LAW OFFICES OF RONALD A. MARRON
RONALD A. MARRON (SBN 175650)
ron@consumersadvocates.com
ALEXIS M. WOOD (270200)
alexis@consumersadvocates.com
KAS L. GALLUCCI (SBN 288709)
kas@consumersadvocates.com
ELISA PINEDA (SBN 328285)
elisa@consumersadvocates.com
651 Arroyo Drive
San Diego, California 92103
Telephone: (619) 696-9006
Facsimile: (619) 564-6665

UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF CALIFORNIA

ADAM BENTE, individually and on behalf of all others similarly situated and the general public,

Plaintiff,

v.

UKG, INC.,

Defendant.

Case No: **'22CV289 GPC WVG**

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff ADAM BENTE ("Plaintiff"), individually and on behalf of all others similarly situated and the general public, by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant UKG, Inc. ("UKG" or "Defendant") to, without limitation, obtain actual and exemplary damages, injunctive relief, restitution, and obtain a declaration that Defendant's actions were unlawful as further set forth below. Plaintiff alleges the following based upon personal knowledge as to himself and his own acts, and on information and belief as to all other matters, including, *inter alia*, any investigation conducted by and through his attorneys:

INTRODUCTION

1. Plaintiff brings this class action against UKG for its failure to implement and maintain reasonable security procedures and practices with respect to the sensitive and confidential personal information UKG obtains from its customers' employees; the consequent data breach of its systems that began in December of 2021; and the resultant shut down of payroll services that is ongoing as of the filing of this Class Action Complaint.

2. UKG is one of the world's biggest workforce management software companies. The company collects, stores, and processes data for thousands of companies and millions of workers. UKG's clients broadly range between corporate and public organizations, including the likes of PepsiCo, Tesla, GameStop, the University of California system, the County of Santa Clara, and many private and public hospital and healthcare organizations.

3. As a result of its lack of adequate security measures, UKG was attacked by hackers who launched a ransomware attack on UKG's timekeeping system, Kronos Private Cloud, on or around December 11, 2021.

4. The data breach exposed millions of workers' sensitive and confidential personal identifying information ("PII") to cybercriminals.

5. To make matters worse, the attack also crippled timekeeping and

payroll systems, resulting in workers not being paid, being paid late, or being paid incorrectly.

6. The timing of the data breach could not have come at a worse time, leaving many employees to worry over their privacy and paychecks during the peak of the holiday season as well as the latest surge of the COVID-19 pandemic.

7. Many of the affected organizations include hospitals and healthcare systems, including Plaintiff's employer, Family Health Centers of San Diego ("FHCSD"), a nonprofit clinic provider of health care dedicated to providing affordable health care and support services.

8. FHCSD provides care to over 227,000 patients each year, of whom 91% are low income and 29% are uninsured. FHCSD is one of the largest community clinic providers in the nation, operating 58 clinics across San Diego County.

9. As a result of UKG's payroll services going offline, all FHCSD employees were delayed payment of their paychecks.

10. All FHBCSD employees were forced to find alternative sources of income to pay their bills, mortgages, and necessities, again during the midst of the holiday season.

11. Even after FHCSD got around to distributing paychecks to its employees, many FHCSD employees were either paid inaccurately and/or not at all.

12. In the months following the data breach, all FHCSD employees have had to invest significant time and expense into determining the amount of any unpaid wages, bonuses, and/or paid time off.

13. In addition to their paychecks being affected, Plaintiff's and all FHCSD employees' sensitive and confidential PII was obtained by unauthorized hackers and sold on the dark web. As a result, FHCSD employees not only have to deal with the loss of wages and the resulting consequences, but also have had to invest time and money into securing their personal and financial information.

14. Plaintiff brings this class action to redress these injuries, on behalf of

himself and on behalf of individuals similarly situated and the general public.

PARTIES

15. Plaintiff Adam Bente is a citizen and resident of the State of California. Plaintiff is an employee of Family Health Centers of San Diego. Plaintiff has been employed by FHCSD as a business analyst since 2017.

16. Defendant UKG, Inc. is a corporation formed under the laws of the State of Delaware, with dual corporate headquarters in Weston, Florida and Lowell, Massachusetts.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), because at least one member of the Class, as defined below is a citizen of a different state than UKG, there are more than 100 members of the Classes, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs.

18. The Court has general personal jurisdiction over UKG because, at all relevant times, UKG has had systematic and continuous contacts with the State of California. UKG is registered to do business in California with the California Secretary of State under entity number C2111426. UKG regularly contracts with a multitude of businesses and organizations in California to provide continuous and ongoing human resource services, including timekeeping and payroll services.

19. This Court has specific personal jurisdiction over UKG because Plaintiff's claims arise from UKG's specific contacts with the State of California – namely, UKG's provision of payroll and other human resource services to a multitude of companies in California, UKG's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent connection with such services.

20. Venue is proper in this Southern District of California pursuant to 28 U.S.C. § 1391(b)(2) because the injury in this case substantially occurred in this

District.

FACTUAL ALLEGATIONS

21. UKG Inc. (an acronym for Ultimate Kronos Group) is a workforce management software company that provides human resource services, including timekeeping and payroll services, to companies across the globe. Among the many products and services that it offers, UKG provides software known as the "Kronos Private Cloud" and "UKG Workforce Central," which are timekeeping and payroll services.

22. UKG was formed as a result of a $22 billion merger in 2020 between Ultimate Software and Kronos. The company has 13,000 employees across the globe, and amidst a global pandemic, was able to generate over $3 billion in revenue in its first year of business. It is one of the largest cloud computing companies in the world and a leading global provider of workforce management services.

23. UKG provides its timekeeping and payroll services to a multitude of companies and organizations, including many that operate in California, the like of which include but are not limited to, PepsiCo, Tesla, GameStop, the University of California system, the County of Santa Clara, and many private and public hospital and healthcare organizations, including FHCSD. UKG provides timekeeping and payroll services to thousands of employers.

24. In connection with those services, UKG collects, stores, and processes sensitive personal data for thousands of companies and millions of workers. Prior to the data breach, UKG had enacted a privacy notice in which it states UKG collects PII of individuals from a variety of sources, including directly from its customers and their employees. The privacy notice contains a section entitled "Customers' Information [and the Information of Their Employees and Job Applicants]", which states that UKG collects data including, but not limited to "name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers." *See* **Exhibit 1** [UKG privacy notice]. Source:

https://www.ukg.com/privacy.

25. UKG also collects banking information in connection with its provision of direct deposit payroll processes as well as employee identification numbers. For example, under "Use of Personal Information", under the subsection titled "Customers' Information (and the Information of Their Employees)," UKG's privacy notice states UKG uses the PII of its customers' employees to provide its customers with services. *See* **Exhibit 1.**

26. UKG's website indicates that its services, among other things, allows its customers to ensure accurate, on-time pay and to quickly generate payroll documents, such as paychecks and direct-deposit files.

27. On December 13, 2021, UKG posted an announcement regarding the data breach on its website. The announcement confirmed that that a ransomware attack was made on UKG's Kronos Private Cloud. The Kronos Private Cloud includes Defendant's UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions. UKG further claimed that the data breach did not affect UKG Pro, UKG Ready, UKG Dimensions, or any other UKG product or solutions. Defendant confirmed that as a result of the attack, Kronos Private Cloud solutions was offline.

