JASON M. WUCETICH (STATE BAR NO. 222113)
jason@wukolaw.com
DIMITRIOS V. KOROVILAS (STATE BAR NO. 247230)
dimitri@wukolaw.com
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201

MICHAEL S. MORRISON (SBN 205320)
mmorrison@amfllp.com
ERIN A. LIM (SBN 323930)
elim@amfllp.com
ALEXANDER MORRISON + FEHR LLP
1900 Avenue of the Stars, Suite 900
Los Angeles, CA 90067
Telephone: (310) 394-0888
Facsimile: (310) 394-0811

Attorneys for Plaintiffs
WILLIAM MULLER and ANTONIO KNEZEVICH,
individually and on behalf of all others similarly situated

[*Additional Counsel Listed on Next Page*]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE UKG INC CYBERSECURITY LITIGATION

THIS DOCUMENT RELATES TO:

All Actions

CASE NO. 22-CV-00346-SI

CLASS ACTION

CONSOLIDATED COMPLAINT FOR:

(1) NEGLIGENCE
(2) NEGLIGENCE PER SE
(3) UNJUST ENRICHMENT
(4) DECLARATORY JUDGMENT
(5) BREACH OF CONTRACT
(6) VIOLATION OF THE CAL. CONSUMER PRIVACY ACT, CAL. CIV. CODE § 1798.150
(7) VIOLATION OF THE CAL. CUSTOMER RECORDS ACT, CAL. CIV. CODE § 1798.84
(8) VIOLATION OF THE CAL. UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200
(9) VIOLATION OF THE RIGHT TO PRIVACY, CAL. CONST. ART. 1, § 1

DEMAND FOR JURY TRIAL

RONALD A. MARRON (SBN 175650)
ron@consumesradvocates.com
ALEXIS M. WOOD (SBN 270200)
alexis@consumersadvocates.com
KAS L. GALLUCCI (SBN 288709)
kas@consumersadvocates.com
LAW OFFICES OF RONALD A. MARRON
651 Arroyo Drive
San Diego, CA 92103
Tel: (619) 696-9006
Fax: (619) 564-6665

Attorneys for Plaintiff
ADAM BENTE, individually and on behalf of all others similarly situated

JONATHAN M. LEBE (SBN 284605)
jon@lebelaw.com
ZACHARY T. GERSHMAN (SBN 328004)
zachary@lebelaw.com
NICOLAS W. TOMAS (SBN 339752)
nicolas@lebelaw.com
LEBE LAW
777 S. Alameda Street, Second Floor
Los Angeles, CA 90021
Tel: (213)444-1973

Attorneys for Plaintiffs
CINDY VILLANUEVA, individually and on behalf of all others similarly situated

Pursuant to this Court's May 20, 2022, order on consolidation, Plaintiffs William Muller, Antonio Knezevich, Adam Bente, and Cindy Villanueva (collectively referred to herein as "Plaintiffs"), individually and on behalf of all others similarly situated, hereby bring this consolidated class action complaint against defendant UKG Inc. ("UKG") as follows:

SUMMARY OF THE CASE

1. This putative class action arises from UKG's negligent failure to implement and maintain reasonable cybersecurity procedures and practices with respect to the sensitive and confidential personal information UKG obtains from its customers' employees, the consequent massive cybersecurity breach of its systems that began in December 2021, and the resultant shut down of timekeeping and payroll services that lasted for months and continued through the filing of the initial complaints in the cases underlying this consolidated action. UKG is a multi-billion-dollar workforce management technology company that provides third-party human resources services, including timekeeping and payroll services, to companies around the globe. In connection with those services, UKG collects, stores, and processes personal information and data for thousands of companies and millions of workers, including a multitude of companies and workers in California and throughout the nation. UKG's clients form a broad cross section of corporate America 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, including Family Health Centers of San Diego and Wellpath

Recovery Solutions, LLC.

2. Due to its lack of adequate cybersecurity measures, UKG suffered a ransomware attack and data breach on or around December 11, 2021. That breach not only exposed workers' personal information to cybercriminals, but also crippled timekeeping and payroll systems for millions of employees, resulting in workers who were not paid, paid late, or paid incorrectly. To compound the matter, the timing of the breach left workers worrying about these financial issues and data concerns in the midst of the holiday season, wondering if they would be able to make ends meet and how long the problem would continue. Those worries proved concrete, as UKG took months to purportedly rectify its security problems.

3. Plaintiffs, who are each employees of UKG's various customers and were impacted by the breach and whose wages were affected, bring this class action complaint to redress these injuries, on behalf of themselves and a nationwide class and California subclass of similarly situated persons. Plaintiffs assert claims on behalf of a nationwide class for negligence, negligence per se, unjust enrichment, declaratory judgment, breach of contract, and common law invasion of privacy. Plaintiffs also bring claims on behalf of a California subclass for violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*, violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*, and for invasion of privacy based on the California Constitution, Art. 1, § 1. Plaintiffs seek, among other things, compensatory damages, punitive and exemplary damages, statutory damages pursuant to Cal. Civ. Code § 1798.150(b), injunctive relief, attorneys' fees, and costs of suit.

PARTIES

4. Plaintiff William Muller is a citizen and resident of the State of California who worked as a truck driver for New Bern Transport Corporation, an exclusive carrier and wholly-owned subsidiary of PepsiCo, during the time of the events alleged herein.

5. Plaintiff Antonio Knezevich is a citizen and resident of the State of California who worked as a truck driver for Tesla, Inc., during the time of the events alleged herein.

6. Plaintiff Adam Bente is a citizen and resident of the State of California who

worked as a business analyst for Family Health Centers of San Diego during the time of the events alleged herein.

7. Plaintiff Cindy Villanueva is a citizen and resident of the State of California who worked as a registered nurse for Wellpath Recovery Solutions, LLC, during the time of the events alleged herein.

8. On information and belief, defendant UKG Inc. is a corporation organized and existed under the laws of the State of Delaware, with dual corporate headquarters in Weston, Florida, and Lowell, Massachusetts.

9. Plaintiffs bring this action on behalf of themselves, on behalf of the general public as a Private Attorney General pursuant to California Code of Civil Procedure § 1021.5 and on behalf of a class and subclass of similarly situated persons pursuant Federal Rule of Civil Procedure 23.

JURISDICTION & VENUE

10. This Court has general personal jurisdiction over UKG Inc. because, at all relevant times, it 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. UKG regularly contracts with a multitude of businesses and organizations in California to provide continuous and ongoing human resources services, including timekeeping and payroll services. And UKG does in fact actually provide such continuous and ongoing human resources services to such companies in California.

11. Furthermore, this Court has specific personal jurisdiction over UKG Inc. because the claims in this action stem from its 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 collection, maintenance, and processing of the personal data of Californians in connection with such services, UKG's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent cybersecurity attack and security breach of such data in December 2021 that resulted from UKG's failures.

