cybercriminal has the victim's up-to-date PII, which will match the victim's information from trusted data sources, like the credit bureaus. With this information, the criminal can then successfully pass identity verification systems without raising any red flags. In this way, Fullz packages, which are made possible by up-to-date and compromised elements of PII, enable fraudsters to carry out various forms of identity theft, including taking out fraudulent loans.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud.

118. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, a reasonable person is expected to take steps and spend time to address the dangerous

situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

119. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiffs and Class Members to protect themselves by reviewing account statements and monitoring their credit reports, in addition to enrolling in the offered free credit monitoring program.

120. Defendant's extensive suggestion of steps that Plaintiffs and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs' and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiffs and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant's Notice Letter.

121. Plaintiffs and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, freezing their payment cards, contacting credit bureaus to place freezes on their accounts, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

122. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

123. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

124. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

Diminution of Value of Private Information.

125. Private Information is a valuable property right.[36] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

[34] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[35] *See* FEDERAL TRADE COMMISSION, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[36] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

126. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[37]

127. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[38] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[39,40] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive cash rewards, including eligibility for $500 monthly prizes. [41]

128. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by their compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

129. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the

---

[37] *See, e.g.*, John T. Soma, *et al.*, C*orporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted)..

[38] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[39] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, L.A. TIMES (NOV. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Feb. 5, 2026).

[40] DATACOUP, https://datacoup.com/ (last visited Feb. 5, 2026).

[41] https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (last visited Feb. 7, 2026).

foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

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

132. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, upon information and belief, thousands to tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

Future Costs of Credit and Identity Theft Monitoring is Reasonable and Necessary.

134. Given the type of targeted attack, the sophisticated criminal activity, and the type of Private Information involved in this case, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

135. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employee-benefit management company of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

136. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

137. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain.

138. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. In connection with receiving benefits under their contracts for employment, Plaintiffs and other reasonable employees understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant's clients.

Plaintiffs' Experiences and Injuries

Plaintiff Alexander

139. Plaintiff Alexander is a Benefits Recipient who was required to provide her Private Information to Defendant as a condition of her employment and to receive services from Kelly Benefits.

140. Upon information and belief, Ms. Alexander's Private Information was stolen from Kelly Benefits' systems, networks, and/or software in the Data Breach.

141. Kelly Benefits possessed Ms. Alexander's Private Information before, during, and after the Data Breach.

142. Because of the Data Breach, Ms. Alexander's confidential Private Information is in the hands of cybercriminals. As such, Ms. Alexander and other Class Members are at imminent risk of identity theft and fraud.

143. As a result of the Data Breach, Ms. Alexander must expend hours of her time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

144. Ms. Alexander places significant value on the security of her Private Information and does not readily disclose it. Ms. Alexander has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

145. Ms. Alexander has 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 Private Information compromised by the Data Breach. Indeed, following the Data Breach, a fraudulent account was opened in Ms. Alexander's name and she received notice that some of her Private Information has been found on the dark web.

146. Ms. Alexander has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Kelly Benefits is protected and

safeguarded from future data breaches. Absent court intervention, Ms. Alexander's and Class Members' Private Information will be wholly unprotected and at-risk of future data breaches.

147. As a direct and traceable result of the Data Breach, Ms. Alexander suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kelly Benefits' possession and is subject to further unauthorized disclosures so long as Kelly Benefits fails to undertake appropriate and adequate measures to protect her Private Information.

148. The Data Breach has caused Ms. Alexander to suffer fear, anxiety, and stress, which has been compounded by the fact that Kelly Benefits has still not informed her of key details about the Data Breach.

Plaintiff Anderson

149. Plaintiff Anderson is a Benefits Recipient who was required to provide her Private Information to Defendant as a condition of her employment and to receive services from Kelly Benefits.

150. Upon information and belief, Ms. Anderson's Private Information was stolen from Kelly Benefits' systems, networks, and/or software in the Data Breach.

151. Kelly Benefits possessed Ms. Anderson's Private Information before, during, and after the Data Breach.

152. Because of the Data Breach, Ms. Anderson's confidential Private Information is in the hands of cybercriminals. As such, Ms. Anderson and other Class Members are at imminent risk of identity theft and fraud.

153. As a result of the Data Breach, Ms. Anderson must expend hours of her time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

154. Ms. Anderson places significant value on the security of her Private Information and does not readily disclose it. Ms. Anderson has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

155. Ms. Anderson has 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 Private Information compromised by the Data Breach. Indeed, following the Data Breach, multiple fraudulent charges were made on one of her financial accounts and unknown individuals applied for loans that appeared on her credit report.