28. UKG advised its customers "that it may take up to several weeks to restore system availability," and that as such, the company "strongly recommends that [customers] evaluate and implement alternative business continuity protocols related to the affected UKG solutions."[1]

29. On December 17, 2021, Defendant then posted on its website "New Questions & Answers for Impacted and Non-Impacted Customers" that, among

[1] UKG Workforce Central – Leo Daley, *Communications sent to impacted Kronos Private Cloud (KPC) customers beginning December, 13 at 12:45AM ET*, UKG, https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US (last visited Mar. 4, 2022).

other things, stated the following question and answer:

> **Precisely what information was accessed or exposed?**
> Our investigation is ongoing and we are working diligently to determine if customer data has been compromised.[2]

30. On December 28, 2021, UKG finally acknowledged the potential exposure of sensitive employee PII as follows:

> Regarding data exfiltration - our investigation is still ongoing and we are working diligently with cybersecurity experts to determine whether and to what extent sensitive customer or employee data has been compromised. As is typical in ransomware incidents, it may take several more weeks or more to fully determine whether a specific customer's sensitive data (and what kind of data) may have been compromised. If we learn that sensitive customer business data and/or employee data (PII) was exposed because of this attack, we will meet any obligations we have to inform affected customers and take appropriate steps to protect affected individuals.[3]

31. On January 22, 2022, UKG posted an update to its website stating that "[b]etween January 4 and January 22, **all** affected customers in the Kronos Private Cloud were restored with safe and secure access to their core time, scheduling, and HR/payroll capabilities. We are now focused on the restoration of supplemental features and non-production environments and are extraordinarily grateful for the patience and partnership our customers have shown."[4]

32. UKG's carefully worded announcement failed to clarify that UKG's

---

[2] *New Questions & Answers for Impacted and Non-Impacted Customers as of 12/17/2021 at 2:30pm ET*, UKG, https://www.ukg.com/KPCupdates/Archive (last visited Mar. 4, 2022).

[3] *Status Update as of Dec 28, 2022*, UKG, https://www.ukg.com/KPCupdates/Archive (last visited Mar. 4, 2022).

[4] *Status Update as of Jan 22, 2022*, UKG, https://www.ukg.com/KPCupdates/Archive (last visited Mar. 4, 2022) (emphasis in original).

payroll services were still **not** fully operational, and as a result, many FHCSD employees' paychecks continued to be paid late, inaccurately, and/or not at all.

33. UKG confirmed as such on February 11, 2022, when it announced that only the first phase of the restoration process was complete and that many of Kronos Private Cloud applications, such as Citrix, Workforce Analytics, and non-production environments, were still offline.[5]

34. The February 11, 2022, announcement went on to state that UKG had discovered and notified customers whose personal data of its employees "was exfiltrated."[6]

35. UKG claimed the theft of personal data was contained to employees of only two of its customers, however, in the same announcement, UKG admits its forensic investigation is still ongoing.[7]

36. The announcement provided a link for use only by its customers to obtain further information on UKG's investigation and security practices.[8] Upon information and belief, this information was not shared with the employees of UKG's customers who were affected by the data breach.

37. As of the filing of this complaint, news sources have confirmed that PUMA North America, Inc. ("Puma") is one of the affected customers. A data breach notification submitted by Puma to the Office of the State Attorney General of Maine states the personal data of over 6,632 individuals was stolen in the attack on UKG's Kronos Private Cloud software.[9]

38. A sample notification letter to affected employees of Puma from UKG

---

[5] *Status Update as of Feb 11, 2022*, UKG, https://www.ukg.com/KPCupdates/Archive (last visited Mar. 4, 2022).

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] Data Breach Notifications, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/10394643-6f4e-49ff-884a-9977602932a9.shtml (last visited Mar. 4, 2022).

again confirms that UKG's investigation is still ongoing, and that up to now, UKG can only confirm "that a malicious actor or actors accessed the cloud-based environment earlier in 2021 [and] stole data from that environment and encrypted the environment." Under a section titled **"What Information Was Involved?"**, the sample letter states "[t]he personal information involved included your [Extra2]" but does not state what information was stolen.[10]

39. To date, UKG has not confirmed what information was stolen.

40. Online sources indicate that PepsiCo employees' PII was also stolen during the data breach. PepsiCo employees impacted by the breach have reported hacking of their banking information in the weeks following the breach. Furthermore, Twitter users have likewise reported that as a result of the UKG security breach, hackers obtained workers' phone numbers and began phishing scams. For example, on December 26, 2021, at 1:58 P.M., Twitter user @_genosis_ tweeted: "For all those who have been affected by the Kronos hack please be aware of this. They have already managed to scam a couple hundred employees from another company so be on the look out!" That twitter user posted an image of a text chain stating:

> Hey Team just a heads up. My sister in law is the HR director [for] Gatorade. They too have been hit by the KRONOS outage. She let me know yesterday that the people that hacked kronos did in fact get employee phone #'s and names. They are now calling PepsiCo/Gatorade employees and saying their work for kronos and are calling to verify employee info. They have managed to scam a couple hundred employees already. Make sure your teams [know] that there is ZERO reason anyone would ever call them and [ask] for their info.

[10] UKG Sample Data Breach Notification Letter, file:///C:/Users/elisa/Downloads/EXPERIAN_H4870_UKG-Puma_L03_Proof%20Multi%20and%20L04_Dep%20Multi.pdf (last visited Mar. 4, 2022).

41. Upon information and belief, the hackers responsible for the data breach stole the PII of all employees of UKG's customers.

42. UKG's website provides the following with regard to its Kronos Private Cloud software: "At Kronos, data security is a top priority. Our Chief Information Security Officer is the designated management representative responsible for implementing policies and procedures to protect and safeguard our customers' workforce data."[11]

43. Upon information and belief, UKG's Chief Information Security Officer is John McGregor.

44. The FBI created a technical guidance document for Chief Information Officers and Chief Information Security Officers that complies already existing federal government and private industry best practices and mitigation strategies to prevent and respond to ransomware attacks. The document is titled *How to Protect Your Networks from Ransomware* and states that on average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. Yet, there are very effective prevention and response actions that can significantly mitigate the risks.[12]

45. Preventative measure include:

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

---

[11] *Security: Kronos private cloud security and workforce ready reliability*, KRONOS, https://www.kronos.com/security (last visited Mar. 4, 2022).

[12] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed Mar. 2, 2022).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[13]

46. UKG could have prevented the data breach by properly utilizing best practices as advised by the federal government.

[13] *Id.*

47. UKG's failure to safeguard the PII of employees of Defendant's customers is exacerbated by the repeated warnings and alerts from public and private institutions, including the federal government, directed to protecting and securing sensitive data. Experts studying cyber security routinely identify companies such as UKG that collect, process, and store massive amounts of data on cloud-based systems as being particularly vulnerable to cyberattacks because of the value of the PII that they collect and maintain. Accordingly, UKG knew or should have known that it was a prime target for hackers.

48. According to the 2021 Thales Global Cloud Security Study, more than 40% of organizations experienced a cloud-based data breach in the previous 12 months. Yet, despite these incidents, the study found that nearly 83% of cloud-based businesses still fail to encrypt half of the sensitive data they store in the cloud.[14]

49. Upon information and belief, Kronos did not encrypt Plaintiff's and Class Members' PII involved in the data breach.

50. Defendant's knowledge that it was a target of hackers is further underscored by the massive number of ransomware attacks on payroll companies such as UKG.

51. This past November, Frontier Software, a payroll software, experienced a ransomware attack that compromised the sensitive information of between 38,000 to 80,000 South Australian government employees.[15]

52. In March of 2021, PrismHR, a Massachusetts-based payroll company that services over 80,000 organizations, suffered a massive outage after suffering a

[14] Maria Henriquez, *40% of organizations have suffered a cloud-based data breach*, SECURITY, Oct. 29, 2021, https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-data-breach (last visited Mar. 4, 2022).

[15] Emily Kuhnert, *Payroll Security Breaches,* PAPAYAGLOBAL, Feb. 27, 2020, https://papayaglobal.com/blog/list-of-payroll-security-breaches/, (last visited Mar. 4, 2022).

cyberattack on its payroll cloud-based system.[16]

53. In January of 2021, 6,000 employees' PII was stolen during a ransomware attack on Arup's, a UK-based third-party payroll provider.[17]

54. In May of 2020, Interserver, a payroll vendor for Britain's Ministry of Defense, was hacked. The hackers obtained the sensitive information of up to 100,000 past and current employees.[18]

55. In February of 2020, the Phoenix Pay System fell prey to a data breach exposing the PII of more than 69,000 Canadian federal employees.[19]

56. Despite knowing the prevalence of data breaches, UKG failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. UKG has the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized breaches. UKG failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure vulnerabilities were avoided or remedied and that Plaintiff's and Class Members' data were protected.

57. As of the date of this Complaint — nearly two months after the breach — UKG's systems remain disabled, its systems remain unsecured, and the harm resulting from the data breach remains unrectified.