12. This Court has diversity subject matter jurisdiction under 28 U.S.C. § 1332(d) in that the mater in controversy exceeds the sum or value of $5,000,000, exclusive of interests and costs, and is a class action in which members of the class defined herein include citizens of a State different from the defendant. Specifically, defendant UKG Inc. is a citizen of the states of Delaware and/or Florida and/or Massachusetts, and the plaintiff class and/or subclasses defined herein include citizens of other states, including California.

13. Venue is proper in the Northern District of California under 28 U.S.C. § 1391 (b)(1)-(2) and (c)(2) in that defendant UKG Inc. resides within this judicial district and, alternatively, because a substantial part of the events or omissions giving rise to the claims alleged herein occurred within this judicial district, specifically UKG's provision of payroll, timekeeping, and other human resource services to a multitude of companies in California, UKG's collection, maintenance, and processing of the personal data of Californians in connection with such services, UKG's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent ransomware attack and security breach of such data in December 2021 that resulted from UKG's failure. In addition, Plaintiffs are informed and believe and thereon allege that members of the class and subclass defined below reside in the Northern District.

INTRADISTRICT ASSIGNMENT

14. Assignment to the San Francisco/Oakland divisions is proper because a substantial part of the events or omissions which give rise to the claims herein occurred within San Francisco County. Further, pursuant to Civil L. R. 3-2(c), all civil actions which arise in the counties of Alameda, Contra Costa, Del Norte, Humboldt, Lake, Marin, Mendocino, Napa, San Francisco, San Mateo, or Sonoma shall be assigned to the San Francisco/Oakland Divisions. A substantial part of the events or omissions giving rise to the claims herein occurred also within these counties and therefore assignment to the San Francisco/Oakland divisions is proper.

FACTUAL BACKGROUND

15. UKG (an acronym for Ultimate Kronos Group) is a workforce management technology company with dual headquarters in Florida and Massachusetts that provides human

resource services, including timekeeping and payroll services, to a multitude of companies worldwide. The company was founded in April 2020 as the result of a merger between Ultimate Software and Kronos Incorporated. UKG has reportedly been valued at $22 billion, generates approximately $3.5 billion in revenue per year, and is one of the largest cloud computing companies in the world. Among other products in its suite of services, UKG provides services known as the "Kronos Private Cloud" and "UKG Workforce Central," which are timekeeping and payroll services.

16. UKG provides its timekeeping and payroll services to a multitude of companies and organizations nationwide, including many that operate in California, the likes of which include, 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 Family Health Centers of San Diego and Wellpath Recovery Solutions, LLC. UKG's timekeeping and payroll services affect thousands of employers and millions of employees.

17. In connection with those services, UKG collects, stores, and processes sensitive personal data for thousands of companies and millions of workers. Through its software, UKG provides services to employers to track employees' hours, pay, and time records. In doing so, UKG retains sensitive information related to payroll records such as direct deposit information, bank account information, addresses, and social security numbers, among other things, along with the time records themselves.

18. According to its own privacy policy, available at www.ukg.com/privacy, in connection with its services, UKG collects personal information of individuals from a variety of sources, including directly from its customers and their employees. The privacy policy 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." On information and belief, UKG also collects banking information in connection with provision of direct deposit payroll processes as well as employee identification numbers.

19. As a corporation doing business in California, UKG is legally required to protect

personal information from unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction.

20. UKG knew that it was a prime target for hackers given the significant amount of sensitive personal information processed through its computer data and storage systems. Experts studying cybersecurity routinely identify companies such as UKG that collect, process, and store massive amounts of data for other companies as being particularly vulnerable to cyberattacks because of the value of the personal information that they collect and maintain and due to the massive scope of the adverse impact from a breach. UKG's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

21. 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 as described herein to ensure vulnerabilities were avoided or remedied and that Plaintiffs' and class members' data were protected.

22. Specifically, on or around the weekend of December 11, 2021, UKG experienced a massive cybersecurity breach as a result of a ransomware attack, which the company disclosed at the beginning of the next week and which was widely reported by the media on December 17, 2021.[1] The cybersecurity incident impacted, among other things, UKG's "Kronos Private Cloud", which is a data storing device for the company's services, including its timekeeping and payroll services. The cybersecurity attack came after a longstanding security flaw in widely used software across the internet, called Log4j, was made public, opening the door in many companies' systems to hackers. As a result of the cybersecurity attack, UKG's timekeeping and payroll services were disabled, crippling critical wage payment infrastructure for millions of workers.

[1] *See* https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html. (Last visited June 19, 2022).

23. In addition to payroll issues, the cybersecurity attack has also resulted in data privacy problems, as the data maintained by UKG includes social security numbers and, on information and belief, banking information, among other things. The City of Cleveland announced in a statement after the breach that UKG alerted it that social security numbers of workers may have been stolen by the hackers inside UKG's network.[2]

24. On information and belief, the personal information UKG collects and which was impacted by the cybersecurity attack includes individuals' first name or first initial and individuals' 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.

25. On December 13, 2021, UKG made the following announcement on its website:

> We are reaching out to inform you of a cyber security incident that has disrupted the Kronos Private Cloud.
>
> As we previously communicated, late on Saturday, December 11, 2021, we became aware of unusual activity impacting UKG solutions using Kronos Private Cloud. We took immediate action to investigate and mitigate the issue, and have determined that this is a ransomware incident affecting the Kronos Private Cloud — the portion of our business where UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions are deployed. At this time, we are not aware of an impact to UKG Pro, UKG Ready, UKG Dimensions, or any other UKG products or solutions, which are housed in separate environments and not in the Kronos Private Cloud.

[2] *See* https://clecityhall.com/2021/12/13/city-of-cleveland-statement-on-ultimate-kronos-group-cybersecurity-incident/ (Last visited June 19, 2022).

> We are working with leading cybersecurity experts to assess and resolve the situation, and have notified the authorities. The investigation remains ongoing, as we work to determine the nature and scope of the incident.
>
> We deeply regret the impact this is having on you, and we are continuing to take all appropriate actions to remediate the situation. We recognize the seriousness of this issue and will provide another update within the next 24 hours.[3]

26. UKG later made updates to its website postings and announcements purporting to characterize the nature of the cybersecurity attack, and the extent to which personal information was impacted. UKG's statements, however, were vague. UKG's statements failed to provide any details regarding the types of personal information at issue. UKG's statements were further limited to characterizations about exfiltration. UKG's statements failed to address what types of personal information were purportedly exfiltrated. UKG's statements further failed to address the extent to which personal information was otherwise impacted, including the extent to which personal information was subject to unauthorized access, disclosure, theft, modification, use, or destruction.