156. Ms. Anderson has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Kelly Benefits, is protected and safeguarded from future data breaches. Absent court intervention, Ms. Anderson's and Class Members' Private Information will be wholly unprotected and at-risk of future data breaches.

157. As a direct and traceable result of the Data Breach, Ms. Anderson suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data

Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kelly Benefits' possession and is subject to further unauthorized disclosures so long as Kelly Benefits fails to undertake appropriate and adequate measures to protect her Private Information.

158. The Data Breach has caused Ms. Anderson to suffer fear, anxiety, and stress, which has been compounded by the fact that Kelly Benefits has still not informed her of key details about the Data Breach.

Plaintiff Dohrman

159. Plaintiff Dohrman is a Benefits Recipient who was required to provide his Private Information to Defendant as a condition of his employment and to receive services from Kelly Benefits.

160. Upon information and belief, Mr. Dohrman's Private Information was stolen from Kelly Benefits' systems, networks, and/or software in the Data Breach.

161. Kelly Benefits possessed Mr. Dohrman's Private Information before, during, and after the Data Breach.

162. Because of the Data Breach, Mr. Dohrman's confidential Private Information is in the hands of cybercriminals. As such, Mr. Dohrman and other Class Members are at imminent risk of identity theft and fraud.

163. As a result of the Data Breach, Mr. Dohrman must expend hours of his time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

164. Mr. Dohrman places significant value on the security of his Private Information and does not readily disclose it. Mr. Dohrman has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

165. Mr. Dohrman has 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 Private Information compromised by the Data Breach. Indeed, following the Data Breach, Mr. Dohrman received notice that some of his Private Information has been found on the dark web.

166. Mr. Dohrman has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Kelly Benefits, is protected and safeguarded from future data breaches. Absent court intervention, Mr. Dohrman's and Class Members' Private Information will be wholly unprotected and at-risk of future data breaches.

167. As a direct and traceable result of the Data Breach, Mr. Dohrman suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of his Private Information; (iii) lost or diminished value of his Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to his Private

Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kelly Benefits' possession and is subject to further unauthorized disclosures so long as Kelly Benefits fails to undertake appropriate and adequate measures to protect his Private Information.

168. The Data Breach has caused Mr. Dohrman to suffer fear, anxiety, and stress, which has been compounded by the fact that Kelly Benefits has still not informed him of key details about the Data Breach.

Plaintiff Evans

169. Plaintiff Evans is a Benefits Recipient who was required to provide his Private Information to Defendant as a condition of his employment and to receive services from Kelly Benefits.

170. Upon information and belief, Mr. Evans's Private Information was stolen from Kelly Benefits' systems, networks, and/or software in the Data Breach.

171. Kelly Benefits possessed Mr. Evans's Private Information before, during, and after the Data Breach.

172. Because of the Data Breach, Mr. Evans's confidential Private Information is in the hands of cybercriminals. As such, Mr. Evans and other Class Members are at imminent risk of identity theft and fraud.

173. As a result of the Data Breach, Mr. Evans must expend hours of his time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

174. Mr. Evans places significant value on the security of his Private Information and does not readily disclose it. Mr. Evans has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

175. Mr. Evans has 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 Private Information compromised by the Data Breach. Indeed, following the Data Breach, Mr. Evans has experienced multiple unauthorized bank charges.

176. Mr. Evans has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Kelly Benefits, is protected and safeguarded from future data breaches. Absent court intervention, Mr. Evans's and Class Members' Private Information will be wholly unprotected and at-risk of future data breaches.

177. As a direct and traceable result of the Data Breach, Mr. Evans suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of his Private Information; (iii) lost or diminished value of his Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kelly Benefits' possession and is subject to further unauthorized disclosures so long as Kelly Benefits fails to undertake appropriate and adequate measures to protect his Private Information.

178. The Data Breach has caused Mr. Evans to suffer fear, anxiety, and stress, which has been compounded by the fact that Kelly Benefits has still not informed him of key details about the Data Breach.

Plaintiff Law

179. Plaintiff Law is a Benefits Recipient who was required to provide his Private Information to Defendant as a condition of his employment and to receive services from Kelly Benefits.

180. Upon information and belief, Mr. Law's Private Information was stolen from Kelly Benefits' systems, networks, and/or software in the Data Breach.

181. Kelly Benefits possessed Mr. Law's Private Information before, during, and after the Data Breach.

182. Because of the Data Breach, Mr. Law's confidential Private Information is in the hands of cybercriminals. As such, Mr. Law and other Class Members are at imminent risk of identity theft and fraud.