PLAINTIFF'S ALLEGATIONS

58. Plaintiff has worked as a business analyst for the Family Health Centers

---

[16] Lawrence Abrams, *Payroll giant PrismHR outage likely caused by ransomware attack*, Bleeping Computer, Mar. 2, 2021, https://www.bleepingcomputer.com/news/security/payroll-giant-prismhr-outage-likely-caused-by-ransomware-attack/, (last visited Mar. 4, 2022).

[17] *Id.*

[18] Emily Kuhnert, *Payroll Security Breaches,* PAPAYAGLOBAL, Feb. 27, 2020, https://papayaglobal.com/blog/list-of-payroll-security-breaches/, (last visited Mar. 4, 2022).

[19] *Id.*

of San Diego since 2017. Plaintiff's responsibilities include reviewing and reporting data to obtain government grants necessary to FHCSD's mission of providing affordable health care services to low-income individuals in the San Diego community. FHCSD is the nation's tenth largest health center with more than 1,800 dedicated employees.

59. FHCSD uses Kronos Privates Cloud to process payroll. On December 12, 2021, FHCSD notified its employees that as a result of a malware attack on UKG's system, FHCSD's payroll software was offline. As a direct and foreseeable result of UKG's negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, FHCSD's timekeeping and payroll systems became crippled and remained completely offline for weeks following the data breach. FHCSD lacked an adequate contingency plan to accurately pay workers and was forced to switch to manually inputting payroll.

60. On December 13, 2021, FHCSD notified its employees that employees would need to maintain and submit "manual timesheets" for time worked following the data breach. FHCSD further instructed it employees that for payroll accumulated before December 10, 2021, FHCSD would need to utilize employees' employment status to process payroll. FHCSD instructed employees who had concerns with this method of calculating payroll to contact FHCSD.

61. Plaintiff, like all Class Members, was delayed payment of his paycheck following the data breach. Following the data breach, Plaintiff's payroll was scheduled to be processed by December 17, 2021. The resultant shutdown of UKG's payroll services caused each FHCSD employee, including Plaintiff, to not receive their paycheck until after Christmas. Plaintiff and Class Members had to endure weeks without payment while working during the Omicron surge in the midst of the holiday season.

62. Plaintiff, like all Class Members, has lost time and expenses from having to mitigate the consequences of the delay in payment of his paychecks.

63. Plaintiff, like all Class Members, also had his PII, including but not limited to his name, company name, address, email address, time and attendance and schedule information, and Social Security Number, exposed as a result of UKG's negligent failure to safekeep his information.

64. As a direct and foreseeable result of UKG's negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Plaintiff and Class Members also suffered harm in that their sensitive PII has been exposed to cybercriminals and they now have an increased risk and fear of identity theft and fraud.

65. Since the data breach, Plaintiff has received on average, per day 5-6 spam calls to his cell phone and countless spam e-mails. Further, shortly after the data breach, Plaintiff received a notification from his credit card company that his Social Security number had been discovered on the dark web. Upon information and belief, Plaintiff's Social Security number, cell phone number and e-mail address were exfiltrated by the hackers who obtained unauthorized access to Plaintiff's and Class Members' PII.

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

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

can cause a lot of problems.[20]

67. Accordingly, Plaintiff and Class Members have suffered harm in the form of increased fear and risk of identity theft and fraud resulting from the data breach.

CLASS ACTION ALLEGATIONS

68. Plaintiff seeks to represent the following Classes:

> **Nationwide Data Breach Class:** All United States citizens whose personal information was exposed as a result of the Kronos Data Breach.
>
> **California Data Breach Subclass:** All California residents whose personal information was exposed as a result of the Kronos Data Breach
>
> **Nationwide Payroll Class:** All United States citizens whose paychecks were paid late, inaccurately, and/or not at all as a result of the Kronos Data Breach.
>
> **California Payroll Subclass:** All California residents whose paychecks were paid late, inaccurately, and/or not at all as a result of the Kronos Data Breach.

69. Excluded from the Classes is Defendant and its subsidiaries and affiliates; all employees of Defendant and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the Class; Plaintiff's counsel and UKG's counsel and members of their immediate families; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

---

[20] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.ssa.gov%2Fpubs%2FEN-05-10064.pdf&chunk=true (last visited Mar. 4, 2022).

70. Plaintiff reserves the right to modify, expand or amend the above Class definitions or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

71. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class Members is impracticable. While Plaintiff is informed and believes that there are likely hundreds of thousands of members in each Class and Subclass, the precise number of Class Members is unknown to Plaintiff. Class Members may be identified through objective means including Defendant's own records. Class Members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

72. **Commonality and Predominance:** This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members, including, without limitation:

a. Whether Defendants owed a duty to Plaintiff and Class Members to secure and safeguard their PII;

b. Whether Defendants failed to use reasonable care and reasonable methods to secure and safeguard Plaintiff's and Class Members' PII;

c. Whether Defendants properly implemented security measures as required by state law and/or industry standards to protect Plaintiff's and Class Members' PII from unauthorized access, capture, dissemination and misuse;

d. Whether Plaintiff and members of the Class were injured and suffered damages and ascertainable losses as a result of Defendants' actions or failure to act, including but not limited to the exposure of their PII to unauthorized third parties and loss of wages;

e. Whether Defendants engaged in active misfeasance and misconduct alleged herein;

f. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendants' failure to provide adequate security proximately caused Plaintiff's and Class Members' injuries; and

h. Whether Plaintiff and Class Members are entitled to declaratory and injunctive relief.

73. **Typicality:** Plaintiff is a member of the Classes. Plaintiff's claims are typical of the claims of all Class Members because Plaintiff, like other Class Members, suffered theft of his PII and lost wages as a result.

74. **Adequacy of Representation:** Plaintiff is an adequate Class representative because he is a member of the Classes and his interests do not conflict with the interests of other Class Members that he seeks to represent. Plaintiff is committed to pursuing this matter for the Classes with the Classes' collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type and Plaintiff intends to prosecute this action vigorously. Plaintiff, and his counsel, will fairly and adequately protect the Class's interests.

75. **Predominance and Superiority:** As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's case will also resolve them for the Classes' claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against UKG, so it would be impracticable for Class Members to individually seek redress for UKG's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized

litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

76. This class action is also properly brought and should be maintained as a class action because Plaintiff seeks injunctive relief on behalf of each Class on grounds generally applicable to each Class. Certification is appropriate because Defendants have acted or refused to act in a manner that applies generally to the injunctive Class (i.e., Defendants failed to reasonably protect Plaintiff and Class Members' PII from unauthorized third-party hackers). Thus, any injunctive relief or declaratory relief would benefit the Class as a whole.

77. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE

(On Behalf of all Classes)

78. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

79. Given the highly sensitive nature of the PII UKG collects from its employees and the likelihood of harm resulting from its unauthorized access, acquisition, use, or disclosure, UKG owes Plaintiff and Class Members a duty to exercise reasonable care in protecting this information. This duty includes implementing and maintaining reasonable security procedures and practices appropriate to the nature of the PII that were compliant with and/or better than industry-standard practices. UKG's duties included a duty to design, maintain, and

test its security systems to ensure that Plaintiff's and Class Members' PII was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by its own security systems regarding intrusions to its networks, and to promptly, properly, and fully notify its customers, Plaintiff, and Class Members of any data breach.

80. It was foreseeable to UKG that a failure to use reasonable measures to protect the highly sensitive and confidential information of its customers' employees could result in injury to said employees.

81. Actual and attempted breaches of data security were reasonably foreseeable to UKG given that other payroll companies had recently been breached before as well as the known frequency of data breaches and various warnings from industry experts.

82. In connection with the conduct described above, UKG acted wantonly, recklessly, and with complete disregard for the consequences Plaintiff and Class Members would suffer if their highly sensitive and confidential PII, including but not limited to name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers, was accessed by unauthorized third parties.

83. UKG had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, but UKG also knew that it was more likely than not Plaintiff and other Class Members would be harmed.

84. UKG's duty also arose 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 PII by companies such as UKG.

85. Various FTC publications and data security breach orders further form the basis of UKG's duty. According to the FTC, the need for data security should be factored into all business decision making.[21]

86. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[22] Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack 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. Additionally, the FTC recommends that companies 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.

