UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ELIZABETH TAYLOR, on behalf of herself and all others similarly situated, Plaintiffs, vs. UKG, INC., and BETH ISRAEL DEACONESS HOSPITAL - PLYMOUTH, INC. Defendants.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Elizabeth Taylor ("Ms. Taylor" or "Plaintiff") on behalf of herself and all others similarly situated (the "Class" or "Class Members"), brings this action against Defendants UKG, Inc. ("UKG") and Beth Israel Deaconess Hospital - Plymouth, Inc. ("Beth Israel") (collectively, the "Defendants") to obtain damages, restitution, and injunctive relief for the Class. Plaintiff alleges the following based on personal knowledge, the investigation of counsel, and information and belief.

NATURE OF THE ACTION

1. Plaintiff and Class Members are hourly employees who were not paid the full amount of wages to which they are entitled for all of their work in a timely fashion by Defendants.

2. Plaintiff and Class Members provided their personally identifiable information ("PII") to Defendants at their request, including names, addresses, employee IDs, and social security numbers. Due to Defendants' failure to implement and maintain reasonable safeguards to protect Plaintiff's PII, criminals obtained access to Plaintiff's PII, which resulted in substantial

harm to Plaintiff and the Class.[1]

3. This class action seeks to redress Defendants' unlawful withholding of wages for Plaintiff and Class Members and the negligent disclosure of over 8 million employees' PII in a massive data breach on or around December 11, 2021 ("Data Breach"). On that date, and possibly on others, Defendants' inadequate security measures allowed unauthorized individuals to access and render unusable a workforce management software application Defendants used to process payroll and store data that contained the PII of Plaintiff and other individuals.[2]

4. As a result of the Data Breach, Plaintiff and Class Members were not timely paid the full amount of wages to which they are entitled.

5. Plaintiff and the Class Members also now bear an immediate and heightened risk of all manners of identity theft. Plaintiff has incurred, and will continue to incur, damages in the form of, *inter alia*, an imminent threat of identity theft, loss of privacy and the value of personal information, deprivation of the benefit of the bargain, and/or the additional damages set forth in detail below.

JURISDICTION AND VENUE

6. This Court has personal jurisdiction over Defendant Beth Israel Deaconess Hospital - Plymouth, Inc., because it maintains a headquarters in and has its principal place of business in Massachusetts.

7. This Court has personal jurisdiction over Defendant UKG Inc. because it has had systematic and continuous contacts with the State of Massachusetts. UKG is registered to do business in Massachusetts with the Massachusetts Secretary of State. UKG contracts with many

[1] *See UKG Kronos Community*, Communications Sent to Impact Kronos Private Cloud (KPC) Customers, https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US.
[2] *See id.*

businesses in Massachusetts to provide human resources services, including payroll services.

8. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and Plaintiff and one or more members of the classes are residents of a different state from a defendant.

9. This Court has jurisdiction over the Massachusetts Wage Act claim pursuant to M.G.L c. 149, § 150, as well as the federal supplemental jurisdiction statute 28 U.S.C. § 1367(a).

10. Venue is proper in the District of Massachusetts because, pursuant to 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to the claims occurred in Massachusetts.

PARTIES

11. Plaintiff Elizabeth Taylor is a citizen of Massachusetts and a resident of Carver, Massachusetts.

12. On approximately December 11, 2021, Plaintiff's PII was exposed in the Data Breach. On one or more weeks after December 11, 2021, Plaintiff was not timely paid for the full amount of wages due and her PII was exposed. If Plaintiff had known that Defendants would not adequately protect her PII, she would have either refused to provide such information, or taken action to challenge the condition of employment imposed by Defendant Beth Israel that she disclose PII and prohibit Defendants' access to this sensitive and private information until the Data Breach security issue was resolved.

13. Defendant Beth Israel Deaconess Hospital – Plymouth, Inc. is a Massachusetts Corporation with its principal place of business at 275 Sandwich St., Plymouth, MA 02360.

14. Defendant UKG Inc. is a Delaware Corporation with its principal place of business

at 2000 Ultimate Way, Weston, FL 33326.

FACTUAL BACKGROUND

A. Plaintiff's Status As An Employee

15. Plaintiff was employed by Beth Israel as an hourly employee during the relevant time period.

16. During the relevant time period, Beth Israel employed hourly employees to work in numerous sectors of the health care industry.

17. Plaintiff's principal job duties included, but were not limited to, providing care for Beth Israel's patients as a registered nurse.

18. Plaintiff was paid on an hourly basis.

19. Beth Israel regularly scheduled Plaintiff's work hours.

20. Plaintiff regularly reported her hours to Beth Israel, as instructed by Beth Israel.

21. Beth Israel regularly received reports indicating the hours worked by Plaintiff.

22. On or about December 13, 2021, Beth Israel instituted a "payment freeze" for all hourly employees, such that the pay for each pay period following that date was set arbitrarily to the period prior to the freeze, with limited exception.

23. Beth Israel failed to pay Plaintiff the full amount of wages to which she was entitled for all of her work time in a timely fashion.

24. Plaintiff or Plaintiff's representative made numerous requests for payment of their wages in full, but these requests were denied.

25. Plaintiff did not furnish her work gratuitously.

26. Plaintiff worked with the expectation that she would be paid in full for all hours worked in a timely fashion.

27. Beth Israel did not expect Plaintiff to perform any work for Defendant gratuitously.

28. UKG operated and provided a workforce and management software, Kronos Private Cloud, by which Beth Israel maintained and distributed its payroll to employees.

29. UKG was acting in the interest of Beth Israel in relation to Plaintiff, Class Members, and all employees, by providing this workface and management software.

30. Defendants set compensation policies for Plaintiff and the Class. Defendants were jointly responsible for ensuring that Plaintiff and the Class were properly paid each pay period. Defendants were also jointly responsible for the unlawful withholding of payments subsequent to the Data Breach.

B. UKG's Data Breach.

31. Due to inadequate security measures, on or about December 11, 2021, UKG was the subject of a ransomware attack, whereby criminals obtained access to Plaintiff's and Class Members' PII and Kronos Private Cloud was rendered unusable.[3]

32. Kronos Private Cloud is used by thousands of employers, including Beth Israel, and 8 million employees to manage work schedules, track hours, and calculate paychecks.[4]

33. Defendants store employees' PII in Kronos Private Cloud, which can include, *inter alia*, employee names, addresses, employee ID numbers, and social security numbers.[5]

34. The PII of millions of individuals may have been exposed to unauthorized cybercriminals when they gained access to UKG's server.[6]

---

[3] *Id.*
[4] Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, NPR (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.
[5] Jennifer Korn, *Kronos ransomware attack could impact employee paychecks and timesheets for weeks*, CNN (Dec. 17, 2021), https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html.
[6] *See id.*

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.