27. Though the cybersecurity attack impacted millions of workers, many if not all workers affected by the breach did not find out about it through direct communications or notices from UKG, but instead through public postings such as the one above, from news outlets, or from their employer. Workers remained in the dark about the extent of personal information compromised because UKG has yet to provide legally compliant notice to those impacted.

28. As result of the cybersecurity attack, UKG's timekeeping and payroll services remained inoperable for many weeks and months, resulting in many of its customers' employees continuing to be paid late, inaccurately, or not at all.

29. Upon information and belief, the hackers responsible for the data breach stole the personal information of all employees of UKG's customers, including Plaintiffs. Because of the nature of the breach and of the personal information stored or processed by UKG, Plaintiffs are informed and believe that all categories of personal information were further subject to unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction. Plaintiffs are

[3] *See* https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US (last visited June 20, 2022).

informed and believe that criminals would have no purpose for hacking UKG other than to exfiltrate or steal, or destroy, use, or modify as part of their ransom attempts, the coveted personal information stored or processed by UKG.

30. The personal information exposed by UKG as a result of its inadequate data security is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen personal information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

31. When malicious actors infiltrate companies and copy and exfiltrate the personal information that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.

32. The information compromised in this unauthorized cybersecurity attack involves sensitive payroll information, which is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Whereas here, the information compromised is difficult and highly problematic to change—driver's license numbers, social security numbers, addresses, and banking information. Further, Plaintiffs and class members cannot easily recreate, and/or cannot recreate at all or in full, the timekeeping information that was stored on UKG's systems and ransomed, made unavailable, or destroyed due to the hackers' actions. Plaintiffs and class members have accordingly lost that information as a result of the cybersecurity breach.

33. Once personal information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personal information being harvested from the victim, as well as personal information from family, friends, and colleagues of the original victim.

34. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' personal information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' personal

information to others who do the same.

35. Federal and state governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. Indeed, the Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices.

36. According to the FTC, the need for data security should be factored into all business decision-making.[4] 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.[5] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct 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 the breach.

37. Also, 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.[6]

38. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personal information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §

[4] *See* Federal Trade Commission, Start with Security (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 20, 2022).

[5] *See* Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 20, 2022).

[6] *See id.*

45.

39. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. UKG's website provided 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."[7] Upon information and belief, UKG's Chief Information Security Officer is John McGregor. The FBI created a technical guidance document for Chief Information Officers and Chief Information Security Officers that compiles 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.[8] 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.
- 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;

[7] *Security: Kronos private cloud security and workforce ready reliability,* Kronos, https://web.archive.org/web/20220405205443/https://www.kronos.com/security (Archived April 5, 2022).

[8] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed June 20, 2022).

and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

41. UKG could have prevented the cybersecurity attack by properly utilizing best practices as advised by the federal government, as described in the preceding paragraphs, but failed to do so.

42. UKG's failure to safeguard against a cybersecurity attack 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 cybersecurity 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 personal information that they collect and maintain. Accordingly, UKG knew or should have known that it was a prime target for hackers.

43. 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.[10]

[9] *Id.*

[10] Maria Henriquez, *40% of organizations have suffered a cloud-based data breach*, Security,

44. Upon information and belief, UKG did not encrypt Plaintiffs' and class members' personal information involved in the data breach.

45. 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.

46. 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.[11]

47. In March of 2021, PrismHR, a Massachusetts-based payroll company that services over 80,000 organizations, suffered a massive outage after suffering a cyberattack on its payroll cloud-based system.[12]

48. In January of 2021, 6,000 employees' personal information was stolen during a ransomware attack on Arup's, a UK-based third-party payroll provider.[13]

49. 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.[14]

50. In February of 2020, the Phoenix Pay System fell prey to a data breach exposing the personal information of more than 69,000 Canadian federal employees.[15]

51. Despite knowing the prevalence of data breaches, UKG failed to prioritize cybersecurity by adopting reasonable security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. UKG has the resources to prevent an attack, but neglected to adequately invest in cybersecurity, despite the growing number of well-publicized breaches. UKG failed to fully implement each and all of the above-described data security best

---

Oct. 29, 2021, https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-datq-breach (last visited June 20, 2022).

[11] Emily Kuhnert, *Payroll Security Breaches*, PapayaGlobal, Feb. 27, 2020, https://papayaglobal.com/blog/list-of-payroll-security-breaches/ (last visited June 20, 2022).

[12] Lawrence Abrams, *Payroll Giant PrismHR outage likely caused by ransomeware attack*, Bleeping Computer, Mar. 2, 2021, https://www.bleepingcomputer.com/news/security/payroll-giant-prismhr-outage-likely-caused-by-ransomware-attack/ (last visited June 20, 2022).

[13] *Id.*

[14] Emily Kuhnert, *Payroll Security Breaches*, PapayaGlobal, Feb. 27, 2020, https://papayaglobal.com/blog/list-of-payroll-security-breaches (last visited June 20, 2022).

[15] *Id.*

practices. UKG further 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 Plaintiffs' and class members' data were protected.

Plaintiffs' Facts

52. Plaintiff William Muller works as a truck driver in California for New Bern Transport Corporation, an exclusive carrier and wholly-owned subsidiary of PepsiCo (New Bern and PepsiCo are collectively referred to herein as PepsiCo). PepsiCo is a client of UKG and utilizes its human resources services, including timekeeping and payroll services, for employees of various entities under the PepsiCo corporate umbrella. In connection with those services, UKG, through PepsiCo, collects, maintains, and processes sensitive personal information of Plaintiff, including, but not limited to, his name, company name, address, e-mail address, time and attendance and schedule information, social security number, employee identification number, and banking information.

53. Plaintiff Antonio Knezevich works as a truck driver in California for Tesla, Inc. Tesla is a client of UKG and utilizes its human resources services, including timekeeping and payroll services, for employees. In connection with those services, UKG collects, maintains, and processes sensitive personal information of Plaintiff, including, but not limited to, his name, company name, address, e-mail address, time and attendance and schedule information, social security number, employee identification number, and banking information.

54. 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, PepsiCo's and Tesla's timekeeping and payroll systems became crippled, and Plaintiffs' and other workers' time and attendance data was lost. PepsiCo and Tesla lacked an adequate contingency plan to accurately pay workers, instead relying on UKG to remedy the breach and re-enable its systems. For months, however, that did not occur. As a stop-gap measure, since the breach PepsiCo and Tesla have adopted a practice of calculating wages due to employees based on, among other things, the averaging of their hours in the weeks prior to the breach. That practice has proved woefully inadequate, resulting in Plaintiffs and employees like Plaintiffs 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 California law. As but one example, Plaintiffs and other PepsiCo and Tesla drivers worked extensive extra overtime hours since the breach due to it being the busy holiday season. However, PepsiCo's and Tesla's haphazard averaging techniques naturally failed to account for those overtime hours because, among other reasons, they were based on stale data from a less busy season earlier in the year. Accordingly, Plaintiffs, along with other PepsiCo and Tesla employees, have experienced significant monetary loss as consequence of UKG's security breach. Indeed, PepsiCo specifically communicated to its employees, including through oral statements and written presentations, that the company's failure to pay employees fully and properly during this time period was the direct result of the Kronos cybersecurity incident and UKG's delays in fixing problems stemming from that incident.