87. UKG's duty also arose from its unique position as one of the largest cloud computing companies in the world whose services constitute a linchpin of the payroll services of a substantial fraction of the nation. As set forth above, the data

---

[21] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[22] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.com/system/files/documents/plain-language/pdf-0136_proteting-personal-informaiton.pdf.

breach herein affected thousands of companies and millions of employees. UKG undertakes its collection of sensitive PII of employees generally through direct relationships between UKG and employers, generally without the direct consent of employees who have no option but to be affected by UKG's actions. Plaintiff and Class Members cannot "opt out" of UKG"s activities. UKG holds itself out as a trusted steward of consumer and employee data, and thereby assumed a duty to reasonably protect that data. Plaintiff and Class Members, and indeed the general public, collectively repose a trust and confidence in UKG to perform that stewardship carefully. Otherwise consumers and employees would be powerless to fully protect their interests regarding their PII, which is controlled by UKG. Because of its crucial role within the payroll system, UKG was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the UKG data breach. By obtaining, collecting, using, and deriving a benefit from Plaintiff' and Class Members' PII, UKG assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff' and Class Members' PII from disclosure.

88. UKG admits that it has an enormous responsibility to protect employee data, that it is entrusted with this data, and that it did not live up to its responsibilities to protect the PII at issue here.

89. UKG's privacy policy has a specific "Security" section which states:

> To prevent unauthorized access or disclosure, to maintain data accuracy, and to allow only the appropriate use of your PII, UKG utilizes physical, technical, and administrative controls and procedures to safeguard the information we collect.
>
> To protect the confidentiality, integrity, availability and resilience of your PII, we utilize a variety of physical and logical access controls, firewalls, intrusion detection/prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our websites.

> We limit access to your PII and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your PII are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.

90. UKG also had a duty to safeguard the PII of Plaintiff and Class Members and to promptly notify them and their employers of a breach because of state laws and statutes that require UKG to reasonably safeguard PII, as detailed herein, including Cal. Civ. Code § 1798.80 *et seq.*

91. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, cancel or change usernames or passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, develop alternative timekeeping methods or other tacks to avoid untimely or inaccurate wage payments, and take other steps to mitigate or ameliorate the damages caused by UKG's misconduct.

92. UKG also owed a duty to Plaintiff and Class Members to exercise reasonable care to avoid sudden disruption of their human resources services, including their timekeeping and payroll services. UKG undertook of its own volition responsibility to provide continuous and ongoing timekeeping and payroll services to the employers of Plaintiff and Class Members, knowing that such services were for the benefit of making timely wage payments to them, among other things, and that any disruption, particularly any sudden disruption, would cause Plaintiff and Class Members harm.

93. UKG breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. UKG breached these duties by, among other

things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) prevent the breach; (c) detect the breach while it was ongoing; (d) maintain security systems consistent with industry standards and necessary to avoid the disabling of payroll systems for thousands of companies and millions of workers; (e) disclose that Plaintiff's and Class Members' PII in UKG's possession had been or was reasonably believed to have been stolen or compromised; and (f) avoid disruption and continued disruption of its timekeeping and payroll services.

94. UKG knew or should have known of the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks on payroll vendors such as UKG.

95. Through UKG's acts and omissions described in this Complaint, including UKG's failure to provide adequate security and its failure to protect the PII of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, UKG unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PII. UKG further failed to timely and accurately disclose to customers, Plaintiff, and Class Members that their PII had been improperly acquired or accessed and was available for sale to criminals on the dark web. Indeed, Plaintiff and Class Members received no notice of the breach directly from UKG. UKG issued a public statement and in some instances issued notices to its customers (the employers of Plaintiff and Class Members) but failed to adequately describe all types of PII that were exfiltrated, stolen, disclosed, or accessed by the ransomware attackers.

96. UKG further breached its duty to Plaintiff and Class Members to exercise reasonable care to avoid sudden disruption of their human resources services, including their timekeeping and payroll services, by allowing its systems to remain disabled for multiple weeks (and counting) and failing to adequately and timely remedy its security vulnerabilities.

97. But for UKG's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised nor their timekeeping and payroll services disabled.

98. As a direct and proximate result of UKG's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. As a result of UKG's failure to protect Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII has been accessed by malicious cybercriminals.

99. Plaintiff's and the Class Members' injuries include:

a. damages stemming from Plaintiff and Class Members not being fully paid for all time worked, not being paid overtime, being provided inaccurate wage statements or no wage statements at all, not being provided meal and rest breaks or compensation in lieu thereof, all in violation of federal and state laws;

b. damages stemming from the fear and anxiety of Plaintiff and Class Members concerning whether they would be fully, timely, and accurately paid for all time worked during the 2021-2022 holiday season, and regarding how long such disruptions to their payroll systems would continue;

c. theft of their PII;

d. costs associated with requested credit freezes;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. costs associated with purchasing credit monitoring and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were

permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

j. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

k. damages to and diminution of value of their PII entrusted, directly or indirectly, to UKG with the mutual understanding that UKG would safeguard Plaintiff' and the Class Members' data against theft and not allow access and misuse of their data by others;

l. continued risk of exposure to hackers and thieves of their PII, which remains in UKG's possession and is subject to further breaches so long as UKG fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members;

m. loss of the inherent value of their PII;

n. and other significant additional risks of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

COUNT II

UNJUST ENRICHMENT

(On behalf of all Classes)

100. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

101. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by UGK and that was ultimately converted, stolen, removed, deleted, exfiltrated, or disclosed in the UKG data breach. This PII was conferred on UKG in most cases by third parties, Class Members' employers, but in some instances directly by Plaintiff and Class Members themselves.

102. UKG was benefitted by the conferral upon it of the PII pertaining to Plaintiff and Class Members and by its ability to retain and use that information. UKG understood that it was in fact so benefitted.

103. UKG also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential, and its value depended upon UKG maintaining the privacy, security, and confidentiality of that PII.

104. But for UKG's willingness and commitment to maintain its privacy, security, and confidentiality, that PII would not have been transferred to and entrusted with UKG. Further, if UKG has disclosed that its data security measures were inadequate, UKG would not have been permitted to continue in operation by regulators, its shareholders, and participants in the marketplace.

105. As a result of UKG's wrongful conduct as alleged in this Complaint (including among other things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct in facilitating the theft of that PII), UKG has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Among other things, UKG has and continues to benefit and profit from the sale of the PII and from its contracts to use that PII to process timekeeping and payroll, while the value to Plaintiff and Class Members has been diminished.

106. UKG's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

107. Under the common law doctrine of unjust enrichment, it is inequitable for UKG to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and Class Members in an unfair and unconscionable manner. UKG's retention of such benefits under circumstances making such retention inequitable constitutes unjust enrichment.

108. The benefit conferred upon, received, and enjoyed by UKG was not conferred officiously or gratuitously, and it would be inequitable and unjust for UKG to retain the benefit.

109. UKG is therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on UKG as a result of its wrongful conduct, including specifically the value to UKG of the PII that was stolen and the payroll systems that were compromised in the UKG data breach and the profits UKG is receiving from the use, sale, and processing of that information, including any profits from its timekeeping and payroll services.

COUNT III

BREACH OF CONTRACT

(On behalf of all Nationwide and California Data Breach Class and Subclass)

110. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

111. UKG's privacy policy is an agreement between UKG and its customers as well as the employees of its customers, who include Plaintiff and Class Members, and who provided their PII to UKG.

112. This privacy policy applied to Plaintiff and Class Members who

accepted UKG's promise and entered into a contract with UKG when they entrusted their highly sensitive and confidential e-PHI to UKG as part of a transaction for medical goods and services.

113. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of UKG's breach of contract.

COUNT IV

COMMON LAW INVASION OF PRIVACY – INTRUSION UPON SECLUSION

(On behalf of the Nationwide and California Data Breach Class and Subclass)

114. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

115. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

116. UKG intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and Class Members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's and Class Members' PII. Only UKG had control over its systems.

117. UKG's conduct is especially egregious and offensive as they failed to have any adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and Class Members' information.

118. At all times, UKG was aware that Plaintiff's and Class Members' PII in their possession contained highly sensitive and confidential PII, including but not limited to name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers.

119. Plaintiff and Class Members have a reasonable expectation in their e-

PHI, which contains highly sensitive medical information.

120. UKG intentionally configured their systems in such a way that stored Plaintiff's and Class Members' PII to be left vulnerable to malware/ransomware attack without regard for Plaintiff's and Class Members' privacy interests.

