



RECEIVED

JAN 12 2023

OFFICE OF CONSUMER AFFAIRS

mwe.com

Edward Zacharias
Attorney at Law
ezacharias@mwe.com
+1 617 535 4018

January 5, 2024

VIA USPS CERTIFIED MAIL

Undersecretary Edward A. Palleschi
Office of Consumer Affairs and Business Regulation
501 Boylston St., Suite 5100
Boston, MA 02116
data.breaches@mass.gov

Re: Data Security Incident

Dear Undersecretary Palleschi,

We write on behalf of UKG, a provider of human resources, payroll, and workforce management solutions, whose customers include hospitals and health systems. UKG recently experienced an incident resulting from the inadvertent disclosure of a report containing personal information of employees of New York City Health + Hospitals ("NYCH+H") to five other UKG customers. On behalf of UKG, we write to provide you notice of the incident and inform you that Massachusetts residents were impacted. This letter also explains the steps that have been taken to address the incident.

What Happened? On April 17, 2023, a UKG employee created a file that included the personal information of NYCH+H employees as part of a data conversion of NYCH+H employee records from one UKG business solution to another (the "File"). The UKG employee then inadvertently saved the File to a shared system folder in which training templates and materials used with customers were saved. Thereafter, UKG employees unknowingly copied the shared folder, which included the File, onto five different customer environments in connection with training sessions conducted with those customers. On October 30, 2023, UKG became aware of the inadvertent disclosure of NYCH+H data and, upon investigation, determined that the File was accessed on nine occasions by six separate userIDs associated with five UKG customers. The incident was limited to the File, and the File was only available to the five customers for a limited period of time. Importantly, *there is no evidence that the information was used by any unauthorized recipient for a fraudulent purpose*. Furthermore, there is no evidence that the incident impacted other applications, customers, or systems within UKG's environment and the incident did not cause any business interruption to NYCH+H or UKG.

What Information was Impacted? The incident impacted the personal information of approximately 14 residents of this jurisdiction, all of which are employees of NYCH+H. The information involved included the following data elements of NYCH+H's employees: names, addresses, demographic information, recent salary information, social security numbers, and banking account and routing information. The incident **did not** impact the personal health information or medical records of employees.



RECEIVED

JAN 12 2023

OFFICE OF CONSUMER AFFAIRS

mwe.com

Edward Zacharias
Attorney at Law
ezacharias@mwe.com
+1 617 535 4018

January 5, 2024

VIA USPS CERTIFIED MAIL

Undersecretary Edward A. Palleschi
Office of Consumer Affairs and Business Regulation
501 Boylston St., Suite 5100
Boston, MA 02116
data.breaches@mass.gov

Re: Data Security Incident

Dear Undersecretary Palleschi,

We write on behalf of UKG, a provider of human resources, payroll, and workforce management solutions, whose customers include hospitals and health systems. UKG recently experienced an incident resulting from the inadvertent disclosure of a report containing personal information of employees of New York City Health + Hospitals ("NYCH+H") to five other UKG customers. On behalf of UKG, we write to provide you notice of the incident and inform you that Massachusetts residents were impacted. This letter also explains the steps that have been taken to address the incident.

What Happened? On April 17, 2023, a UKG employee created a file that included the personal information of NYCH+H employees as part of a data conversion of NYCH+H employee records from one UKG business solution to another (the "File"). The UKG employee then inadvertently saved the File to a shared system folder in which training templates and materials used with customers were saved. Thereafter, UKG employees unknowingly copied the shared folder, which included the File, onto five different customer environments in connection with training sessions conducted with those customers. On October 30, 2023, UKG became aware of the inadvertent disclosure of NYCH+H data and, upon investigation, determined that the File was accessed on nine occasions by six separate userIDs associated with five UKG customers. The incident was limited to the File, and the File was only available to the five customers for a limited period of time. Importantly, *there is no evidence that the information was used by any unauthorized recipient for a fraudulent purpose*. Furthermore, there is no evidence that the incident impacted other applications, customers, or systems within UKG's environment and the incident did not cause any business interruption to NYCH+H or UKG.

What Information was Impacted? The incident impacted the personal information of approximately 14 residents of this jurisdiction, all of which are employees of NYCH+H. The information involved included the following data elements of NYCH+H's employees: names, addresses, demographic information, recent salary information, social security numbers, and banking account and routing information. The incident **did not** impact the personal health information or medical records of employees.

Undersecretary Layla R. D'Emilia
January 5, 2024
Page 2

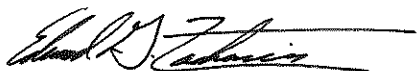
Steps UKG has taken. When UKG learned of the security incident, it initiated its incident response plan, taking steps to determine the scope, mitigate any impacts, and determine the root cause. This included promptly taking action to remove the File from the shared system folder, deleting the File from each customer's environment within UKG's control, and ensuring that no further copies of the File were available within UKG or customer environments managed by UKG. Further, UKG confirmed that the File was not downloaded to any UKG employee's computer.