55. Plaintiff Adam Bente worked as an employee for Family Health Centers of San Diego ("FHCSD"). a nonprofit clinic provider of health care dedicated to providing affordable health care and support services when the cybersecurity incident occurred. 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. Plaintiff had worked there since 2017. His responsibilities included 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.

56. FHCSD uses Kronos Privates Cloud to process payroll. On December 12, 2021, FHCSD notified its employees that as a result of a ransomware 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 cybersecurity procedures and practices and the resultant attack of its systems, FHCSD's timekeeping and payroll systems became crippled and remained completely offline for weeks following the incident. FHCSD lacked an adequate contingency plan to accurately pay workers and was forced to switch to manually inputting

payroll.

57. On December 13, 2021, FHCSD notified its employees that employees would need to maintain and submit "manual timesheets" for time worked following the attack. 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.

58. Plaintiff Bente, like class members, was delayed payment of his paycheck following the cybersecurity attack. Following the attack, Plaintiff's payroll was scheduled to be processed by December 17, 2021. The resultant shutdown of UKG's payroll services caused FHCSD employees, including Plaintiff, to not receive their paycheck until after Christmas. Plaintiff Bente and class members had to endure weeks without payment while working during the Omicron surge in the midst of the holiday season.

59. As a result of UKG's payroll services going offline, FHCSD employees were delayed payment of their paychecks. FHCSD employees were forced to find alternative sources of income to pay their bills, mortgages, and necessities, again during the midst of the holiday season. Even after FHCSD got around to distributing paychecks to its employees, many FHCSD employees were either paid inaccurately and/or not at all. In the months following the cybersecurity attack, FHCSD employees have had to invest significant time and expense into determining the amount of any unpaid wages, bonuses, and/or paid time off. Plaintiff Bente, like employees of FHCSD and other class members, has lost time and expenses from having to mitigate the consequences of the delay in payment of his paychecks.

60. Plaintiff Cindy Villanueva works as a registered nurse for Wellpath Recovery Solutions, LLC. On December 14, 2021, Ms. Villanueva received a notice from Wellpath alerting her that the company's Kronos HR & Time Keeping Systems, operated by UKG, were undergoing a ransomware incident affecting Kronos Private Cloud Services, causing a complete outage of Wellpath's timekeeping and payroll system. The barebones notice provided to Plaintiff only provided basic and vague information relating to the breach. As a result of the incident, Wellpath's timekeeping and payroll system was completely inoperable and unavailable, affecting

all of its employees' payroll and timekeeping records and resulting in monetary loss to Plaintiff and other Wellpath employees. The notice also stated that the breach resulted in a disruption of "hundreds to thousands of other companies." Significantly, Plaintiff never received legally compliant or timely notice from Defendant related to the breach, and to date, has not been informed by Defendant of what type of personal information is implicated in the breach. Like Plaintiff Villanueva, members of the class(es) defined herein have similarly experienced significant monetary loss as a result of the cybersecurity attack because their employers have likewise failed to pay them on time, failed to pay them accurately, or failed to pay them at all due to the crippling of their employers' payroll systems that resulted from the UKG breach.

61. In addition to lost wages, 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, all Plaintiffs, like all class members, have also suffered harm in that their sensitive personal information has been exposed to cybercriminals and they have increased stress, risk, and fear of identity theft and fraud. This is not just a generalized anxiety of possible identify theft, privacy, or fraud concerns, but a concrete stress and risk of harm resulting from an actual breach and accompanied by actual instances of reported problems suspected to stem from the breach. In connection with counsel's investigation of this case, workers impacted by the breach, including PepsiCo employees, have reported hacking of their banking information in the weeks following the breach. Twitter users have further 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.[16]

Accordingly, Plaintiffs have suffered harm in the form of increased stress, fear, and risk of identity theft and fraud resulting from the breach.

62. Furthermore, since the cybersecurity attack, Plaintiffs have received increased amounts of spam calls. Plaintiff Bente has received on average per day 5-6 spam calls to his cell phone and countless spam e-mails. Further, shortly after the attack, 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 his and class members' personal information, as were the social security numbers of all Plaintiffs and class members.

63. 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.[17]

64. Furthermore, class members are well aware of the security breach event, as it has impacted their payroll and been widely reported in the media. They are likewise well aware that their sensitive personal information, including social security numbers and potentially banking information, risks being available to other cybercriminals on the dark web. Accordingly, all Plaintiffs and class members have suffered harm in the form of increased stress, fear, and risk of

[16] https://twitter.com/_genosis_/status/1475224472802058240?s=20&t=VvoP-5yfsSrWKYl-geAOQA (last viewed June 20, 2022).

[17] *Identify Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 20, 2022).

identity theft and fraud resulting from the data breach. Upon information and belief, UKG has failed to offer credit monitoring services to all class members, including Plaintiffs. Accordingly, Plaintiffs and class members have incurred, and/or will incur out-of-pocket expenses related to credit monitoring and identify theft prevention to address these concerns.

CLASS ACTION ALLEGATIONS

65. Plaintiffs bring this action on behalf of themselves and all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23, including Rule 23(b)(1)-(3) and (c)(4). Plaintiffs seek to represent the following class and subclasses:

> **Nationwide Class**. All persons in the United States whose personal information and/or employers' payroll systems were compromised in or as a result of the cybersecurity attack UKG Inc. announced on or around December 11, 2021.
>
> **California Subclass.** All persons residing in California whose personal information and/or employers' payroll systems were compromised in or as a result of the cybersecurity attack UKG Inc. announced on or around December 11, 2021.

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

66. Plaintiffs reserve the right to amend or modify the class definitions with greater particularity or further division into subclasses or limitation to particular issues.

67. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes are ascertainable, as described further below:

a. Numerosity: The potential members of the class as defined are so numerous that joinder of all members of the class is impracticable. While the precise number of class members at issue has not been determined, Plaintiffs believe the

cybersecurity breach affected tens of millions of workers nationwide and at least many tens of thousands within California.

b. Commonality: There are questions of law and fact common to Plaintiffs and the class that predominate over any questions affecting only the individual members of the class. The common questions of law and fact include, but are not limited to, the following:

i. Whether UKG owed a duty to Plaintiffs and class members to exercise due care in collecting, storing, processing, and safeguarding their personal information;

ii. Whether UKG owed a legal duty to Plaintiffs and class members to exercise due care to avoid sudden disruption of its human resources services, including their timekeeping and payroll services;

iii. Whether UKG breached those duties;

iv. Whether UKG implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information of class members;

v. Whether UKG acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and class members' personal information;

vi. Whether UKG knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and class members' personal information secure and prevent loss or misuse of that personal information;

vii. Whether UKG adequately addressed and fixed the vulnerabilities which permitted the cybersecurity attack to occur;

viii. Whether UKG caused Plaintiffs and class members damages;

ix. Whether the damages UKG caused to Plaintiffs and class members include lost wages resulting from the disabling of UKG's timekeeping and payroll services, and damages for the harm caused to Plaintiffs' wage payment infrastructure systems;

x. Whether the damages UKG caused to Plaintiffs and class members includes the increased stress, risk, and fear of identity theft and fraud resulting from the access and exfiltration, theft, or disclosure of their personal information;

xi. Whether UKG violated the law by failing to promptly notify class members that their personal information had been compromised;

xii. Whether Plaintiffs and class members are entitled to credit monitoring, identity theft protection, and related monetary relief;

xiii. Whether UKG's failure to implement and maintain reasonable security procedures and practices constitutes negligence;

xiv. Whether UKG's failure to implement and maintain reasonable security procedures and practices constitutes negligence per se;

xv. Whether UKG's failure to implement and maintain reasonable security procedures and practices constitutes violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a);

xvi. Whether UKG's failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; as well as violations of the laws of the state of Massachusetts, Delaware, and Florida (the states of which UKG is a citizen), including: the Massachusetts Data Security Statute, Mass. Gen. Laws. Ann. Ch. 93A, §§ 1-2(a), 201 Mass. Code Regs. 17.01-05, the Delaware Computer Security Breach Act, 6 Del. Code Ann. §§ 12B-102, *et seq.*, the Delaware Consumer Fraud Act, 6 Del. Code §§ 2513 *et seq.*, and Florida's Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201 *et seq.*

xvii. Whether the California subclass is entitled to actual pecuniary damages under the private rights of action in the California Customer Records Act,

Cal. Civ. Code § 1798.84 and the California Consumer Privacy Act, Civ. Code § 1798.150, and the proper measure of such damages, and/or statutory damages pursuant § 1798.150(a)(1)(A) and the proper measure of such damages.

c. Typicality. The claims of the named Plaintiffs are typical of the claims of the class members because all had their personal information and/or payroll systems compromised as a result of UKG's failure to implement and maintain reasonable security measures and the consequent data breach.

d. Adequacy of Representation. Plaintiffs will fairly and adequately represent the interests of the class. Counsel who represent Plaintiffs are experienced and competent in consumer and employment class actions, as well as various other types of complex and class litigation.

e. Superiority and Manageabilty. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Plaintiffs is not practicable, and questions of law and fact common to Plaintiffs predominate over any questions affecting only Plaintiff. Each Plaintiff has been damaged and is entitled to recovery by reason of Defendant's unlawful failure to adequately safeguard their data. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. As any civil penalty awarded to any individual class member may be small, the expense and burden of individual litigation make it impracticable for most class members to seek redress individually. It is also unlikely that any individual consumer would bring an action solely on behalf of himself or herself pursuant to the theories asserted herein. Additionally, the proper measure of civil penalties for each wrongful act will be answered in a consistent and uniform manner. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There

will be no difficulty in the management of this action as a class action, as Defendant's records will readily enable the Court and parties to ascertain affected companies and their employees.

68. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the class as a whole.

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

a. Whether UKG owed a legal duty to Plaintiffs and class members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

b. Whether UKG breached that legal duty to Plaintiffs and class members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

c. Whether UKG owed a legal duty to Plaintiffs and class members to exercise due care to avoid sudden disruption of its human resources services, including their timekeeping and payroll services;

d. Whether UKG breached that legal duty to Plaintiffs and class members to exercise due care to avoid sudden disruption of its human resources services, including their timekeeping and payroll services;

e. Whether UKG failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether UKG failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information compromised in the breach; and

g. Whether class members are entitled to actual damages, credit monitoring, injunctive relief, statutory damages, and/or punitive damages as a result of UKG's wrongful conduct as alleged herein.

FIRST CAUSE OF ACTION
(Negligence, By Plaintiffs and the Nationwide Class Against All Defendants)

70. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

71. UKG owed a duty to Plaintiffs and class members to exercise reasonable care in obtaining, storing, using, processing, deleting and safeguarding their personal information in its possession from being compromised, stolen, accessed, and/or misused by unauthorized persons. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information 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 Plaintiffs' and class members' personal information 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, Plaintiffs, and class members of any data breach.

72. UKG's duties to use reasonable care arose from several sources, including but not limited to those described below.

73. UKG had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their personal information 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 Plaintiffs and other class members would be harmed.

74. 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 personal information by companies such as UKG.

75. 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.[18] 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.[19] Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct 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. The FBI has also issued guidance on best practices with respect to data security that also form the basis of UKG's duty of care, as described above.[20]

76. In addition, individual states have enacted statutes based on the FTC Act that also created a duty, including, among others, those referenced in paragraph 67.b.xvi.

77. 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 cybersecurity attack herein affected

[18] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

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

[20] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed June 20, 2022).

thousands of companies and millions of employees. UKG undertakes its collection of sensitive personal information 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. Plaintiffs 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. Plaintiffs 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 personal information, 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 Plaintiffs and class members as a result of the UKG data breach. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and class members' personal information, UKG assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and class members' personal information from disclosure.

78. 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 personal information at issue here.

79. 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 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.[21]

Accordingly, UKG admits that it has a duty and responsibility to adequately safeguard Plaintiffs' and class members' personal information.

80. UKG also had a duty to safeguard the personal information of Plaintiffs 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 personal information, as detailed herein, including Cal. Civ. Code § 1798.80 *et seq.*

81. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiffs 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.

82. UKG also owed a duty to Plaintiffs 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 Plaintiffs 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 Plaintiffs and class members harm.

83. Plaintiffs and class members have taken reasonable steps to maintain the confidentiality of their personal information.

84. UKG breached the duties it owed to Plaintiffs 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

[21] https://www.ukg.com/privacy (Last viewed June 20, 2022).

sufficient to protect the personal information of Plaintiffs 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 Plaintiffs' and class members' personal information in UKG's possession had been or was reasonably believed to have been stolen or compromised; (f) avoid disruption and continued disruption of its timekeeping and payroll services; and (g) failing to comply fully even with its own purported security practices.

85. UKG knew or should have known of the risks of collecting and storing personal information and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks on payroll vendors and known coding vulnerabilities previously reported by news media and Alibaba earlier in 2021. Specifically, among other things, the Log4Shell is a software vulnerability in Apache Log4j 2, a popular Java library for logging error messages in applications. The vulnerability, published prior to the data breach, enables an attacker to take control of a device on the internet if the device is running certain versions of Log4j 2. These vulnerabilities had been reported earlier in 2021. The sheer scope of UKG's operations, which affect thousands of employers and millions of employees, further shows that UKG knew or should have known of the risks and possible harm that could result from its failure to implement and maintain reasonable security measures. On information and belief this is but one of the several vulnerabilities that plagued UKG's systems and led to the data breach.