121. The disclosure of the sensitive and confidential PII of hundreds of thousands of employees, was highly offensive to Plaintiff and Class Members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

122. UKG's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. UKG's conduct would be especially egregious to a reasonable person as UKG publicly disclosed Plaintiff's and Class Members' sensitive and confidential PII, including but not limited to name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers, without their consent, to an "unauthorized person," i.e., hackers.

123. As a result of UKG's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

124. Plaintiff and Class Members have been damaged as a direct and proximate result of UKG's intrusion upon seclusion and are entitled to just compensation.

125. Plaintiff and Class Members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened risk of future invasions of privacy.

COUNT V

INVASION OF PRIVACY

ART. I, SEC 1 OF THE CALIFORNIA CONSTITUTION

(On behalf of the Nationwide and California Data Breach Class and Subclass)

126. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

127. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

128. The right to privacy in California's constitution creates a private right of action against private and government entities.

129. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

130. UKG violated Plaintiff's and Class Members' constitutional right to privacy by collecting, storing, and disclosing their PII in which they had a legally protected privacy interest, and in which they had a reasonable expectation of privacy in, in a manner that was highly offensive to Plaintiff and Class Members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

131. UKG has intruded upon Plaintiff's and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential PII.

132. UKG's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived

Plaintiff and Class Members of the ability to control the circulation of their PII, which is considered fundamental to the right to privacy.

133. Plaintiff and Class Members had a reasonable expectation of privacy in that: (i) UKG's invasion of privacy occurred as a result of UKG's security practices including the collecting, storage, and unauthorized disclosure of its customers' employees' PII; (ii) Plaintiff and Class Members did not consent or otherwise authorize UKG to disclosure their PII; and (iii) Plaintiff and Class Members could not reasonably expect UKG would commit acts in violation of laws protecting privacy.

134. As a result of UKG's actions, Plaintiff and Class Members have been damaged as a direct and proximate result of UKG's invasion of their privacy and are entitled to just compensation.

135. Plaintiff and Class Members suffered actual and concrete injury as a result of UKG's violations of their privacy interests. Plaintiff and Class Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

136. Plaintiff and the Class seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as disgorgement of profits made by UKG as a result of its intrusions upon Plaintiff's and Class Members' privacy.

COUNT VI

Violation of the California Consumer Privacy Act, Cal. Civ. Code §§1798.100 *et seq.*)

(On behalf of the California Data Breach Subclass)

137. Plaintiff re-alleges and incorporates by reference all preceding

allegations as if fully set forth herein.

138. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted PII, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's 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 any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

139. UKG is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million. Indeed, its revenue reaches into the many billions per year.

140. Plaintiff and Class Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

141. The PII of Plaintiff and Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the PII UKG collects and which was impacted by the data breach includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport

number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

142. UKG knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's and Class Members' PII and that the risk of a data breach or theft was highly likely. UKG failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and the Class Members. Specifically, UKG subjected Plaintiff's and Class Members' nonencrypted and nonredacted PII to an unauthorized access and exfiltration, theft, or disclosure as a result of the UKG's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

143. As a direct and proximate result of UKG's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and Class Members' PII included exfiltration, theft, or disclosure through UKG's servers, systems, and website, and/or the dark web, where hackers further disclosed UKG's customers' and their employees' PII.

144. As a direct and proximate result of UKG's acts, Plaintiff and Class Members were injured and lost money or property, including but not limited to lost wages due to the disabling of their payroll and timekeeping services, the loss of Plaintiff' and the Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses described above.

145. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiff and Class Members by way of this Complaint seek actual pecuniary damages suffered as a result of UKG's violations described herein. Plaintiff has issued a notice of these alleged violations pursuant to § 1798.150(b) and intends to amend this Complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

COUNT VII

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT, Cal. Civ. Code §§ 1798.80 et seq.,

(On Behalf of the California Data Breach Subclass)

146. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

147. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that PII about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain PII about Californians to provide reasonable security for that information."

148. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains PII about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure."

149. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

150. Plaintiff and Class Members are "customers" within the meaning of

Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided PII to UKG, directly and/or indirectly through their employers, for the purpose of obtaining a service from UKG.

151. The PII of Plaintiff and Class Members' at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the PII UKG collects and which was impacted by the data breach includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

152. UKG knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and that the risk of a data breach or theft was highly likely. UKG failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and Class Members. Specifically, UKG failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII of Plaintiff and Class Members from unauthorized access, destruction, use, modification, or disclosure. UKG further subjected Plaintiff's and Class Members' nonencrypted and nonredacted PII to an unauthorized access and exfiltration, theft, or disclosure as a

result of the UKG's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

153. As a direct and proximate result of UKG's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the PII of Plaintiff and the Class Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the PII of Plaintiff and Class Membersby the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

154. As a direct and proximate result of UKG's acts or omissions, Plaintiff and Class Members were injured and lost money or property, including but not limited to lost wages due to the disabling of their payroll and timekeeping services, the loss of Plaintiff's and Class Members'legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

COUNT VIII

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200, *et seq.*

(On Behalf of the California Data Breach and Payroll Subclasses)

155. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

156. UKG is a "person" as defined by Cal. Bus. & Prof. Code §17201.

157. UKG violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

158. UKG's business acts and practices are "unlawful" under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.* ("UCL"), because, as

alleged above, UKG violated the California common law, California Constitution, and the other state and federal statutes and causes of action described herein.

159. UKG's business acts and practices are "unfair" under the UCL, because, as alleged above, California has a strong public policy of protecting individuals' privacy interests, including protecting individuals' personal data. UKG violated this public policy by, among other things, engaging in unfair business practices because it made material misrepresentations and omissions concerning the information that UKG assured patients it would protect their highly sensitive and confidential e-PHI, which deceived and misled patients. UKG's conduct violates the policies of the statutes referenced herein.

160. UKG's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of UKG's collecting, storing, disclosing, and otherwise misusing Plaintiff's and Class Members' PII is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiff and Class Members were completely unaware of UKG's conduct, they could not have possibly avoided the harm.

161. UKG's business acts and practices are also "fraudulent" within the meaning of the UCL. UKG misrepresented that it maintained sufficient data security measures and systems to protect Plaintiff's and Class Members' PII. UKG never disclosed that these practices were severely deficient.

162. UKG's unlawful, unfair, and deceptive acts and practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, which was a direct and proximate cause of the data breach and omitting, suppressing, and concealing the material fact of that failure;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve

security and privacy measures following well-publicized cybersecurity incidents, which was a direct and proximate cause of the data breach and omitting, suppressing, and concealing the material fact of that failure;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, and CIPA, which was a direct and proximate cause of the data breach and omitting, suppressing, and concealing the material fact of that failure;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act and CIPA;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

(g) 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 Plaintiff's and Class Members' PII, including duties imposed by the FTC Act and CIPA.

163. UKG's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of UKG's data security and ability to protect the confidentiality of Plaintiff's and Class Members' PII.

164. As a direct and proximate result of UKG's unfair, unlawful, and

fraudulent acts and practices, Plaintiff and Plaintiff's and Class Members were injured and lost money or property, i.e., lost wages, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, as well as the costs passed through from UKG to its customers and their employees for their timekeeping and payroll services; fees and interest incurred as a result of the loss of wages; time and expenses related to tracking the amount of said lost wages; costs to be spent for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

165. UKG's violations were, and are, willful, deceptive, unfair, and unconscionable.

166. Plaintiff and Class Members have lost money and property as a result of UKG's conduct in violation of the UCL, as stated in herein and above.

167. By deceptively storing, collecting, and disclosing their PII, UKG has taken money or property from Plaintiff and Class Members.

168. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; restitution; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT IX

REQUEST FOR RELIEF UNDER THE DECLARATORY JUDGMENT ACT

28 U.S.C. § 2201, *et seq.*

(On Behalf of all Classes)

169. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

170. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the

parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

171. An actual controversy has arisen in the wake of the data breach regarding UKG'S present and prospective common law and statutory duties to reasonably safeguard Plaintiff and Class Members' personal informaiton and whether UKG is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches. Plaintiff alleges that UKG's data security practices remain inadequate.

