Jonathan M. Lebe, State Bar No. 284605
Jon@lebelaw.com
Zachary T. Gershman, State Bar No. 328004
Zachary@lebelaw.com
Nicolas W. Tomas, State Bar No. 339752
Nicolas@lebelaw.com
**Lebe Law, APLC**
777 S. Alameda Street, Second Floor
Los Angeles, CA 90021
Telephone: (213) 444-1973

Attorneys for Plaintiff Cindy Villanueva,
Individually and on behalf of all others similarly situated

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

| | |
|---|---|
| Cindy Villanueva, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>vs.<br><br>UKG, Inc.,<br><br>Defendant. | **CLASS ACTION COMPLAINT FOR:**<br><br>1. Negligence;<br>2. Breach of Contract;<br>3. Violation of the CCPA (Cal. Civ. Code § 1798.150, *et seq.*);<br>4. Violation of the CRA (Cal. Civ. Code § 1798.80, *et seq.*);<br>5. Violation of the Right to Privacy (Cal. Const., art. I § 1); and<br>6. Violation of the Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*).<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiff Cindy Villanueva ("Plaintiff"), individually and on behalf of others similarly situated, alleges as follows:

## NATURE OF ACTION AND INTRODUCTORY STATEMENT

1. Every year millions of Americans have their most valuable personal information ("PI") stolen and sold online because of unauthorized data disclosures. Despite the dire warnings about the severe impact of unauthorized data disclosures

on Americans of all economic strata, companies still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data about their customers or potential customers.

2. Defendant UKG, Inc., known as Ultimate Kronos Group, ("Defendant") is a multinational technology company providing payroll, timekeeping, and human resource services to companies and businesses nationwide using its software including, "Kronos Private Cloud" and "UKG Workforce Central." Defendant provides its services to thousands of large employers, who in turn, have millions of end-users. Defendant is one of the largest, if not the largest, provider of workforce management services to major employers. In doing so, Defendant collects the most sensitive and confidential PI of millions of users of its software.

3. Through its software, Defendant provides services to employers to assist in tracking employee's hours, pay, and time records. In doing so, Defendant retains sensitive information related to payroll records such as direct deposit information, bank account information, addresses, and social security numbers, among other things.

4. As a corporation doing business in California, Defendant is legally required to protect PI from unauthorized access and exfiltration.

5. On or around December 11, 2021, Defendant's cloud-based time and attendance systems, including "Kronos Private Cloud" and other UKG systems were exploited by hackers through a ransomware attack causing a massage outage of their payroll system and exposing millions of worker's information to cybercriminals as a result of Defendant's failure to equip its system with reasonable and adequate security.

6. On December 13, 2021, Defendant's Executive Vice President, Bob Hughes made the following announcement on Defendant's 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.
>
> We are working with leading cyber security 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."[1]

7. Though this unauthorized data breach impacted millions of workers, many workers affected by the breach did not find out about the breach from Defendant, but instead found out about it through public postings such as the one above, from news outlets, or from their employer. To date, many workers are still in the dark as to what type of PI was compromised by this breach, because Defendant has yet to provide legally compliant notice to those impacted of the breach to those impacted.

8. More recently, on March 4, 2022, Defendant made the following update regarding the data breach:

> "Our forensic investigation is now complete. As previously communicated, the investigation determined that the personal data of individuals associated with two of our customers was exfiltrated as a result of the incident. Both affected customers have been notified, so if you have not heard from us directly, you can feel confident that we have found no evidence that any personal data of individuals associated with your organization was

[1] UKG Workforce Central – Leo Daley, https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US (last visited Mar. 10, 2022).

exfiltrated."[2]

9. On information and belief, Defendant has not provided legally compliant notice to the millions of workers whose information was not only exfiltrated, but also unlawfully disclosed and accessed as a result of the breach. To date, Defendant has not confirmed what type of PI was accessed, disclosed, stolen, or exfiltrated.

10. As a result of Defendant's failure to provide reasonable and adequate data security, Plaintiff's and putative class members' PI has been exposed to those who should not have access to it. Plaintiff and putative class members are now at much higher risk of identity theft and for cybercrimes of all kinds, especially considering the highly valuable and sought-after PI stolen here—financial information relating to millions of worker's payroll records.

11. In addition to the privacy implications, the resulting data breach massively disrupted payroll systems for many large companies that use Defendant's payroll services, including many grocery stores, insurance companies, hospitals, department stores, food manufacturers, and a plethora of other businesses who rely on Defendant's services for processing their employee's payroll information. This massive disruption of Defendant's payroll and timekeeping system resulted in many workers being paid late, being paid incorrectly, or not being paid at all during the holiday season and during the Covid-19 pandemic.