183. As a result of the Data Breach, Mr. Law must expend hours of his time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

184. Mr. Law places significant value on the security of his Private Information and does not readily disclose it. Mr. Law has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

185. Mr. Law has 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 Private Information compromised by the Data Breach. Indeed, following the Data Breach, Mr. Law has experienced attempts to login into his accounts.

186. Mr. Law has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Kelly Benefits, is protected and safeguarded from future data breaches. Absent court intervention, Mr. Law's and Class Members' Private Information will be wholly unprotected and at-risk of future data breaches.

187. As a direct and traceable result of the Data Breach, Mr. Law suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of his Private Information; (iii) lost or diminished value of his Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kelly Benefits' possession and is subject to further unauthorized disclosures so long as Kelly Benefits fails to undertake appropriate and adequate measures to protect his Private Information.

188. The Data Breach has caused Mr. Law to suffer fear, anxiety, and stress, which has been compounded by the fact that Kelly Benefits has still not informed him of key details about the Data Breach.

Plaintiff O'Brien

189. Plaintiff O'Brien is a Benefits Recipient who was required to provide her Private Information to Defendant as a condition of her employment and to receive services from Kelly Benefits..

190. Upon information and belief, Ms. O'Brien's Private Information was stolen from Kelly Benefits' systems, networks, and/or software in the Data Breach.

191. Kelly Benefits possessed Ms. O'Brien's Private Information before, during, and after the Data Breach.

192. Because of the Data Breach, Ms. O'Brien's confidential Private Information is in the hands of cybercriminals. As such, Ms. O'Brien and other Class Members are at imminent risk of identity theft and fraud.

193. As a result of the Data Breach, Ms. O'Brien must expend hours of her time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

194. Ms. O'Brien places significant value on the security of her Private Information and does not readily disclose it. Ms. O'Brien has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

195. Ms. O'Brien has 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 Private Information compromised by the Data Breach. Indeed, Ms. O'Brien had four fraudulent attempted charges on

her Chase Bank credit card, on March 24, 2025, July 3, 2025, July 13, 2025 and August 4, 2025, totaling over $3600, from four different vendors including Microsoft and Cebu Air, Inc.

196. Ms. O'Brien has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Kelly Benefits, is protected and safeguarded from future data breaches. Absent court intervention, Ms. O'Brien's and Class Members' Private Information will be wholly unprotected and at-risk of future data breaches.

197. As a direct and traceable result of the Data Breach, Ms. O'Brien suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kelly Benefits' possession and is subject to further unauthorized disclosures so long as Kelly Benefits fails to undertake appropriate and adequate measures to protect her Private Information.

198. The Data Breach has caused Ms. O'Brien to suffer fear, anxiety, and stress, which has been compounded by the fact that Kelly Benefits has still not informed her of key details about the Data Breach.

Plaintiff Parks

199. Plaintiff Parks is a Benefits Recipient who was required to provide her Private Information to Defendant as a condition of her employment and to receive services from Kelly Benefits.

200. Upon information and belief, Ms. Parks' Private Information was stolen from Kelly Benefits' and systems, networks, and/or software in the Data Breach.

201. Kelly Benefits possessed Ms. Parks' Private Information before, during, and after the Data Breach.

202. Because of the Data Breach, Ms. Parks' confidential Private Information is in the hands of cybercriminals. As such, Ms. Parks and other Class Members are at imminent risk of identity theft and fraud.

203. As a result of the Data Breach, Ms. Parks must expend hours of her time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

204. Ms. Parks places significant value on the security of her Private Information and does not readily disclose it. Ms. Parks has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

205. Ms. Parks has 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 Private Information compromised by the Data Breach. Indeed, in March 2025, three fraudulent charges were made on Ms. Parks' M&T Bank debit card that resulted in overdrafts of her bank account and the imposition of multiple late fees by M&T Bank, which Ms. Parks had to expend time disputing. Ms. Parks also incurred unreimbursed late fees in March 2025 from two creditors totaling $75, which were the result of the aforementioned fraudulent overdrafts of her bank account.

206. Ms. Parks has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Kelly Benefits, is protected and safeguarded from future data breaches. Absent court intervention, Ms. Parks' and Class Members' Private Information will be wholly unprotected and at-risk of future data breaches.

207. As a direct and traceable result of the Data Breach, Ms. Parks suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kelly Benefits' possession and is subject to further unauthorized disclosures so long as Kelly Benefits fails to undertake appropriate and adequate measures to protect her Private Information.