86. Through UKG's acts and omissions described in this complaint, including UKG's failure to provide adequate security and its failure to protect the personal information of Plaintiffs 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 Plaintiffs' and class members' personal information.

87. UKG further failed to timely and accurately disclose to customers, Plaintiffs, and class members that their personal information had been improperly acquired or accessed and was available for sale to criminals on the dark web. Indeed, Plaintiffs 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 Plaintiffs and class members) but failed to adequately describe all types of personal information that were exfiltrated, stolen, disclosed, accessed, used, or modified by the ransomware attackers and failed to provide the results of the forensic investigation into the cybersecurity attack and its implications.

88. UKG further breached its duty to Plaintiffs 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 months and failing to adequately and timely remedy its security vulnerabilities.

89. But for UKG's wrongful and negligent breach of its duties owed to Plaintiffs and class members, their personal information would not have been compromised nor their timekeeping and payroll services disabled.

90. Plaintiffs and class members relied on UKG to keep their personal information confidential and securely maintained, and to use this information for business purposes only, and to make only authorized disclosures of this information.

91. As a direct and proximate result of UKG's negligence, Plaintiffs 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 Plaintiffs' and class members' personal information, Plaintiffs' and class members' personal information has been accessed by malicious cybercriminals. Plaintiffs' and the class members' injuries include:

a. damages stemming from Plaintiffs 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 stress, fear, and anxiety of Plaintiffs 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 personal information;

d. loss of their time records and other timekeeping and payroll information;

e. costs associated with requested credit freezes;

f. costs associated with credit monitoring and detection and prevention of identity theft and unauthorized use of their financial accounts;

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 attempt 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 personal information being placed in the hands of criminals;

k. damages to and diminution of value of their personal information entrusted, directly or indirectly, to UKG with the mutual understanding that UKG would safeguard Plaintiffs' 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 personal information, 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 Plaintiffs and

class members, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the breach;

m. loss of the inherent value of their personal information;

n. the loss of the opportunity to determine for themselves how their personal information is used;

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

92. In connection with the conduct descried above, UKG acted wantonly, recklessly, and with complete disregard for the consequences Plaintiffs and class members would suffer if their highly sensitive and confidential personal information, including but not limited to name, company name, address, e-mail address, time and attendance and schedule information, social security numbers, and banking information, was access by unauthorized third parties.

SECOND CAUSE OF ACTION
(Negligence Per Se, By Plaintiffs and the Nationwide Class Against All Defendants)

93. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

94. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, 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 personal information by companies such as UKG. Various FTC publications and data security breach orders further form the basis of UKG's duty. In addition, individual states have enacted statutes based on the FTC Act that also created a duty.

95. UKG violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect personal information and not complying with industry standards. UKG's conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored and the foreseeable consequences of a data breach at one of the largest cloud computing companies in the world handling timekeeping and payroll data for thousands of companies and millions of employees.

96. UKG's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

97. Plaintiffs and class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was meant to protect.

98. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the class.

99. UKG is a citizen of the states of Massachusetts, Delaware, and/or Florida, in that it incorporated in Delaware and operates dual headquarters in Massachusetts and Florida. All of its activities are therefore subject to the laws of these states. UKG's actions as described herein constitute unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws. Ann. Ch. 93A, §§ 1-2(a), as well as violations of the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws. Ann. Ch. 93H, § 2; and 201 Mass. Code Regs. 17.01-05, violations of the Delaware Computer Security Breach Act, 6 Del. Code Ann. §§ 12B-102, *et seq.*, the Delaware Consumer Fraud Act, 6 Del. Code §§ 2513 *et seq.*, and violations of Florida's Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201 *et seq.*, specifically in that UKG misrepresented that it would protect the privacy and confidentiality of Plaintiffs and class members' personal information, including by implementing and maintaining reasonable security measures, then failed to do so, and further failed to promptly, fully, and adequately notify Plaintiffs and class members of the breach. UKG's violations of these statutes constitute negligence *per se*. Plaintiffs and class members are within the class of persons these statutes were meant to protect. Moreover, the harm that has occurred is the type of harm that these state statutes intended to guard against.

100. As a direct and proximate result of UKG's negligence, Plaintiffs and class members have been injured as described herein and in paragraph 91 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at

trial.

THIRD CAUSE OF ACTION
(Unjust Enrichment, By Plaintiffs and the Nationwide Class Against All Defendants)

101. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

102. Plaintiffs and class members have an interest, both equitable and legal, in the personal information about them that was conferred upon, collected by, and maintained by UKG and that was ultimately converted, stolen, removed, deleted, exfiltrated, or disclosed in the UKG data breach. This personal information was conferred on UKG in most cases by third parties, class members' employers, but in some instances directly by Plaintiffs and class members themselves.

103. UKG was benefitted by the conferral upon it of the personal information pertaining to Plaintiffs and class members and by its ability to retain and use that information. UKG understood that it was in fact so benefitted.

104. UKG also understood and appreciated that the personal information pertaining to Plaintiffs and class members was private and confidential and its value depended upon UKG maintaining the privacy, security, and confidentiality of that personal information.

105. But for UKG's willingness and commitment to maintain its privacy, security, and confidentiality, that personal information 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.

106. 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 personal information belonging to Plaintiffs and class members without having adequate data security measures, and its other conduct in facilitating the theft of that personal information), UKG has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members. Among other things, UKG has and continues to

benefit and profit from the sale of the personal information and from its contracts to use that personal information to process timekeeping and payroll, while the value to Plaintiffs and class members has been diminished.

107. UKG's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and class members' sensitive personal information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

108. 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 Plaintiffs and class members in an unfair and unconscionable manner. UKG's retention of such benefits under circumstances making such retention inequitable constitutes unjust enrichment.

109. 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.

110. UKG is therefore liable to Plaintiffs 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 personal information 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.

FOURTH CAUSE OF ACTION

(Declaratory Judgment, By Plaintiffs and the Nationwide Class Against All Defendants)

111. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

112. 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 federal and state statutes described in this complaint.

113. An actual controversy has arisen in the wake of the UKG data breach regarding its

present and prospective common law and other duties to reasonably safeguard its customers and their employees' personal information, to avoid disruption of timekeeping and payroll services, and regarding whether UKG is currently maintaining data security measures adequate to protect Plaintiffs and class members from further data breaches that compromise their personal information and timekeeping and payroll services. Plaintiffs allege that UKG's data security measures remain inadequate. UKG denies these allegations. Plaintiffs continue to suffer injury as a result of the compromise of their personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

114. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. UKG continues to owe a legal duty to secure consumers' and employees personal information, including Plaintiffs' and class members' personal information, to timely notify them of a data breach under the common law, Section 5 of the FTC Act, and various state statutes, and to avoid disruption to their timekeeping and payroll services;

b. UKG continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and class members' personal information and by failing to avoid disruption of their timekeeping and payroll services.