12. Defendant's Privacy Policy specifically states that it limits access of PI and data only to those "who have a specific business purpose for maintaining and processing such information." Despite this claim, and other claims in its privacy policy, Defendant allowed its system to be attacked and exploited by hackers, resulting in a massive breach of critical PI of millions of end-users off its payroll system.

13. The PI exposed by Defendant as a result of its inadequate data security

[2] UKG Kronos Private Cloud Status Updates Archives, https://www.ukg.com/KPCupdates/Archive (last visited Mar. 10, 2022).

is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen PI 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.

14. When malicious actors infiltrate companies and copy and exfiltrate the PI 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.

15. The information compromised in this unauthorized data breach 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.

16. Once PI 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 PI being harvested from the victim, as well as PI from family, friends, and colleagues of the original victim.

17. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

18. 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. According to the FTC, the need

for data security should be factored into all business decision-making.[3]

19. 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.[4] 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.

20. 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.[5]

21. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, 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. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security

---

[3] *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 Mar. 10, 2022).

[4] *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 Mar. 10, 2022).

[5] *See Id*.

obligations.[6]

22. Through negligence in securing Plaintiff's and putative class members' PI and allowing access to Plaintiff's and putative class members' PI through malware, Defendant failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and the putative class members' PI. Accordingly, Defendant's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

23. On December 14, 2021, Plaintiff Cindy Villanueva—a Registered Nurse—received a notice from her employer, Wellpath Recovery Solutions, LLC ("Wellpath"), alerting her that Wellpath's Kronos HR & Time Keeping Systems, operated by Defendant, was undergoing a ransomware incident affecting Kronos Private Cloud Services, causing a complete outage of Wellpath's timekeeping and payroll system. (*See* Exhibit A.) The barebones notice provided to Plaintiff only provided basic and vague information relating to the breach. As a result of the breach, Wellpath's payroll and timekeeping system was completely inoperable and unavailable, affecting all of its employee's payroll and timekeeping records. The notice also stated that the breach resulted in a disruption of "hundreds to thousands of other companies." (*See Id.*) Significantly, Plaintiff never received legally compliant or timely notice from Defendant related to the breach, and to date, has not been informed of what type of PI is implicated in the breach.

24. As a result of the unauthorized data disclosure, Plaintiff and putative class members are now at risk for actual identity theft in addition to other forms of fraud. The ramifications of Defendant's failure to keep PI secure are long lasting and severe. Once PI is stolen, fraudulent use of that information and damage to victims may continue for years. The PI belonging to Plaintiff and class members is private, valuable, and sensitive in nature as it can be used to commit a lot of

[6] Federal Trade Commission, Privacy and Security Enforcement Press Releases, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Mar. 10, 2022).

different harms in the hands of the wrong people.

25. Defendant had ample resources necessary to prevent the unauthorized data disclosure, but neglected to adequately implement data security measures, despite its obligations to protect the PI of Plaintiff and putative class members. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the unauthorized access of PI.

26. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and putative class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the unauthorized data disclosure on their lives.

## THE PARTIES

27. Plaintiff Cindy Villanueva is a citizen and resident of the State of California. Plaintiff is a licensed Registered Nurse in the State of California who is employed by Wellpath Recovery Solutions, LLC. Plaintiff's employer is a client of Defendant who uses its payroll and timekeeping system to process its employee's payroll information. Plaintiff was impacted by the data breach and ransomware attack of Defendant's payroll system that took place on or about December 11, 2021, which affected her personal and sensitive information relating to her payroll records.

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

## JURISDICTION AND VENUE

29. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least

one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs. The court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

30. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is registered to conduct business in California, and has sufficient minimum contacts with California.

31. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's and putative class members' claims occurred in this District. Venue is also proper under 28 U.S.C. § 1391(c) because Defendant is a corporation that does business in and is subject to personal jurisdiction in this District. In addition, Plaintiff is informed and believes and thereon alleges that members of the class and subclass defined below reside in the Northern District. 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.

## CLASS ACTION ALLEGATIONS

32. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiff, individually and on behalf of all others similarly situated, brings this lawsuit on behalf of herself and as a class action on behalf of the following classes:

**Nationwide Class:** All persons in the United States whose personal information was accessed, compromised, or stolen as a result of the data breach announced by UKG, Inc. on or around December 11, 2021.