208. The Data Breach has caused Ms. Parks to suffer fear, anxiety, and stress, which has been compounded by the fact that Kelly Benefits has still not informed her of key details about the Data Breach.

Plaintiff Rose

209. Plaintiff Rose is a Benefits Recipient who was required to provide her Private Information to Defendant as a condition of her employment and to receive services from Kelly Benefits..

210. Upon information and belief, Ms. Rose's Private Information was stolen from Kelly Benefits' systems, networks, and/or software in the Data Breach.

211. Kelly Benefits possessed Ms. Rose's Private Information before, during, and after the Data Breach.

212. Because of the Data Breach, Ms. Rose's confidential Private Information is in the hands of cybercriminals. As such, Ms. Rose and other Class Members are at imminent risk of identity theft and fraud.

213. As a result of the Data Breach, Ms. Rose must expend hours of her time and suffer loss of productivity addressing and attempting to ameliorate and mitigate the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

214. Ms. Rose places significant value on the security of her Private Information and does not readily disclose it. Ms. Rose has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

215. Ms. Rose has 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 Private Information compromised by the Data Breach. Indeed, following the Data Breach, she received notice that some of her Private Information has been found on the dark web.

216. Ms. Rose has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Kelly Benefits, is protected and safeguarded from future data breaches. Absent court intervention, Ms. Rose's and Class Members' Private Information will be wholly unprotected and at-risk of future data breaches.

217. As a direct and traceable result of the Data Breach, Ms. Rose suffered actual injury as a result of the unauthorized access and disclosure of her Private Information in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of her Private Information; (iii) lost or diminished value of her Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kelly Benefits' and possession and is subject to further unauthorized disclosures so long as Kelly Benefits fails to undertake appropriate and adequate measures to protect her Private Information.

218. The Data Breach has caused Ms. Rose to suffer fear, anxiety, and stress, which has been compounded by the fact that Kelly Benefits has still not informed her of key details about the Data Breach.

CLASS ACTION ALLEGATIONS

219. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Federal Rule of Civil Procedure 23.

220. The Classes that Plaintiffs seek to represent are defined as follows:

Nationwide Class: All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach, including those who received notice of the Data Breach.

California Subclass: All individuals residing in the State of California whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach, including those who received notice of the Data Breach.

Maryland Subclass: All individuals residing in the State of Maryland whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach, including those who received notice of the Data Breach.

221. Collectively, the Class and Subclasses are referred to as the "Classes" or "Class Members."

222. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

223. Plaintiffs reserve the right to amend the definitions of the Classes or Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

224. The proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

225. Numerosity. The Class Members are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, hundreds of thousands of individuals were impacted. The Classes are apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

226. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class members, including the following:

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

b. Whether Defendant had a duty not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

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

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

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

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

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

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

227. Typicality. Plaintiffs' claims are typical of those of the other members of the Classes because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Classes.

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

229. Adequacy. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringements of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

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

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

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

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

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

235. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

236. Likewise, particular issues under Rule 23(c)(2) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiffs and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard their clients' employees' Private Information; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
NEGLIGENCE & NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class)

237. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the foregoing paragraphs, as if fully set forth herein.

238. Defendant requires Benefits Recipients, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

239. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its clients, which solicitations and services affect commerce.

240. Plaintiffs and Class Members entrusted Defendant with their Private Information with the reasonable and mutual understanding that Defendant would safeguard their information.

241. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

242. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, to ensure that third parties to whom they provided the Private Information did the same, and to safeguard the information from theft.

243. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

244. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which 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.

245. Defendant's duty to use reasonable data security measures includes, among other things: (a) designing, maintaining, and testing its security protocols to ensure that the Private

Information of Plaintiffs and Class Members is adequately secured and protected; (b) removing or deleting sensitive data when no longer needed for authorized purposes; and (c) implementing and maintaining procedures to detect and prevent improper access to and misuse of Plaintiffs' and Class Members' Private Information.

246. Defendant 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 and networks, and the personnel responsible for them, adequately protected the Private Information.

247. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining employment at Defendant's clients and/or receiving benefits managed by Defendant.

248. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Defendant stored valuable Private Information that is routinely targeted by cybercriminals. Plaintiffs and Class Members were the foreseeable and probable victims of any compromise to inadequate data security practices maintained by Defendant.

249. Further, Defendant assumed a duty of reasonable care in making representations in marketing materials and its Privacy Policies, Statements, and Notices concerning data security.

250. Defendant is also bound by industry standards to protect confidential Private Information.

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

252. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former Benefits Recipients' Private Information it was no longer required to retain pursuant to regulations.

253. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class Members of the Data Breach.

254. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

255. Defendant waited months to provide Plaintiffs and the Class such notice.

256. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had

been compromised;

e. Failing to remove any Private Information it was no longer required to retain pursuant to regulations, and;

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

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

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

259. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

260. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

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

262. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach

of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting employee-benefit management companies in possession of Private Information.

263. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

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

265. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

266. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

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

268. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

269. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

270. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

272. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) emotional distress associated with the loss of control over their highly sensitive Private Information; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

273. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not

limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

274. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, 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 Private Information in its continued possession.

275. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

276. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

277. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

278. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the foregoing paragraphs, as if fully set forth herein.

279. Kelly Benefits entered into written contracts with its clients to provide employee-benefit management services, for the benefit of Plaintiffs and Class Members.

280. In exchange, Kelly Benefits agreed to implement adequate security measures to safeguard the Private Information of Plaintiffs and Class Members and to timely and adequately notify them of the Data Breach.

281. These contracts were made expressly for the benefit of Plaintiffs and Class Members, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Kelly Benefits and its clients. Kelly Benefits knew that, if it were to breach these contracts with its clients, its clients' Benefits Recipients—Plaintiffs and Class Members—would be harmed.

282. Kelly Benefits breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

283. Plaintiffs and the Class Members were harmed by Kelly Benefits' breach of its contracts with their clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

284. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

285. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the foregoing paragraphs, as if fully set forth herein.

286. This Count is pleaded in the alternative to the breach of third-party beneficiary contract (Count II).

287. Plaintiffs and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have had their Private Information protected with adequate data security.

288. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

289. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

290. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

291. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information with Defendant.

292. Plaintiffs and Class Members have no adequate remedy at law.

293. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own

profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

294. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

295. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) emotional distress associated with the loss of control over their highly sensitive Private Information; (vii) invasion of their privacy; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

296. 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 its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

297. 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 IV
CALIFORNIA UNFAIR COMPETITION LAW
(On Behalf of Plaintiff Law and the California Subclass)

298. Plaintiff Law ("California Plaintiff") re-alleges and incorporates by reference all of the allegations contained in the foregoing paragraphs, as if fully set forth herein.

299. California Plaintiff brings this Count on his own behalf and on behalf of all California Subclass Members.

300. California Plaintiff pleads this claim for equitable relief, including restitution and injunctive relief, in the alternative to his claims for damages.

301. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

302. Defendant's actions as alleged herein in this Class Action Complaint constitute an "unlawful" practice as encompassed by Cal. Bus. & Prof. Code §§ 17200 *et seq.* because Defendant's actions: (a) violated the California Consumer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*; (b) violated the CCPA, Cal. Civ. Code §§ 1798.100 *et seq.*; (c) constituted negligence; and (d) violated federal law and regulations, including the FTC Act.

303. Defendant's actions as alleged in this Class Action Complaint also constitute an "unfair" practice as encompassed by Cal. Bus. & Prof. Code §§ 17200 *et seq.*, because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious.

304. The harm caused by Defendant' wrongful conduct outweighs any utility of such conduct and has caused—and will continue to cause—substantial injury to the California Subclass, including California Plaintiff. There were ample reasonably available alternatives that would have furthered Defendant's legitimate business practices, including using industry-standard technologies to protect data (e.g., two-factor authorization, effective encryption and anonymization, compartmentalization of sensitive data, software patches, limiting how much data any user may access, and the purging of data no longer necessary for Defendant's services).

305. Defendant also unreasonably delayed in notifying California Plaintiff and California Subclass Members regarding the unauthorized release and disclosure of their Private Information.

306. Additionally, Defendant's conduct was "unfair" because it violated the legislatively declared policies reflected by California's strong data-breach and online-privacy laws, including the California Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, the CCPA, Cal. Civ. Code §§ 1798.100, *et seq.*, and the California constitutional right to privacy, Cal. Const. Art. 1, § 1.

307. Defendant's conduct also is deceptive in violation of the UCL. Defendant's fraudulent business acts and practices include:

a. Failing to adequately secure the personal information of California Plaintiff and California Subclass Members from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts about California Plaintiff and California Subclass Members in a manner highly offensive to a reasonable person;

c. Enabling the disclosure of personal and sensitive facts about California Plaintiff and California Subclass Members without their informed, voluntary, affirmative, and clear consent;

d. Omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure California Plaintiff's and California Subclass Members' personal information.

308. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of California Plaintiff's and California Subclass Members' personal information.