UKG notified NYCH+H on November 2, 2023 and has been in regular communications with NYCH+H in connection with the response efforts. UKG has offered to make any notifications that NYCH+H has determined are required or appropriate to make under applicable laws. Additionally, UKG has engaged the five customers that received access to the File, advised them of the incident, requested each customer to delete any copies of the File in their possession, and received written assurances from each of the five customers related to the same. UKG has also implemented a technical fix within these shared folders to prevent this kind of issue from occurring again in the future.

UKG has conducted a risk assessment of the incident. There is no evidence that the information was used by any unauthorized recipient for a fraudulent purpose and UKG does not believe any individual's personal information is at risk. Nevertheless, at the request and under the authorization of NYCH+H, UKG intends to begin notifying impacted individuals on or around January 5, 2024, and will also notify consumer reporting agencies. Impacted individuals will receive written notice pursuant to the enclosed notification letter template and will be offered complementary credit monitoring services.

For more information: Please do not hesitate to contact us if you have any questions regarding this letter.

Sincerely,



Edward Zacharias

cc: Laura Secor
Senior Corporate Counsel, Privacy and Product
UKG Inc.
laura.secor@ukg.com



Secure Processing Center
20 Oser Ave
Suite 100
Hauppauge, NY 11788

<<Date>>

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Dear <<First Name>> <<Middle Name>> <<Last Name>>:

UKG Inc., and its affiliates and subsidiaries (collectively, “UKG” or “we”), is a provider of payroll and workforce management solutions that provides services to your employer, New York City Health + Hospitals (“NYCH+H”). We place a high value on maintaining the privacy and security of the information we maintain for our customers. We are writing to inform you of an incident involving the inadvertent disclosure of some of your personal information. This letter explains the incident, the measures we have taken in response, and the steps you can take.

What Happened? A file that included the personal information of NYCH+H employees (the “File”) was created by UKG in the normal course of providing services to NYCH+H. On October 30, 2023, UKG became aware that the File was inadvertently exposed to five other customers and promptly opened an investigation. *Importantly, the File was not exposed beyond these five customers and UKG does not have any evidence that your information was used by any unauthorized recipient for a fraudulent purpose or that the security of your personal information is at risk.*

What Information Was Involved? The information in the File included your name, address, demographic information, recent salary information, social security number, and banking and routing information.

What Are We Doing? Data privacy and security are among our highest priorities, and we have extensive measures in place to protect information entrusted to us. Upon discovering the incident, we immediately took action by deleting the File from each customer’s environment within UKG’s control, and ensuring that no further copies of the File were available within UKG or customer environments managed by UKG. Additionally, UKG worked with the five customers that inadvertently received access to the File, advised them of the incident, requested each customer delete any copies of the File in their possession, and received written assurances from each of the five customers related to the same. To help prevent similar incidents from happening in the future, we have changed certain workflow processes and implemented additional procedures to further strengthen the security of our IT system environments, including expanding the scanning and monitoring program of these environments.

What Can You Do? Enclosed with this letter are some steps you can take to protect your information. *Again, we have no evidence that any personal information has been used inappropriately.* However, as a measure of added security and to help protect your identity, we are offering a complimentary 24-month membership to Identity Defense Complete. This product provides you with services including credit monitoring, identity restoration, and \$1,000,000 of identity theft insurance. To activate your membership and start monitoring your personal information, please follow the steps below before your enrollment deadline, <<Enrollment Deadline>>:

Identity Defense Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring

- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance¹²

Identity Defense Enrollment Instructions

To enroll in Identity Defense, visit <https://app.identitydefense.com/enrollment/activate/ukgi>

1. **Enter your unique Activation Code** <<Activation Code>>
Enter your Activation Code and click 'Redeem Code'.
2. **Create Your Account**
Enter your email address, create your password, and click 'Create Account'.
3. **Register**
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. **Complete Activation**
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1-866-622-9303.

For More Information. We regret that this incident occurred and any concern it may cause you. If you have additional questions, please call our dedicated, toll-free call center at 1-888-541-1605, Monday through Friday between 8:00 a.m. and 8:00 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Peter Acton
Vice President, Deputy General Counsel

¹ Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

² Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com (800) 525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com (888) 397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com (800) 916-8800

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a Connecticut resident, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727- 3400, www.oag.dc.gov.

If you are a Kentucky resident, you can obtain information about steps you may take to avoid identity theft from following sources: the FTC (see contact information above), the major consumer credit reporting agencies (see contact information above), and the Office of the Kentucky Attorney General: 700 Capital Avenue, Suite 118, Frankfort, KY 40601-3449, www.ag.ky.gov, 1-888- 432-9257.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1- 800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, (914) 834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, <https://ncdoj.gov>, 1-877-566-7226.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, (401) 274-4400 or file a police report by contacting (401) 444-1000.