**California Subclass:** All persons in California whose personal information was accessed, compromised, or stolen as a result of the data breach announced by UKG, Inc. on or around December 11, 2021.

33. Members of the class and subclass described above will be collectively referred to as "class members." Plaintiff reserves the right to establish other or additional subclasses, or modify any class or subclass definition, as appropriate based on investigation, discovery, and specific theories of liability.

34. Excluded from the class and subclass is Defendant and any entities in which Defendant or its subsidiaries or affiliates have a controlling interest, and Defendant's officers, agents, and employees. Also excluded from the class are the judge assigned to this action, and any member of the judge's immediate family.

35. **Numerosity:** The members of each class are so numerous that joinder of all members of any class would be impracticable. Plaintiff reasonably believes that class members amount to tens of millions of people. The names and addresses of class and subclass members are identifiable through documents maintained by Defendant.

36. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

(a) Whether Defendant represented to class members that it would safeguard Plaintiff's and class members' PI;

(b) Whether Defendant owed a legal duty to Plaintiff and class members in exercising due care in collecting, storing, and safeguarding their PI;

(c) Whether Defendant breached a legal duty to Plaintiff and class members to exercise due care in collecting, storing, and safeguarding their PI;

(d) Whether Plaintiff's and class members' PI was accessed, compromised, or stolen in the unauthorized data disclosure;

(e) Whether a contract existed between Plaintiff and class members, and the terms of that contract;

(f) Whether Defendant breached the contract by having inadequate safeguards;

(g) Whether Defendant failed to adhere to its own posted privacy policy in violation of Cal. Bus. & Prof. Code § 22576;

(h) Whether Defendant's conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq*.;

(i) Whether Defendant's conduct violated the Consumer Records Act, Cal. Civ. Code § 1798.80, *et seq*.;

(j) Whether Defendant violated the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, *et seq*.;

(k) Whether Defendant's conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et eq*.;

(l) Whether Plaintiff and class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

(m) Whether Plaintiff and class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

37. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of other similarly situated class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

38. **Typicality:** Plaintiff's claims are typical of the claims of the other class members because, among other things, Plaintiff and the other class members were injured through substantially uniform misconduct by Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other class

members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other class members arise from the same operative facts and are based on the same legal theories.

39. **Adequacy of Representation:** Plaintiff is an adequate representative of the classes because her interests do not conflict with the interests of the other class members she seeks to represent. Plaintiff has retained counsel competent and experienced in complex class action litigation and Plaintiff will prosecute this action vigorously. The class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

40. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for class members to individually seek redress for Defendant's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

## FIRST CAUSE OF ACTION

### Negligence

### (On behalf of Plaintiff and the Nationwide Class)

41. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

42. Defendant owed a duty to Plaintiff and class members to exercise

reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and class members' PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining, and testing its data security systems to ensure that Plaintiff's and class members' PI in Defendant's possession was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect their breach of the payroll and timekeeping system in a timely manner.

43. Defendant owed a duty of care to Plaintiff and class members to provide security consistent with industry standards, and to ensure that its systems and networks adequately protected the PI it stored, maintained, and/or obtained.

44. Defendant owed a duty of care to Plaintiff and class members because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks involved in allowing its payroll system to be attacked by malware and the resulting breach of sensitive and valuable PI of millions of workers.

45. Defendant knew that the PI of Plaintiff and class members was personal and sensitive payroll information that is incredibly valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the PI of Plaintiff and class members were wrongfully disclosed, if disclosure was not fixed, or if Plaintiff and class members were not provided with timely and legally compliant notice detailing the PI implicated by the data breach.

46. Plaintiff and class members entrusted Defendant with their PI when Defendant obtained their PI from their employer's for payroll services. As such, Defendant had an obligation to safeguard their information and was in the best position to protect against the harm suffered by Plaintiff and class members as a result of the data breach to its payroll system.

47. Defendant's own conduct also created a foreseeable risk of harm to

Plaintiff's and class members' PI. Defendant's misconduct included failing to implement the systems, policies, and procedures necessary to prevent the unauthorized data breach.

48. Defendant knew, or should have known, of the risks inherent in collecting and storing PI and the importance of adequate security. Defendant knew about—or should have been aware of—numerous and well-publicized unauthorized data disclosures affecting businesses, especially companies storing sensitive financial records, such as highly valuable payroll information.

49. Defendant breached its duties to Plaintiff and class members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PI of Plaintiff and class members.