309. The harm from Defendant's conduct was not reasonably avoidable by consumers. California Plaintiff and California Subclass Members were required to provide their Private Information to their employers or benefits providers, which without their consent or knowledge, was turned over to Defendant. California Plaintiff and California Subclass Members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures.

310. There were reasonably available alternatives that would have furthered Defendant's business interests of electronically transferring its customers' information while protecting Private Information.

311. A reasonable person would regard Defendant's derelict data security and the Data Breach as important, material facts that could and should have been disclosed

312. As a direct and proximate result of Kelly Benefits' unfair methods of competition and unfair or deceptive acts or practices and Plaintiff Law's and California Subclass' reliance on them, Plaintiff Law and California Subclass have suffered and will continue to suffer injury,

ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant, since they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

313. As a direct and proximate result of Kelly Benefits' unlawful and unfair practices and acts, Plaintiff Law and California Subclass were injured and lost money or property, including but not limited to the loss of Plaintiff Law's and California Subclass' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

314. Kelly Benefits knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Law's and California Subclass Members' Private Information and that the risk of a data breach or theft was highly likely. Kelly Benefits' actions in engaging in the above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff Law and California Subclass Members.

315. California Plaintiff and California Subclass Members have no adequate remedy at law because the injuries here include an imminent risk of identity theft and fraud that can never be fully remedied through damages, ongoing identity theft and fraud, as well as long term incalculable risk associated with medical fraud.

316. Further, if an injunction is not issued, California Plaintiff and California Subclass Members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. Defendant has still not provided adequate information on the cause and scope of the Data Breach. California Plaintiff and California Subclass Members lack an adequate remedy at law that will reasonably protect against the risk of a further breach.

317. California Plaintiff, on behalf of California Subclass Members seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including but not limited to restitution to Plaintiff Law and California Subclass of money or property Kelly Benefits may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all monies that accrued to Kelly Benefits because of Kelly Benefits' unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT V
CALIFORNIA CONSUMER PRIVACY ACT OF 2018
(On Behalf of Plaintiff Law and the California Subclass)

318. Plaintiff Law re-alleges and incorporates by reference all of the allegations contained in the foregoing paragraphs, as if fully set forth herein.

319. Plaintiff Law brings this Count on his own behalf and on behalf of all California Subclass Members.

320. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical

harm."[42]

321. The CCPA imposes an affirmative duty on businesses that maintain Private Information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

322. The CCPA also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

323. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

324. Plaintiff is a consumer and California resident as defined by Civil Code section 1798.140(i).

325. Defendant is a "business" as defined by Civil Code section 1798.140(d)(2) because it is "organized or operated for the profit or financial benefit of its shareholders or other owners,"

[42] *See* California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/ (last visited Feb. 9, 2026).

and "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the state of California."

326. Plaintiff Law and California Subclass Members' personal information, as defined by Civil Code section 1798.140(v)(1), was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including names, Social Security numbers and health insurance ID numbers were wrongfully taken, accessed, and viewed by unauthorized third parties. Defendant maintained Plaintiff Law's and California Subclass Members' Private Information in a form that allowed criminals to access it.

327. The Data Breach occurred because of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff Law's and California Subclass Members' Private Information. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network, including Defendant Kelly Benefits' cloud-based databases, by hackers and to prevent unauthorized access of Plaintiff Law's and California Subclass Members' Private Information as a result of this attack.

328. Plaintiff Law provided Defendant with written notice of Defendant's violations of the CCPA, on February 3, 2026, pursuant to Civil Code § 1798.150(b)(1). Defendant has not yet responded to this written notice and thus has not cured or is unable to cure the violations described herein. Plaintiff Law seeks all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount between one hundred ($100) and seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

329. On behalf of California Subclass Members, Plaintiff Law presently seeks actual pecuniary damages and injunctive relief in the form of an order enjoining Defendant from continuing to violate the CCPA. Unless and until Defendant is restrained by order of the Court, its wrongful conduct will continue to cause irreparable injury to Plaintiff Law and the California Subclass.

330. If Defendant fails to timely rectify or otherwise cure the CCPA violations described herein, individually and on behalf of the California Subclass, Plaintiff Law reserves his right to amend this Class Action Complaint to seek statutory damages and any other relief the Court deems proper as a result of Defendant's CCPA violations pursuant to Civil Code Section 1798.150(a).

331. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, in addition to actual or statutory damages, Plaintiff Law and California Subclass Members seek injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VI
CALIFORNIA CUSTOMER RECORDS ACT
(On Behalf of Plaintiff Law and the California Subclass)

332. Plaintiff Law re-alleges and incorporates by reference all of the allegations contained in the foregoing paragraphs, as if fully set forth herein.