172. Plaintiff and Class Members continue to suffer injury as a result of the compromise of PII and remain at imminent risk that further compromises of their PII will occur in the future.

173. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that UKG continues to owe a legal duty to secure consumers' PII, to timely notify Plaintiff and Class Members of any data breach, and to establish and implement data security measures that are adequate to secure Plaintiff and Class Members' PII.

174. The Court also should issue corresponding prospective injunctive relief requiring UKG to employ adequate security protocols consistent with law and industry standards to protect Plaintiff and Class Members' PII.

175. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another breach at UKG occurs, Plaintiff and Class Members will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

176. The hardship to Plaintiff and Class Members if an injunction does not issue greatly exceeds the hardship to UKG if an injunction is issued. If another data

breach occurs at UKG, Plaintiff and Class Members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to UKG of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and UKG has a pre-existing legal obligation to employ such measures.

177. Issuance of the requested injunction will serve the public interest by preventing another data breach at UKG, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

RELIEF REQUESTED

Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Defendants including the following:

A. Determining that this matter may proceed as a class action and certifying the Class asserted herein;

B. Appointing Plaintiff as representative of the applicable Classes and appointing Plaintiff's counsel as Class counsel;

C. An award to Plaintiff and the Class of compensatory, consequential, nominal, statutory, and treble damages as set forth above;

D. Ordering injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) provide several years of free credit monitoring and identity theft insurance to all Class Members; and (iv) timely notify consumers of any future data breaches;

E. Entering a declaratory judgment stating that Defendants owe a legal duty to secure Plaintiff's and Class Members' PII and data, to timely notify Plaintiff and Class Members of any data breach, and to establish and implement data security measures that are adequate to secure their PII and data;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: March 4, 2022

/s/ Ronald A. Marron

Ronald A. Marron (175650)
Alexis M. Wood (270200)
Kas L. Gallucci (288709)
Elisa Pineda (328285)
LAW OFFICES OF RONALD A. MARRON
651 Arroyo Drive
San Diego, CA 92103
Tel: (619) 696-9006
Fax: (619) 564-6665
ron@consumersadvocates.com
alexis@consumersadvocates.com
kas@consumersadvocates.com
elisa@consumersadvocates.com

Attorneys for Plaintiff and the Proposed Classes

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

ADAM BENTE, individually and on behalf of all others similarly situated and the general public,

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Law Offices of Ronald A. Marron, 651 Arroyo Drive, San Diego, CA 92103, Telephone: 619-696-9006

DEFENDANTS

UKG, INC.,

County of Residence of First Listed Defendant San Diego 28 U.S.C. 1391(c)(2)
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

'22CV289 GPC WVG

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	☐ 880 Defend Trade Secrets Act of 2016	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	SOCIAL SECURITY	☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 861 HIA (1395ff)	☐ 485 Telephone Consumer Protection Act
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 196 Franchise				☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
				☐ 864 SSID Title XVI	☒ 890 Other Statutory Actions
				☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS			☐ 893 Environmental Matters
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	**Habeas Corpus:**		FEDERAL TAX SUITS	☐ 895 Freedom of Information Act
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee		☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 896 Arbitration
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence		☐ 871 IRS—Third Party 26 USC 7609	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General			☐ 950 Constitutionality of State Statutes
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty	IMMIGRATION		
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	**Other:**	☐ 462 Naturalization Application		
	☐ 448 Education	☐ 540 Mandamus & Other	☐ 465 Other Immigration Actions		
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332(d)(2) CAFA Diversity

Brief description of cause:
Data breach related class action claims for unauthorized exposure of personal information and loss of wages due to loss of vendor services.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ over $5 million

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions):*

JUDGE _____ DOCKET NUMBER _____

DATE
March 4, 2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ Ronald A. Marron

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

Exhibit 1

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

SCOPE

This Privacy Notice (“Notice”) describes UKG’s privacy practices in connection with the use of UKG’s websites, products, services, and any associated applications (“Services”). The Notice also provides information about the choices you have regarding the collection or use of your Personal Information (“PI”) and the rights provided to you, including the ability to access or update information about you.

What Does This Notice Cover?

The Notice applies to PI provided or collected through the use of UKG’s Services by customers, employees, job applicants and/or website visitors. For purposes of this Notice, PI means information collected by UKG, relating to an Identified or Identifiable natural person.

Which Privacy Notice Is Applicable?

Our Customer’s Notice applies when you:

- Use a customer-branded sign-on page; and
- Are an applicant creating a profile or applying for a position with our customer.

This Notice applies when you:

- Use a UKG-branded sign-on page; and
- Are an applicant creating a profile or applying for a position with UKG.

Links to Non-UKG Websites

UKG's websites might contain links to third-party sites for your convenience and/or information. When you access those links, you leave UKG's website and are redirected to a third-party site. UKG does not control third-party sites. The privacy practices of third parties might differ from UKG's privacy practices. We do not endorse or make any representations about third-party websites. When you share PI with third-party websites, the third-party processing is not covered by this Privacy Notice. We encourage you to review the privacy policy of any website or company before sharing PI with them.

CALIFORNIA RESIDENTS - CALIFORNIA PRIVACY NOTICE

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

Information We Collect:

UKG collects PI from several different sources, including:

- Directly from a website visitor, prospects, customers, applicants, or employee;
- Directly or indirectly from website visitors, customers, vendors, service providers or other third parties; and
- From your use, visit or activity on any of our websites or products.

Please review each of the sections below to learn more about how UKG collects PI, and what PI is collected.

Website Visitors

How Do We Collect Personal Information?

UKG collects PI about a website visitor when the visitor visits our website and when the visitor chooses to provide PI. For example, we collect information when you visit our website and when you contact us via our website, provide your email, phone or other similar information, such as the information that you provide when you sign up for a webinar.

What Is collected?

The PI collected from a website visitor includes:

- Name;
- Company;
- Job Title;
- Address;
- Phone Number; and
- Email Address.

Children

We do not knowingly collect PI from children under the age of 13. If you are under the age of 13, please do not submit any PI to UKG. If you have reason to believe that a child under the age of 13 has provided his/her PI to UKG, please contact us in accordance with Section 14 of this Notice, and we will endeavor to delete that information from our databases.

UKG Job Applicants and Employees

How Do We Collect Personal Information?

UKG collects PI about a job applicant when an application for employment with UKG is completed. Additionally, UKG collects information about individuals who create a profile on our website, regardless of whether or not an application is completed.

If hired by UKG following an application, additional information is collected during the onboarding process and throughout the employment relationship. We may also collect information that you have voluntarily made public and/or shared on publicly visible accounts, such as social media platforms.

What Is collected?

The PI collected from an applicant or employee of UKG includes, but is not limited to:

- Personal Identifiers (Name, Address, Age, Date of Birth, Social Security Number);
- Professional or Employment-related Information (Employment Record, Salary);
- Education Information; and

- Personal/Professional Contact information.

Customers' Information (and the Information of Their Employees and Job Applicants)

How Do We Collect Personal Information?

When using our products and services, our customers are solely responsible for determining what PI is collected regarding their employees or job applicants. UKG processes information solely at the direction of its customers and has no direct relationship with the individuals (our customers' employees and applicants) whose PI we process.
The information may be collected through our SaaS solution, by members of our support team who provide support to customers, or by subprocessors engaged by UKG to provide you with the Services. For employees of customers who use Kronos terminals with a biometric or finger scanning device for employee timekeeping, please see the Biometric Data Privacy section of this Notice.

What Is collected?

The PI processed by UKG on behalf of our customers varies, but includes information such as name, company name, address, email address, time and attendance and schedule information, and Social Security Numbers. Please contact your employer or the company with whom you applied to learn more about the information they collect for use with UKG's products and services.

Mobile Application Users

How Do We Collect Personal Information?

UKG collects PI about a user of our mobile application when the user chooses to provide such information. We also collect information about you through the use of mobile analytics software.

What Is Collected?

Our mobile application may record information concerning how often you use the application, the events that occur within the application, aggregated usage, performance data, your location, the type of device used, and from where the application was downloaded. We do not link the information we store within the analytics software to any PI you submit within the mobile application.

Website Activity, Cookies and Other Tracking Technologies

How Do We Collect Personal Information?

UKG collects information through the use of website tracking software, as well as from your use o activity on any of our websites, utilizing cookies and other tracking technologies.