50. In addition, Defendant breached its duty to provide legally compliant and timely notice of the breach to Plaintiff and class members and to adequately disclose what PI was implicated by the breach as described herein and below. Among other things, Defendant failed to notify Plaintiff and class members of what type of PI was disclosed, accessed, stolen, or exfiltrated. Timely notice was required so that Plaintiff and class members can take steps to mitigate the harms of the breach by freezing their credit reports, monitoring their accounts, contacting their financial institutions, obtaining credit monitoring services, and taking other avenues to prevent future harms.

51. Defendant also had a duty to exercise reasonable care to prevent a complete outage of its payroll systems, which in turn, affected millions of workers' ability to receive accurate wages, timely wages, and compliant wages from their employer. Defendant breached its duty by failing to remedy the breach and allowing the outage to continue weeks, and even months for some workers.

52. Because Defendant knew that a breach of its systems would damage millions of individuals whose PI was inexplicably stored or was accessible, including Plaintiff and class members, Defendant had a duty to adequately protect

its data systems and the PI contained and/or accessible therein.

53. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and class members' PI. Defendant's failure to comply with state and federal regulations further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PI.

54. In engaging in the negligent acts and omissions as alleged herein, which permitted thieves to access Defendant's systems that stored Plaintiff's and class members' PI, Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This includes failing to have adequate data security measures and failing to protect Plaintiff's and the class members' PI.

55. Plaintiff and the class members are among the class of persons Section 5 of the FTC was designed to protect, and the injuries suffered by Plaintiff and the class members are the types of injury Section 5 of the FTC Act was intended to prevent.

56. Neither Plaintiff nor the other class members contributed to the unauthorized data breach as described in this Complaint.

57. As a direct and proximate cause of Defendant's conduct, Plaintiff and class members have suffered and/or will suffer injury and damages, including but not limited to: (a) the loss of the opportunity to determine for themselves how their PI is used; (b) the publication and/or theft of their PI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the unauthorized data breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (e) costs associated with placing freezes on credit reports; (f) anxiety,

emotional distress, loss of privacy, and other economic and non-economic losses; (g) the continued risk to their PI, which remains in Defendant's possession (and/or Defendant has access to) and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PI in its continued possession; and, (h) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PI.

58. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and class members, their PI would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PI of Plaintiff and class members and all resulting damages.

59. The injury and harm suffered by Plaintiff and class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other class members' PI.

60. As a result of this misconduct by Defendant, the PI and financial information of Plaintiff and class members was compromised, placing them at a greater risk of identity theft, subjecting them to identity theft, and resulting in disclosure of their PI to third parties without their consent. Plaintiff and class members also suffered diminution in value of their PI in that it is now easily available to hackers on the dark web.

61. As a direct and proximate result of Defendant's negligence, Plaintiff and class members have been injured as described herein, and are entitled to damages including, but not limited to, compensatory, nominal, and consequential damages.

///

///

///

## SECOND CAUSE OF ACTION

**Breach of Contract**

**(On behalf of Plaintiff and the Nationwide Class)**

62. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

63. At all relevant times a contract existed and was in force between Defendant on one hand and Plaintiff 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.

64. These written conditions include, but are not limited to the terms and conditions included in its security section of Defendant's Privacy Notice, which states the following:

> "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."[7]

[7] Privacy Notice, Security, UKG, https://www.ukg.com/privacy#4243725865-507775231 (last visited Mar. 10, 2022).

65. Defendant's privacy policy is an agreement between Defendant and its customers and the end-users including Plaintiff and class members who entrusted Defendant with their PI, including sensitive payroll information and records. Defendant breached its own privacy policy by allowing Plaintiff's and class members' PI to be accessed to persons who do not have a "specific business purpose" for accessing their PI.

66. Defendant also breached these duties and violated these promises by failing to properly safeguard the sensitive personal and financial information of Plaintiff and class members by failing to use the promised safeguards, and by failing to use security measures that comply with federal laws including but not limited to Section 5(a) of the FTC Act, by failing to protect customer records and information from threats, hazards, or unauthorized access, by negligently, carelessly, and recklessly collecting, maintaining, and controlling this information, and by engineering, designing, maintaining, and controlling systems that exposed their end-users' sensitive personal and financial information of which Defendant had possession to control the risk of exposure to unauthorized persons.

67. Defendant violated their commitment to maintain the confidentiality and security of the PI of Plaintiff and class members by failing to comply with applicable laws, regulations, and industry standards relating to data security.