333. Plaintiff Law brings this Count on his own behalf and on behalf of all California Subclass Members.

334. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the

information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

335. Defendant is a business that owns, maintains, or licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass Members.

336. Defendant violated Cal. Civ. Code § 1798.81.5 by failing to implement reasonable measures to protect California Subclass Members' Private Information.

337. Businesses that own or license computerized data that includes personal information are required to notify California residents when their Private Information has been acquired (or has reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

338. Defendant is a business that owns or licenses computerized data that includes Personal Information, as defined by Cal. Civ. Code § 1798.82.

339. Plaintiff Law's and California Subclass Members' Private Information includes personal information identified in Cal. Civ. Code § 1798.82(h) such as their names, Social Security numbers and health insurance ID numbers and is thereby covered by Cal. Civ. Code § 1798.82.

340. Plaintiff and California Subclass Members are "customers" within the meaning of Cal. Civ. Code § 1798.80(c), as their personal information was provided to Defendant in the process receiving benefits administration services.

341. The Data Breach constituted a breach of Defendant's security systems, networks, and servers.

342. Because Defendant reasonably believed that Plaintiff Law and California Subclass Members' Private Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

343. Defendant unreasonably delayed informing Plaintiff Law and California Subclass Members about the breach of security of their Private Information after it knew the Breach had occurred.

344. Upon information and belief, no law enforcement agency instructed Defendant that notification to California Subclass Members would impede an investigation.

345. Thus, by failing to disclose the Data Breach in a timely and accurate manner, Defendant also violated Cal. Civ. Code § 1798.82. Pursuant to Cal. Civ. Code § 1798.84, "[a]ny waiver of a provision of this title is contrary to public policy and is void and unenforceable," "[a]ny customer injured by a violation of this title may institute a civil action to recover damages," and "[a]ny business that violates, proposed to violate, or has violated this title may be enjoined."

346. As a direct and proximate result of Defendant's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff Law and California Subclass Members suffered damages, as described above.

347. As a result of Defendant's violations of Cal. Civ. Code § 1798.82, Plaintiff Law and California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

348. As a direct consequence of the actions as identified above, Plaintiff Law and California Subclass Members incurred additional losses and suffered further harm to their privacy, including, but not limited to, economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the Data Breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive Private Information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

349. Plaintiff Law and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages, any applicable statutory damages, and equitable and injunctive relief.

COUNT VII
MARYLAND PERSONAL INFORMATION PROTECTION ACT
(On Behalf of Plaintiffs Dohrman, Evans, O'Brien and Parks and the Maryland Subclass)

350. Plaintiffs Dohrman, Evans, O'Brien and Parks ("Maryland Plaintiffs") re-allege and incorporate by reference all of the allegations contained in the foregoing paragraphs, as if fully set forth herein.

351. Maryland Plaintiffs bring this Count on their own behalf and on behalf of all Maryland Subclass Members.

352. "To protect Personal Information from unauthorized access, use, modification, or disclosure," the Maryland legislature enacted Md. Comm. Code § 14-3503(a), which requires that any business that "own or license Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the

nature of Personal Information owned or licensed and the nature and size of the business and their operations."

353. Defendant is a business that owns or licenses computerized data that includes Personal Information, as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

354. Maryland Plaintiffs' and Maryland Subclass Members' Private Information includes Personal Information as covered by Md. Comm. Code § 14-3501(d).

355. Md. Comm. Code § 14-3504(b)(2) and 14-3504(c)(2), require Defendant, in the most expedient time possible, to accurately notify individuals of a breach of their data security system without unreasonable delay.

356. Defendant was aware of a breach of its security system, and was obligated to disclose the Data Breach in a timely and accurate fashion, as mandated by Md. Comm. Code § 14-3504(1).

357. On or about April 9, 2025, nearly 70 days after the discovery of the Data Breach, Defendant Kelly Benefits provided Maryland Plaintiffs and Maryland Subclass Members limited notice of the Data Breach.

358. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Md. Comm. Code § 14-3504(b)(2) and 14-3504(c)(2).

359. As a direct and proximate result of Defendant's violations of Md. Comm. Code § 14-3504(b)(2) and 14-3504(c)(2), Maryland Plaintiffs and Maryland Subclass Members suffered damages, as described above.

360. Maryland Plaintiffs seek relief under Md. Comm. Code §13-408, including actual damages and injunctive relief.

COUNT VIII
MARYLAND CONSUMER PROTECTION ACT
(On Behalf of Plaintiffs Dohrman, Evans, O'Brien and Parks and the Maryland Subclass)

361. Plaintiffs Dohrman, Evans, O'Brien, and Parks ("Maryland Plaintiffs") re-allege and incorporate by reference all of the allegations contained in the foregoing paragraphs, as if fully set forth herein.