What is Collected?

The website tracking software automatically captures technical information that is stored in our server's log files. For example, when you visit our websites, We and our partners store and access non-sensitive information from your device, such as cookies or a unique device identifier, and process PI such as your IP address, device manufacturer and model, the type of browser being used, the web pages visited, and the amount of time spent on our website.

To learn more about our use of Cookies and other tracking technologies, please visit our Cookies and Other Tracking Technologies section.

Social Media Features and Widgets

How Do We Collect Personal Information?

Our websites may include social media features, such as video links, "Like" buttons, and widgets such as "Share" buttons or interactive mini-programs, and may set a cookie to enable the feature to function. Social media features and widgets may be hosted by a third party or hosted directly on our websites. Your use and interactions with these features are at your discretion, and are governed by the privacy policy of the companies providing them.

What Is collected?

These features may collect your PI such as your IP address and which website page you are visiting.

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

Why We Use Your Personal Information:

UKG uses PI for several purposes, including:

- To communicate with you regarding our products and/or services;
- To fulfill the purpose(s) for which the information was collected/provided, including providing contractually-obligated products and/or services;
- To improve our website, products and services, through testing, research, analysis and product development;
- For security purposes, such as to prevent unauthorized access or disclosure, to maintain data accuracy, to protect the confidentiality, integrity and availability of your PI and to allow only the

appropriate use of your PI; and
- To comply with all applicable legal obligations.

Please review each of the sections below to learn more about how we use your PI.

Website Visitors

How Do We Use Your Personal Information?

The PI you provide when using our website will be used in accordance with this Privacy Notice. We use your PI to fulfill requests for information about our products and services and to enable you to register and participate in events that we sponsor (including webinars).

UKG Job Applicants and Employees

How Do We Use Your Personal Information?

We use PI of our job applicants and employees for legitimate human resource business purposes, such as:

- Payroll administration;
- Filling open employment positions;
- Maintaining accurate benefits records;
- Complying with governmental reporting requirements;
- Performance management;
- Provision of company network access;
- Authentication of individuals; and
- Security, health and safety management.

Customers' Information (and the Information of Their Employees)

How Do We Use Your Personal Information?

We use your PI to provide you with services, which UKG is contractually obliged to provide to you, to improve these services or communicate with you about our products or services. For employees of customers who use UKG terminals with a biometric or finger scanning device for employee timekeeping, please see the Biometric Data Privacy section of this Notice.

Website Activity, Cookies and Other Tracking Technologies

How Do We Use Your Personal Information?

In order to improve the content and format of our site, UKG uses website tracking software to automatically capture technical information that is then stored in our server's log files. UKG and its partners also utilize cookies and other tracking technologies to measure the preferences of our website visitors, analyze trends, administer the website, track users' movements around the website, and to gather demographic information about our user base as a whole. Please visit our Cookies section below to learn more.

Mobile Application

How Do We Use Your Personal Information?

UKG uses mobile analytics software to allow us to better understand the functionality of our Mobile Software on your phone. We do not link the information we store within the analytics software to any PI you submit within the mobile application.

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

We do not sell PI to third parties. Please review each of the sections below to learn more about how we might disclose your PI.

Affiliates and Subsidiaries:

We might share your PI with our Affiliates and Subsidiaries in order to deliver a product or service complete a task that you requested.

Third Parties (Vendors/Service Providers):

We might engage with third parties (vendors and/or service providers) in order to deliver a product or service (or perform certain functions such as enhancing and/or delivering our product and service offerings) or complete a task that you requested.

We have contracts with third-party providers (vendors and/or service providers) to perform certain functions on our behalf, and only at our direction. Our third parties are bound by confidentiality agreements, only have access to your PI to the extent necessary to provide these contracted services and are only permitted to process your PI in accordance with our instructions (and for the purposes we disclose).

Additional Disclosures

UKG might disclose your PI if we in good faith believe that such action is necessary to:

- Comply with the law or with legal process;
- Protect and defend our rights and property;
- Protect against misuse or unauthorized use of our website;
- Protect the personal safety or property of our users or the public (among other things, this means that if you provide false information or attempt to pose as someone else, information about you may be disclosed as part of any investigation into your actions).

Other than as stated in this Privacy Notice, we will endeavor not to release your PI to unknown or unaffiliated third parties, and we will not cross-reference your PI with that of any other customer or entity.

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

International Transfers

UKG complies with the EU General Data Protection Regulation regarding the transfer of PI from the EU to the U.S. For transfers of PI originating in the EU to UKG for processing by UKG in a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing ‘adequate’ data protection, UKG agrees it will (a) provide at least the same level of privacy protec for PI originating in the EU as required under the U.S.-EU and U.S.-Swiss Privacy Shield frameworks; or

(b) use the form of the Controller-to-Processor Standard Contractual Clauses ("SCCs") currently approved. To facilitate cross-border transfers, such as between the EU, Switzerland, and the United Kingdom and the U.S., we rely on other mechanisms such as Standard Contractual Clauses (SCC) to ensure that appropriate privacy protections and safeguards for personal information are in place.

To learn more about how UKG complies with the Schrems II caselaw, please refer to UKG's Transfer Risk and Impact Statement.

Privacy Shield

UKG complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (Privacy Shield) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom and/or Switzerland, as applicable. UKG has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. To learn more about the Privacy Shield program, and to view our certification, please visit the Privacy Shield website.

UKG is responsible for the processing of PI we receive, defined as any operation or set of operations which is performed upon PI, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, it receives, under the applicable Privacy Shield Framework, and, on occasion, subsequently transfers to a third party acting as an agent on its behalf. UKG complies with the Privacy Shield Principles for all onward transfers of PI from the European Union, the United Kingdom and/or Switzerland, including the onward transfer liability provisions.

With respect to PI received or transferred pursuant to the Privacy Shield Frameworks, UKG is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, UKG may be required to disclose PI in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

APEC

UKG's privacy practices, described in this Privacy Notice, comply with the APEC Cross Border Priv Rules System (CBPR). The APEC CBPR system provides a framework for organizations to ensure t protection of Personal Information transferred among participating APEC economies. More

information about the APEC framework can be found here.

RETENTION OF PERSONAL INFORMATION

COOKIES AND OTHER TRACKING TECHNOLOGIES

BIOMETRIC DATA

DATA SUBJECT RIGHTS

SECURITY

ENFORCEMENT AND VERIFICATION

CHANGES TO THIS PRIVACY NOTICE

CONTACT INFORMATION

CALIFORNIA RESIDENTS - CALIFORNIA PRIVACY NOTICE

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

UKG will only retain PI for the length of time necessary to fulfill the purpose(s) for which the information was collected or as required or permitted by applicable laws, (including the resolution of disputes) and in accordance with our customer contracts.

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

What Are Cookies?

A cookie is a small amount of data which our website stores on your computer, and which we can later retrieve. The cookie cannot be read by a site other than ours. As discussed in our section on Use of Your PI, we use cookies for a number of administrative purposes, including to store your preferences, allowing us to provide website visitors with a better experience.

How Can You Manage the Use of Cookies?

UKG Privacy Center: When you visit our website, you can make choices about our usage of cookies, by navigating to the bottom of our website and clicking “cookie consent choices” or by clicking “Learn More” on the pop-up banner. You also have the option of viewing our existing partners and authorizing or blocking their collection and use of your PI.

Managing Flash Cookies

To manage Flash cookies, please click here.

Managing Cookies Through Your Browser

You can monitor our use of cookies on your computer by setting your Web browser to inform you when cookies are set, or you can prevent the cookies from being set entirely. The “help” portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Please understand that if you disable the use of cookies on your computer, you may be unable to access certain portions or services on our websites.

Advertising and Analytics Cookies

We work with third parties to manage our advertising on other sites. These third parties might use cookies or other similar technologies to provide you advertising based upon your browsing activities and interests. We use standard Google Analytics for general site analytics. To learn more about how Google uses data from sites that use their services, click here.

We have also implemented the following Google Analytics Advertising features for our paid advertising:

- Google Display Network Impression Reporting;
- Google Analytics Demographics and Interest Reporting; and
- Integrated services that require Google Analytics to collect data for advertising purposes, including the collection of data via advertising cookies and identifiers.