68. At all relevant times and in all relevant ways, Plaintiff and class members performed their obligations under the contract in question or were excused from performance of such obligations through the unknown and unforeseen conduct of others.

69. As a direct consequence of the breaches of contract and violations of promises described above, unauthorized users gained access to, exfiltrated, stole, and gained disclosure of the sensitive personal and financial information of Plaintiff and class members, causing them harms and losses including but not limited to (a) economic loss including from unauthorized charges, (b) the loss of

control over the use of their identity, (c) harm to their constitutional right to privacy, (d) lost time dedicated to the investigation of the breach of their own personal information, (e) costs associated with the detection and prevention to cure any harm to their privacy including credit freezes, credit monitoring, and identity theft services, (e) the need for future expenses and time dedicated to the recovery and protection of further loss associated with the continued risk of exposure of their PI, (f) loss of wages stemming from the complete outage of their payroll and timekeeping records, (g) the diminution of value of their PI, (h) and privacy injuries associated with having their sensitive personal and financial information disclosed.

70. Plaintiff and class members were harmed as a result of Defendant's breach because their PI and financial information stemming from their sensitive payroll records was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft. Plaintiff and class members also suffered diminution of value of their PI in that it is now easily available to hackers on the dark web. Plaintiff and class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

71. Plaintiff and class members are entitled to compensatory, consequential, and nominal damages resulting from Defendant's breach of contract.

## THIRD CAUSE OF ACTION

**Violation of the California Consumer Privacy Act ("CCPA")**

**(Cal. Civ. Code § 1798.150)**

**(On behalf of Plaintiff and the California Subclass)**

72. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

73. The CCPA creates a private right of action for violations of the statute

as specified under Cal. Civ. Code § 1798.150(a)(1), which states:

> 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.

74. At all relevant times, Defendant was and still is a "business" under Section 1798.140(b) of the CCPA as a corporation operating in the State of California that collect consumers' personal information, and that either has annual operating revenue above $25 million, collects the personal information of 50,000 or more California residents annually, or derives at least 50 percent of its annual revenue from the sale of personal information of California residents.

75. At all relevant times, Plaintiff and the California subclass were "consumers" under Section 1798.140(g), and also, under the terms of the CCPA as natural persons as defined in Section 17014 of Title 18 of the California Code of Regulations.

76. By the acts described above, Defendant violated the CCPA by negligently, carelessly, and recklessly collecting, maintaining, and controlling Plaintiff's and class members' sensitive personal and financial information and by engineering, designing, maintaining, and controlling systems that exposed Plaintiff's and class members' sensitive personal and financial information of

which Defendant had possession to control the risk of exposure to unauthorized persons, thereby violating their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. Defendant allowed unauthorized users to view, use, manipulate, exfiltrate, and steal the nonencrypted and nonredacted personal information of Plaintiff and class members, including their personal and financial payroll information.

77. Section 1798.150(b) specifically provides that: "No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title." Plaintiff has issued the required notice of these alleged violations to Defendant under Section 1798.150(b) and will be amending this Complaint to seek statutory and injunctive relief upon the expiration of the 30-day cure period pursuant to Section § 1798.150(a). Accordingly, by way of this Complaint, Plaintiff seeks actual pecuniary damages suffered as a result of the violations of the California Consumer Privacy Act on behalf of herself and similarly situated putative class members.

78. As a result of Defendant's violations, Plaintiff and the class members are entitled to all actual and compensatory damages according to proof or statutory damages allowable under the CCPA, whichever are higher, and to such other and further relief as this Court may deem just and proper.

## FOURTH CAUSE OF ACTION

**Violation of the California Customer Records Act ("CRA")**

**(Cal. Civ. Code § 1798.80 *et seq*.)**

**(On behalf of Plaintiff and the California Subclass)**

79. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

80. California Civil Code section 1798.80, *et seq*., known as the

"Customer Records Act" ("CRA") was enacted to "encourage business that own, license, or maintain personal information about Californians to provide reasonable security for that information." Cal. Civ. Code § 1798.81.5(a)(1).

81. Section 1798.81.5(b) of the CRA requires any business that "owns, licenses, or maintains personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," and "to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

82. Section 1798.81.5(d)(1)(B) defines "personal information" as including an individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are 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, (vii) genetic data. Cal. Civ. Code § 1798.81.5(d)(1)(A).

83. Personal information also includes "[a] username or email address in combination with a password or security question and answer that would permit access to an online account." Cal. Civ. Code § 1798.81.5(d)(1)(B).