115. The Court should issue corresponding prospective injunctive relief requiring UKG to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and class members' personal information and timekeeping and payroll services.

116. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at UKG. The risk of another such breach is real, immediate, and substantial. If another breach at UKG occurs, Plaintiffs 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.

117. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to UKG if an injunction is issued. Among other things, if another massive data breach occurs at

UKG, Plaintiffs and class members will likely be subjected to substantial identity theft and other damage, including continuing lost wages from timekeeping and payroll interruptions. 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.

118. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at UKG, thus eliminating the additional injuries that would result to Plaintiffs and the millions of class members whose confidential information would be further compromised.

FIFTH CAUSE OF ACTION
(Breach of Contract, By Plaintiffs and the Nationwide Class Against All Defendants)

119. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

120. At all relevant times a contract existed and was in force between UKG on one hand and Plaintiffs and the class members on the other. This contract was written and was supplemented by implied and written terms that existed and were maintained online on Defendant's website. Any implied contracts or supplemental terms or conditions of the contract were written by Defendant and published electronically to Plaintiff and the class members online in such a manner and through such conduct so as to create promises on the part of the Defendant.

121. These written conditions include, but are not limited to, the terms and conditions included in the security section of UKG's privacy policy.

122. UKG's privacy policy is an agreement between UKG and its customers as well as the employees of its customers, who include Plaintiffs and class members, and who provided their personal information to UKG.

123. UKG's privacy policy has a "Security" section which specifically states:

> 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.

124. This privacy policy constitutes a contract or implied contract between UKG, on the one hand, and Plaintiffs and class members, on the other hand. This contract or implied contract was formed when Plaintiffs and class members entrusted their personal information to their employers, who in turn entrusted it to UKG, and in instances when Plaintiffs and class members provided their personal information directly to UKG. UKG specifically contracted to implement and maintain reasonable security measures and to limit access to Plaintiffs' and class members' data and undertook a responsibility and contractual obligation to do so. UKG undertook these duties specifically for the purpose of facilitating continuing and ongoing payroll and timekeeping services for Plaintiffs and class members.

125. Plaintiffs and class members are further third-party beneficiaries of any such contract between their employers and UKG.

126. Plaintiffs and class members and class members' employers fully performed their obligations under the contracts or implied contracts with UKG.

127. UKG breached its contracts or implied contracts with Plaintiffs and class members and class members' employers by failing to protect their personal information. Specifically, it failed to take reasonable steps to use safe and secure systems to protect that information, failed to have appropriate security protocols and measures in place to protect that information, such as adequate internal and external firewalls, physical security, technological security measures, and encryption, disclosed that information to unauthorized third parties, failed to promptly alert or give notice of the breach to Plaintiffs and class members, and failed to adequately continue to provide ongoing payroll and maintenance services to Plaintiffs and class members.

128. UKG further violated its commitment to maintain the confidentiality and security of the personal information of Plaintiffs and class members by failing to comply with applicable laws, regulations, and industry standards relating to data security.

129. As a direct and proximate result of UKG's breaches of contract, Plaintiffs and class members sustained actual losses, damages, and consequential damages as described above, and are also entitled to recover nominal damages.

SIXTH CAUSE OF ACTION
(Violation of the California Consumer Privacy Act,
Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)
By Plaintiffs and the California Subclass Against All Defendants)

130. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

131. 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 personal information, 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.

132. 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.

133. Plaintiffs and California subclass members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

134. The personal information of Plaintiffs and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information UKG collects and which was impacted by the cybersecurity attack 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.

135. UKG knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's personal information 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 personal information of Plaintiffs and the California subclass. Specifically, UKG subjected Plaintiffs' and the California subclass's nonencrypted and nonredacted personal information 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.

136. As a direct and proximate result of UKG's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and class members' personal information 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' personal information.

137. As a direct and proximate result of UKG's acts, Plaintiffs and the California subclass 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 Plaintiffs' and the subclass's legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

138. 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, Plaintiffs and the California subclass by way of this complaint seek actual pecuniary damages suffered as a result of UKG's violations described herein.

139. On January 19, 2022, March 22, 2022, and March 3, 2022, Plaintiffs Muller and Knezevich, Plaintiff Villanueva, and Plaintiff Bente, respectively, issued a written notice of the violations alleged herein to UKG pursuant to § 1798.150(b), by sending a written notice letter along with a copy of Plaintiff's original complaint via certified mail to UKG's corporate headquarters and to UKG's registered agent for service of process. More than 30 days have since expired and Plaintiffs have received no response. Accordingly, pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b), Plaintiffs also seek statutory damages and injunctive relief.

SEVENTH CAUSE OF ACTION

(Violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, By Plaintiffs and the California Subclass Against All Defendants)

140. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

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

142. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to

protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

143. 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."

144. Plaintiffs and members of the California subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to UKG, directly and/or indirectly through their employers, for the purpose of obtaining a service from UKG.

145. The personal information of Plaintiffs and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information UKG collects and which was impacted by the cybersecurity attack 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.

146. UKG knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's personal information 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 personal information of Plaintiffs and the California subclass. Specifically, UKG

failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiffs and the California subclass from unauthorized access, destruction, use, modification, or disclosure. UKG further subjected Plaintiffs' and the California subclass's nonencrypted and nonredacted personal information 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.

147. As a direct and proximate result of UKG's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiffs and the California subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiffs and the California subclass by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

148. As a direct and proximate result of UKG's acts or omissions, Plaintiffs and the California subclass 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 Plaintiffs' and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiffs seek compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

149. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

150. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to

this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

151. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California subclass, including among other things, the types of personal information that were or are reasonably believed to have been the subject of a breach. Defendant learned of the breach on or about December 11, 2021. Plaintiff and class members were entitled to receive timely notice from Defendant, but instead, found out about the breach of their payroll information from their employers, through news and media outlets, or not at all. As

a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice directly to Plaintiff and class members.

152. Plaintiffs, and on information and belief, many class members affected by the breach, have not received any notice at all from Defendant in violation of Section 1798.82(d).

153. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiffs and class members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

154. As a direct consequence of the actions as identified above, Plaintiffs and class members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred but for the data breach of Defendant's payroll systems, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

EIGHTH CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200 *et seq.* By Plaintiffs and the California Subclass Against All Defendants)

155. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

156. UKG is a "person" 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 "unfair" acts and practices include:

a. UKG failed to implement and maintain reasonable security measures to protect Plaintiffs and California sublcass members' personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and

proximate cause of the UKG data breach. UKG failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry, for example the Log4Shell is a software vulnerability in Apache Log4j 2, a popular Java library for logging error messages in applications. UKG failed to patch these and other problems, which made it trivial for a hacker to penetrate UKG's systems. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the California subclass, whose personal Information has been compromised.

b. UKG's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150).

c. UKG's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of UKG's inadequate security, consumers could not have reasonably avoided the harms that UKG caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

159. UKG has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

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

a. Failing to implement and maintain reasonable security and privacy measures to

protect Plaintiffs and California subclass members' personal information, which was a direct and proximate cause of the UKG data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the UKG data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and California subclass members' personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of the UKG data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and California subclass members' personal information, 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 Plaintiffs and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and California subclass members' personal information; 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 Plaintiffs and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ.

Code § 1798.150.

161. 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 consumers' personal information and ongoing provision of timekeeping and payroll services.

162. As a direct and proximate result of UKG's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California subclass members were injured and lost money or property, including the lost wages directly resulting from the disabling of the timekeeping and payroll systems of the employers of Plaintiffs and subclass members, 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, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, increased stress, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information, and well as the time and expense of finding alternative methods of timekeeping and payroll services.

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

164. Plaintiffs and class members have lost money and property as a result of UKG's conduct in violation of the UCL, as stated herein and above.

165. By deceptively storing, collecting, and disclosing their personal information, UKG has taken money or property form Plaintiffs and class members.

166. UKG acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and California subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

167. Plaintiffs and California subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from UKG's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5;

injunctive relief; and other appropriate equitable relief, including public injunctive relief.

NINTH CAUSE OF ACTION
(Invasion of Privacy)

(Count 1 – Common Law Invasion of Privacy – Intrusion Upon Seclusion By Plaintiffs and the Nationwide Class Against All Defendants)

168. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

169. 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.

170. UKG intentionally intruded upon the solitude, seclusion and private affairs of Plaintiffs 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 Plaintiffs' and class members' personal information. Only UKG had control over its systems.

171. UKG's conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiffs' and class members' personal information.

172. At all times, UKG was aware that Plaintiffs' and class members' personal information in their possession contained highly sensitive and confidential personal information, including but not limited to name, company name, address, email address, time and attendance and schedule information, and social security numbers.

173. Plaintiffs and class members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

174. UKG intentionally configured their systems in such a way that stored Plaintiffs' and class members' personal information to be left vulnerable to malware/ransomware attack without regard for Plaintiff's and class members' privacy interests.

175. The disclosure of the sensitive and confidential personal information 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.

176. 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 Plaintiffs' and class members' sensitive and confidential personal information, 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.

177. As a result of UKG's actions, Plaintiffs and class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

178. 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.

179. Plaintiffs 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 stress, fear, anxiety and risk of future invasions of privacy.

(Count 2 –Invasion of Privacy – Cal. Const. Art. 1, § 1
By Plaintiffs and the California Subclass Against All Defendants)

180. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

181. 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." Cal. Const, Art. I, § 1.

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

183. 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.

184. UKG violated Plaintiffs' and class members' constitutional right to privacy by collecting, storing, and disclosing their personal information 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 Plaintiffs and class members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

185. UKG has intruded upon Plaintiffs' and class members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

186. 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 Plaintiffs and class members of the ability to control the circulation of their personal information, which is considered fundamental to the right to privacy.

187. Plaintiffs 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' personal information; (ii) Plaintiffs and class members did not consent or otherwise authorize UKG to disclosure their personal information; and (iii) Plaintiffs and class members could not reasonably expect UKG would commit acts in violation of laws protecting privacy.

188. As a result of UKG's actions, Plaintiffs 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.

189. Plaintiffs and class members suffered actual and concrete injury as a result of UKG's violations of their privacy interests. Plaintiffs 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 stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

190. Plaintiffs and class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs 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 Plaintiffs' and class members' privacy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves, the nationwide class, and the California subclass, pray for the following relief:

1. An order certifying the nationwide class and California subclass as defined above pursuant to Fed. R. Civ. P. 23 and declaring that Plaintiffs are proper class representatives and appointing Plaintiffs' counsel as class counsel;
2. Permanent injunctive relief to prohibit UKG from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. Compensatory, consequential, general, and nominal damages in an amount to be proven at trial, in excess of $5,000,000;
4. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;
5. Punitive, exemplary, and/or trebled damages to the extent permitted by law;
6. Statutory damages pursuant to Cal. Civ. Code § 1798.150(a)(1)(A);
7. A declaration of right and liabilities of the parties;
8. Costs of suit;
9. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;
10. Pre- and post-judgment interest at the maximum legal rate;
11. Distribution of any monies recovered on behalf of members of the class or the general public via fluid recovery or *cy pres* recovery where necessary and as applicable to

prevent Defendant from retaining the benefits of their wrongful conduct; and

12. Such other relief as the Court deems just and proper.

Dated: June 21, 2022

ALEXANDER MORRISON + FEHR LLP

WUCETICH & KOROVILAS LLP

By: /s/ Dimitrios V. Korovilas
DIMITRIOS V. KOROVILAS
Attorneys for Plaintiffs
William Muller and Antonio Knezevich,
individually and on behalf of
all others similarly situated

LEBE LAW

By: /s/ Jonathan M. Lebe
JONATHAN M. LEBE
Attorneys for Plaintiff Cindy Villanueva,
individually and on behalf of
all others similarly situated

LAW OFFICE OF RONALD A. MARRON

By: /s/ Alexis M. Wood
ALEXIS M. WOOD
Attorneys for Plaintiff Adam Bente,
individually and on behalf of
all others similarly situated

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the putative class and subclass, hereby demand a trial by jury on all issues of fact or law so triable.

Dated: June 21, 2022

ALEXANDER MORRISON + FEHR LLP

WUCETICH & KOROVILAS LLP

By: /s/ Dimitrios V. Korovilas
DIMITRIOS V. KOROVILAS
Attorneys for Plaintiffs
William Muller and Antonio Knezevich,
individually and on behalf of
all others similarly situated

LEBE LAW

By: /s/ Jonathan M. Lebe
JONATHAN M. LEBE
Attorneys for Plaintiff Cindy Villanueva,
individually and on behalf of
all others similarly situated

LAW OFFICE OF RONALD A. MARRON

By: /s/ Alexis M. Wood
ALEXIS M. WOOD
Attorneys for Plaintiff Adam Bente,
individually and on behalf of
all others similarly situated

ATTESTATION PURSUANT TO LOCAL CIVIL RULE 5-1(h)(3)

Pursuant to Local Civil Rule 5-1(h)(3), I hereby attest that each of the other signatories have concurred in the filing of the foregoing document.

Dated: June 21, 2022

By: /s/ Dimitrios V. Korovilas
DIMITRIOS V. KOROVILAS