If you wish to opt-out of the Google Analytics Advertising features that we use, click here.

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

As previously stated, UKG does not collect or control customer employee data. For customers who use UKG terminals with a biometric or finger scanning device, the collection of customer employee finger scan data is undertaken and controlled by the customer. Our customers collect such employee data through their use of the finger scanning devices and related software, and either store the data at the customer controlled site or on secure space (in accordance with applicable law) made available by UKG in a cloud environment for that purpose.

This data is used by the customer for employee verification in connection with its employee timekeeping purposes. Such data consists solely of templates created from mathematical algorithms, not fingerprints. Customer employee finger scan data, or templates as described above, may be among the customer employee data collected or stored by UKG customers.

A copy of UKG's data security policy applicable to the secure space on which customers can store employee data can be accessed at: www.kronos.com/security. UKG has put reasonable measures in place to minimize its access to customer employee finger scab data from its customers. On the rare occasions when UKG accesses customer employee finger scan data (e.g. for technical support), it is done pursuant to a customer's instruction, and subject to strict handling procedures, and UKG permanently destroys such data promptly after the specific purpose for accessing the data has been satisfied. Customers are responsible for destroying customer employee finger scan data that they collect, control, possess or store. Any questions regarding customer biometric or finger scan employee data, including any applicable retention schedule or destruction process, should be directed to the appropriate employer.

DATA SUBJECT RIGHTS

SECURITY

ENFORCEMENT AND VERIFICATION

CHANGES TO THIS PRIVACY NOTICE

CONTACT INFORMATION

CALIFORNIA RESIDENTS - CALIFORNIA PRIVACY NOTICE

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

UKG will take reasonable steps to ensure that all PI of UKG employees, job applicants and website visitors is accurate and complete for the intended use. As previously stated, we will only use PI in ways that are consistent with the purposes for which it was collected, as required or permitted by law, or as you might subsequently authorize.

In accordance with all applicable law, we enable you to exercise some or all of the following rights regarding our collection, use, and sharing of your PI:

- Access the PI we maintain about you;
- Update or correct any inaccurate or incomplete PI about you;
- Request that we delete your PI;
- Object to or restrict the processing of your PI;
- Receive the PI you have previously provided to UKG, in a machine-readable format, allowing you to transfer that PI to another company at your discretion;
- Not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you; and
- File a complaint directly with the relevant Supervisory Authority about how we process your PI.

Exercising Your Rights

To protect your privacy and security, we take reasonable steps to verify your identity, before granting access to your PI. Please follow the instructions below based on your relationship with UKG, and provide the requested information to allow us to adequately address your request. We will respond to your request within a reasonable timeframe.

If you are a resident of California, please review our CCPA Notice here.

Web Visitors

If you are a Non-California resident and would like to request access to your Personal Information, and/or request erasure (right to be forgotten) of PI previously provided, please click here.

UKG Job Applicants and Employees

If you are a current or former employee or you previously applied for employment with UKG (including Ultimate Software, Kronos, and their respective subsidiaries), and reside in the European Union, Switzerland or the United Kingdom, and would like to request access to your PI, and/or request erasure (right to be forgotten) of PI previously provided, you may submit your request via email at privacy@ukg.com.

For current and previous UKG employees, please indicate the right you are exercising. In order to verify your identity, your request must include the following:

- Your full name and email address associated with your profile;
- Your preferred contact number; and
- Your hire date, which can be found by current or former employees (up to one year following termination) within your profile, or on your offer letter. We require your hire date to be provided in the MM/DD/YY format.

If you previously applied for employment with UKG, please indicate the right you are exercising. In order to verify your identity, your request must include the following:

- Your full name and email address associated with your profile;
- Your preferred contact number; and
- The number of employment opportunities you have applied for with UKG, as well as the Job Title and Job Code associated with each application, which can be found in your profile, under the Applications tab.

Our Customer's Job Applicants and Employees

When processing PI on behalf of a customer, UKG has no direct business relationship with the individuals whose PI it processes (applicants or employees of our customers).

If you are a current or former employee or job applicant of one of UKG's customers, please contact your employer/former employer/company you applied with directly to exercise your rights relating to your PI. As a processor, UKG does not respond to requests from our customer's applicants or employees unless that customer is no longer in business.

Denial of Requests

UKG may deny a request relating to a Data Subject's individual rights as permitted by applicable law. UKG will endeavor to timely notify you regarding any decision and reason(s) for denial.

Dispute Resolution

In accordance with this Notice, UKG will investigate and attempt to resolve complaints and disputes regarding the use and disclosure of your PI. Additionally, UKG agrees to cooperate with Data Protection Authorities within the European Union and the Federal Data Protection and Information Commissioner in Switzerland, or authorized representatives for disputes specific to Human Resource information received from the European Union, the United Kingdom and Switzerland.

Any privacy-related dispute or concern that is still unable to be resolved to your satisfaction shall be handled in accordance with applicable dispute resolution procedures through our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

We strongly encourage you to raise any complaints you may have with regard to this Privacy Notice and/or our activation of this Notice to us prior to proceeding to the arbitration procedure described in the prior paragraph.

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

SECURITY

To prevent unauthorized access or disclosure, to maintain data accuracy, and to allow only the appropriate use of your PI, UKG utilizes physical, technical, and administrative controls and procedures to safeguard the information we collect.

To protect the confidentiality, integrity, availability and resilience of your PI, we utilize a variety of physical and logical access controls, firewalls, intrusion detection/prevention systems, network and database monitoring, anti-virus, and backup systems. We use encrypted sessions when collecting or transferring sensitive data through our websites.

We limit access to your PI and data to those persons who have a specific business purpose for maintaining and processing such information. Our employees who have been granted access to your PI are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.

ENFORCEMENT AND VERIFICATION

CHANGES TO THIS PRIVACY NOTICE

CONTACT INFORMATION

CALIFORNIA RESIDENTS - CALIFORNIA PRIVACY NOTICE

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

SECURITY

ENFORCEMENT AND VERIFICATION

UKG will periodically assess its operations to validate compliance with this Privacy Notice.

When we have knowledge that one of our employees or third parties is using or disclosing PI in a manner contrary to this Privacy Notice, we will take reasonable steps to prevent or stop the use or disclosure. We hold our employees and third parties accountable for maintaining the trust that our customers place in us.

CHANGES TO THIS PRIVACY NOTICE

CONTACT INFORMATION

CALIFORNIA RESIDENTS - CALIFORNIA PRIVACY NOTICE

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

SECURITY

ENFORCEMENT AND VERIFICATION

CHANGES TO THIS PRIVACY NOTICE

This Notice describes our current PI protection policies approved on October 1, 2021. UKG reserves the right to modify or amend this Notice at any time consistent with applicable laws. We encourage you to periodically review this page for the latest information on our privacy practices.

CONTACT INFORMATION

CALIFORNIA RESIDENTS - CALIFORNIA PRIVACY NOTICE

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

SECURITY

ENFORCEMENT AND VERIFICATION

CHANGES TO THIS PRIVACY NOTICE

CONTACT INFORMATION

At any time, you may contact UKG with questions or concerns about this Privacy Notice at privacy@ukg.com.

Written responses may also be submitted to:

Ultimate Kronos Group
Attention: VP Deputy General Council
900 Chelmsford St.
Lowell, MA 01851

Those residing in the EU may contact our Data Protection Officer (DPO) via email at privacy@ukg.com. The DPO also serves as UKG's representative in Europe and is located at:

Ultimate Kronos Group
Attention: Data Privacy Officer
53 rue d'Hauteville
75010 Paris, France

UKG will respond to all correspondence within a reasonable timeframe, including as required by applicable law.

CALIFORNIA RESIDENTS - CALIFORNIA PRIVACY NOTICE

Privacy Notice

Protecting Your Personal Information

UKG Inc., comprised of Ultimate Software, Kronos, and their respective subsidiaries (collectively, “UKG”, “we” and/or “us”) are committed to protecting the privacy of the individuals who visit our website (“Visitors”) and individuals who use UKG’s Services (“Users” and/or “you”) as an employee or applicant of UKG or one of its customers.

The California Consumer Privacy Act ("CCPA") provides certain privacy-related rights to California residents. Please click here to learn more about UKG's privacy practices and compliance with the CCPA.

ClassAction.org