84. At all relevant times, Defendant was and still is a "business" under the terms of the CRA as sole proprietorships, partnerships, corporations, associations, financial institutions, or other groups, operating in the State of California that

owned or licensed computerized data that included the personal information of Plaintiff and the California subclass.

85. At all relevant times, Plaintiff and the California subclass were "customers" under the terms of the CRA as natural persons who provided personal information to Defendant for the purpose of obtaining a service from Defendant.

86. As alleged in detail above, Defendant failed to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," and "to protect the personal information from unauthorized access, destruction, use, modification, or disclosure," resulting in the massive breach at issue in this complaint that occurred on or around December 11, 2021.

87. By the acts described above, Defendant violated the CRA by allowing unauthorized access to Plaintiff's and class members' personal and financial information, including highly sensitive payroll information.

88. Moreover, the statute 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.

89. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under Section 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.

90. Defendant failed to provide the legally compliant notice under Section 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 employer or through news and media outlets. As a result, Defendant has violated Section 1798.82 by not providing legally compliant and timely notice directly to Plaintiff and class members.

91. Plaintiff, 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).

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

93. As a direct consequence of the actions as identified above, Plaintiff 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, 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.

94. As a direct result of Defendant's violation of the California Customer Records Act, Plaintiff and class members were harmed because their PI and financial information stemming from their sensitive payroll records was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft. Plaintiff and class members also suffered diminution of value of their PI in that it is now easily available to hackers on the dark web. Plaintiff and class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

95. Cal. Civ. Code § 1798.84(b) provides that "[a]ny customer injured as a result of violating the CRA may institute a civil action to recover damages."

96. As a result of Defendant's violations, Plaintiff and class members are entitled to all actual and compensatory damages according to proof, and to non-

economic injunctive relief allowable under the CRA, and to such other and further relief as this Court may deem proper.

**FIFTH CAUSE OF ACTION**

**Violation of the California Constitution's Right to Privacy**

**(California Constitution, Article I, Section 1)**

**(On behalf of Plaintiff and the California Subclass)**

97. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

98. 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.)

99. The right to privacy in California's constitution creates a private right of action against private and government entities. Indeed, "[t]he California Constitution creates a private right that protects individuals from intrusions by private parties." *In re Google Location History Litigation*, 428 F. Supp. 3d 185, 196 (N.D. Cal. Dec. 19, 2019).

100. Plaintiff and the California subclass have a legally recognized and protected privacy interest in their personal, financial, and payroll information provided to and obtained by Defendant, including but not limited to an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes such as the theft of funds and property.

101. Plaintiff and class members reasonably expected Defendant would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their personal and financial information and the unauthorized use of their accounts.

102. Defendant's conduct described herein resulted in a serious invasion of

the privacy of Plaintiff and the California subclass, as the release of personal and financial information, such as the sensitive information Defendant stored in its payroll system could highly offend a reasonable individual. Indeed, the unauthorized access of Plaintiff's and class members' personal and financial information implicated by Defendant's breach rises to the requisite level of an egregious breach of social norms for purposes of establishing an invasion of privacy.

103. As a direct consequence of the actions as identified above, Plaintiff 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, 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 system.

## SIXTH CAUSE OF ACTION

**Violation of the Unfair Competition Law ("UCL")**

**(Cal. Bus. Prof. Code § 17200, *et seq*.)**

**(On behalf of Plaintiff and the California Subclass)**

104. Plaintiff hereby re-alleges and incorporates by reference the above allegations by reference as if fully set forth herein.

105. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

106. By engaging in the above-described unfair business acts and practices, Defendant committed and continues to commit one or more acts of unlawful, unfair, and fraudulent conduct within the meaning of the UCL. These acts and

practices constitute a continuing and ongoing unlawful business activity, as defined by the UCL, and justify the issuance of an injunction and any other equitable relief pursuant to the UCL.

107. Plaintiff and class members were entitled to assume, and did assume, that Defendant would take appropriate measures to keep their PI and safe. Defendant did not disclose at any time that Plaintiff's and class members' PI was vulnerable to hackers because Defendant's data security measures were inadequate.

108. Defendant violated the UCL by misrepresenting, both by affirmative conduct and by omission, the safety of its payroll and timekeeping system, Kronos Private Cloud, specifically the security thereof, and their ability to safely store Plaintiff's and class members' PI and sensitive payroll information. Defendant also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies, and by failing to provide legally compliant notice to Plaintiff and class members detailing the full implication of the breach, as required by the California Consumer Records Act.

109. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and Cal. Bus. & Prof. Code § 22576 (as a result of Defendant failing to comply with its own posted privacy policies).

110. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, none of Defendant's actions or inactions can be said to have had any utility at all. Defendant's failures were clearly injurious to Plaintiff and class members, directly causing the harms alleged below.

111. Defendant also engaged in unfair business practices under the

"tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected.") Indeed, Defendant's acts and omissions thus amount to a clear violation of the law.

112. Defendant also engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it has affected millions of class members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and class members' PI to third parties without their consent, diminution in value of their PI, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff's and class members' PI remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions also violated Section 5(a) of the Federal Trade Commission Act. *See In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

113. Defendant's acts and practices constitute a continuing and ongoing unlawful business activity defined by the UCL. In particular, Defendant failed and continues to fail to implement and maintain reasonable security procedures and practices appropriate to protect the PI, failed and continues to fail to inform Plaintiff

and class members of the full implications of the breach of their PI, and made and continues to make misrepresentations to customers regarding the nature and quality of their data protection, all in violation of, *inter alia*, the following California laws:

(a) Negligence as defined in California Civil Code section 1714;

(b) California Civil Code section 1798.81.5(b);

(c) California Civil Code section 1798.82(a);

(d) California Civil Code section 1798.150(a);

(e) Cal. Bus. & Prof. Code § 22576; and

(f) California Constitution, Article I, Section 1.

114. Defendant's conduct is contrary to the public welfare as it transgresses civil statutes of the State of California designed to protect individuals' constitutional and statutory right to privacy, violates established public policy, and has been pursued to attain an unjustified monetary advantage for Defendant by creating personal disadvantage and hardship to Plaintiff and class members. As such, Defendant's business practices and acts have been immoral, unethical, oppressive, and unscrupulous and have caused injury to Plaintiff and class members far greater than any alleged countervailing benefit.

115. Defendant made and continues to make the representations set forth above, including but not limited to specific representations in their privacy policy regarding the nature and quality of their data security and their representations that they limit access Plaintiff's and class members' PI only to those who have a specific business purpose for maintaining and processing such information. These false representations were, and continue to be made, likely to deceive the public and reasonable consumers. Defendant, at all times when it made these representations, knew them to be false and intended to, and did, induce reliance upon these false representations by Plaintiff and class members, who reasonably relied upon the aforementioned statements and representations and, as a consequence, suffered economic harms and losses.

116. As a direct and proximate consequence of the actions as identified above, Plaintiff and class members suffered and continue to suffer harms and losses including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and attempts to cure any harm to their privacy, 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 and financial information disclosed.

117. In addition, Plaintiff's and class members' PI was taken and is in the hands of those who will use it for their own advantage, or will sell it for value, making it clear that the hacked information is of tangible value. Plaintiff and class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

118. Plaintiff seeks an order of this Court awarding injunctive relief and any other relief allowed under the UCL, including interest and attorneys' fees pursuant to, *inter alia*, Code of Civil Procedure section 1021.5, and to such other and further relief as this Court may deem just and proper.

## PRAYER FOR RELIEF

Plaintiff, on her own behalf and on behalf of all others similarly situated, prays for relief and judgment against Defendant, as follows:

1. For an order certifying the proposed Class and Subclass pursuant to Federal Rules of Civil Procedure, Rule 23;

2. For an order appointing Plaintiff, Cindy Villanueva, as class representative.

3. For appointment of Lebe Law, APLC as class counsel for all purposes;

4. For an order enjoining Defendant, its affiliates, successors,

transferees, assignees, and the officers, directors, partners, agents, and employees thereof, and all other persons acting or claiming to act on their behalf or in concert with them, from continuing the unlawful practices as set forth herein, including but not limited to employing substandard data safety protocols to protect Plaintiff's and class members' payroll information and PI.

5. Requiring Defendant to provide appropriate credit monitoring services to Plaintiff and class members;

6. For actual, compensatory, consequential, and nominal damages according to proof pursuant to the California Civil Code and all other applicable laws and regulations;

7. For civil and statutory penalties available under applicable law;

8. For pre-judgment and post-judgment interest;

9. Finding that Defendant's conduct was negligent, unfair, and unlawful business practices as alleged herein;

10. Enjoining Defendant from engaging in further negligent, unfair, and unlawful business practices alleged herein;

11. For an award of attorneys' fees, costs, and expenses as authorized by applicable law; and

12. For such other and further relief as this Court may deem just and proper.

Dated: March 21, 2022

**LEBE LAW, APLC**

By: /s/ Jonathan M. Lebe

Jonathan M. Lebe
Zachary T. Gershman
Nicolas W. Tomas
Attorneys for Plaintiff Cindy Villanueva, individually and on behalf of all others similarly situated

## DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

Dated: March 21, 2022

**LEBE LAW, APLC**

By: /s/ Jonathan M. Lebe

Jonathan M. Lebe
Zachary T. Gershman
Nicolas W. Tomas
Attorneys for Plaintiff Cindy Villanueva, individually and on behalf of all others similarly situated

# EXHIBIT A

Urgent: Kronos Cybersecurity Incident

Wellpath Communications <Communications@Wellpath.us>

Tue 12/14/2021 10:58 AM

To Craig Diamond <craig.diamond@wellpath.us>

Email Priority: Urgent
Read Immediately

# Urgent: Kronos Cybersecurity Incident

**To:** All Wellpath Team Members
**From:** Wellpath Cybersecurity Team

Wellpath Team Members,

**As you may have seen in the news, UKG Kronos, Wellpath's Kronos HR & Time Keeping Systems partner, is undergoing a ransomware incident affecting Kronos Private Cloud Services, which is the host for Wellpath's timekeeping system. These systems have been unavailable since Saturday night 12/11. Here is the communication from UKG Kronos.**

This means Wellpath Kronos HR & Time Keeping Systems are completely inoperable and unavailable which affects the way you will enter time, request PTO, and more.

Our most important priorities are to pay you accurately and timely, and ensure your personal data is secure.

**Key Information:**

- **At this time there is no indication that any personal individual data has been extracted from the environments.**
- This is a global outage which impacts a number of UKG/Kronos data centers and customers. Wellpath was disrupted along with hundreds to thousands of other companies.
- UKG/Kronos has communicated it could take weeks to get the systems back online.
- You will be paid during this incident. Our teams are working on solutions to ensure your pay is accurate and timely.
- In the next few days more information with be forthcoming regarding interim manual processes. In the meantime:
  - If you swipe in and out at a time clock, continue to do so until further notice.
  - Work with your supervisor on manual recording of time-keeping, PTO requests, and other HR related requests.

Wellpath has established a multi-departmental team that is developing the processes and procedures required to ensure

that all Wellpath Team Members continue to get paid in a timely and accurate fashion. The interim processes, such as manual time tracking, will create some extra work for our Team Members, but are required to ensure everyone is paid accurately.

Please be on the lookout for additional updates and instructions from Wellpath Communications and your leaders.

**Questions & Comments:**

Please direct questions to your manager.

# CIVIL COVER SHEET

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

## I. (a) PLAINTIFFS

Cindy Villanueva, individually and on behalf of all others similarly situated

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

**(c)** Attorneys *(Firm Name, Address, and Telephone Number)*

Jonathan M. Lebe (SBN 284605), Zachary Gershman (SBN 328004), Nicolas W. Tomas (SBN 339752);
Lebe Law, APLC, 777 S. Alameda St., Second Floor, Los Angeles CA 90021, Telephone: (213) 444-1973

## DEFENDANTS

UKG, Inc.

County of Residence of First Listed Defendant Broward County
*(IN U.S. PLAINTIFF CASES ONLY)*

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

Attorneys *(If Known)*

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

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

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

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

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

**CONTRACT**
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

**REAL PROPERTY**
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

**TORTS**

**PERSONAL INJURY**
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

**PERSONAL INJURY**
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

**PERSONAL PROPERTY**
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

**CIVIL RIGHTS**
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

**PRISONER PETITIONS**

**HABEAS CORPUS**
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

**OTHER**
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

**FORFEITURE/PENALTY**
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

**LABOR**
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

**IMMIGRATION**
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

**BANKRUPTCY**
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

**PROPERTY RIGHTS**
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

**SOCIAL SECURITY**
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

**FEDERAL TAX SUITS**
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

**OTHER STATUTES**
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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

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

## VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act, 28 U.S.C. 1332(d)

Brief description of cause:
Data breach; breach of privacy.

## VII. REQUESTED IN COMPLAINT:

✔ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

**DEMAND $**

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

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

JUDGE

DOCKET NUMBER

## IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

**(Place an "X" in One Box Only)** ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

**DATE** 03/21/2022

**SIGNATURE OF ATTORNEY OF RECORD**

# INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

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

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

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

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

**II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

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

**IV. Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

**V. Origin.** Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

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

**VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

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

**IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

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