362. Maryland Plaintiffs bring this Count on their own behalf and on behalf of all Maryland Subclass Members.

363. Defendant is a "person" as defined by Md. Code, Com Law § 13-101(h).

364. Defendant's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Code Ann., Com. Law § 13-101(i) and § 13-303.

365. Maryland Plaintiffs and Maryland Subclass Members are "consumers" as defined by Md. Code Ann., Com. Law § 13-101(c).

366. Defendant advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Code Ann., Com. Law § 13-101(d) by nature of the benefits enrollment services it offers.

367. Defendant violated Md. Code Ann., Com. Law §§ 13-301 and 13-301, *et seq.*, by engaging in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Maryland in connection with the sale and advertisement of "consumer goods" or "consumer services" (as defined by Md. Code Ann., Com. Law § 13-101(d)), including the following:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are another; and

c. Advertising its goods and services with intent not to sell them as advertised.

d. Failing to implement and maintain reasonable security and privacy measures to protect Maryland Plaintiffs' and Maryland Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

e. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures after previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Maryland Plaintiffs' and Maryland Subclass Members's Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Misrepresenting that it would protect the privacy and confidentiality of Maryland Plaintiffs' and Maryland Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

h. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Maryland Subclass Members Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

i. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Maryland Plaintiffs' and Maryland Subclass Members' Private Information; and

j. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Maryland Plaintiffs' and Maryland Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code Ann., Com. Law § 14-3503.

368. Defendant's representations and omissions were material because they were likely to deceive Maryland Plaintiffs and Maryland Subclass Members about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information. Defendant's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

369. Defendant intended to mislead Maryland Plaintiffs and Maryland Subclass Members and induce them to rely on its misrepresentations and omissions.

370. Had Defendant disclosed to Maryland Plaintiffs and Maryland Subclass Members residing in Maryland that its data systems were not secure and thus were vulnerable to attack, Defendant could not have continued in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Maryland Plaintiffs' and Maryland Subclass Members' Private Information as part of the services Defendant provided and for which Maryland Subclass Members paid without advising Maryland Subclass Members that Defendant's data security practices were insufficient to maintain the safety and confidentiality of Maryland Plaintiffs' and Maryland Subclass Members' Private Information. Accordingly, Maryland Plaintiffs and the Maryland Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

371. Defendant acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Fraud Act and recklessly disregarded Maryland Plaintiffs and Maryland Subclass Members' rights. Defendant: (i) represented in its information privacy and confidentiality policies that it was implementing reasonable security measures to protect Maryland Plaintiffs' and Maryland Subclass Members' sensitive personal information; and (ii) failed to implement reasonable data security measures. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45.

372. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices and Maryland Plaintiffs' and Maryland Subclass Members' reliance on them, Maryland Plaintiffs and Maryland Subclass Members have suffered and will

continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant, since they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

373. As a direct and proximate result of Defendant's unlawful, unfair, and deceptive practices and acts, Maryland Plaintiffs and Maryland Class Members were injured and lost money or property, including but not limited to the loss of Maryland Plaintiffs' and Maryland Subclass Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

374. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Maryland Plaintiffs' and Maryland Class Members' Private Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Maryland Plaintiffs and Maryland Subclass Members.

375. Plaintiffs and Class Members have no adequate remedy at law.

376. Maryland Plaintiffs, on behalf of Maryland Subclass Members, seek relief including but not limited to restitution of money or property Defendant may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all monies that

accrued to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

PRAYER FOR RELIEF

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

A. An order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

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

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

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

E. An award of attorneys' fees and costs as allowed by law;

F. Prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiffs, individually and on behalf of the Class Members, hereby demand a trial by jury on all claims so triable.

Dated: February 9, 2026

By: */s/ Cyril V. Smith*

Cyril V. Smith (Fed. Bar No. 07332)
ZUCKERMAN SPAEDER LLP
100 East Pratt Street – Suite 2440
Baltimore, Maryland 21202
Telephone: 410-332-0444
csmith@zuckerman.com

Raina C. Borrelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

James J. Pizzirusso (Fed. Bar No. 20817)
HAUSFELD LLP
1201 17th Street N.W., Suite 600
Washington, D.C. 20036
Telephone: 202-540-7200
jpizzirusso@hausfeld.com

Interim Co-Lead Class Counsel and Liaison Counsel