UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

James T. Buechler, and all others similarly situated, Plaintiff, v. MedQuest Pharmacy, Inc., a Utah Corporation, Innovations Group, Inc., a Delaware Corporation, and UpHealth, Inc., a Delaware Corporation, Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff James T. Buechler ("Plaintiff"), individually and on behalf of all other similarly situated individuals, and by and through his undersigned counsel files this Class Action Complaint against MedQuest Pharmacy, Inc. ("MedQuest"), Innovations Group, Inc. ("IGI"), a subsidiary of UpHealth, Inc. ("UpHealth"), and UpHealth (collectively, "Defendants"), and alleges the following based upon personal knowledge of facts and upon information and belief based upon the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. With this action, Plaintiff seeks to hold Defendants responsible for the harms they caused Plaintiff and the nearly 40,000 similarly situated persons in the massive and preventable data breach that took place between October 27, 2021, and October 30, 2021, by

which cybercriminals gained access to Defendants' inadequately protected systems where sensitive personal information was kept unprotected (the "Data Breach" or "Breach").[1]

2. The cybercriminals gained access to Defendants' system with the apparent intention of stealing protected personal information and protected health information of thousands of individuals whose information was stored on Defendants' computer systems.

3. UpHealth is a digital health technology platform that partners with providers, hospitals, health systems, healthcare facilities, and payors to manage care for customers.[2] UpHealth is a publicly traded company registered with the U.S. Security and Exchange Commission.

4. MedQuest and IGI are subsidiary companies of UpHealth. MedQuest retails prescription and non-prescription medicines. MedQuest serves customers in the State of Utah and is licensed to dispense to patients in all 50 states.[3]

5. MedQuest collaborates with its partners and affiliates to develop a "customized approach to medication…known as personalized healthcare" to customize medications to the needs of individual patients.[4]

6. Plaintiff and Class members are required, as patients of Defendants and their affiliate partners, to provide Defendants with their "Personal and Medical Information" (defined below), with the assurance that such information will be kept safe from unauthorized access. By taking possession and control of Plaintiff's and Class members' Personal and

[1] *See* https://www.hipaajournal.com/memorial-health-system-confirms-216k-patients-affected-by-august-2021-ransomware-attack/#:~:text=MedQuest%20Pharmacy%20Data%20Breach%20Affects,detected%20on%20November%2018%2C%202021.
[2] *See* https://www.crunchbase.com/organization/uphealth-22eb
[3] *See* https://medquest.com/
[4] *See* https://medquest.com/

Medical Information, Defendants assume a duty to securely store the Personal and Medical Information of Plaintiff and the Class.

7. Defendants breached this duty and betrayed the trust of Plaintiff and Class members by failing to properly safeguard and protect their Personal and Medical Information, thus enabling cybercriminals to compromise their systems and steal this sensitive information.

8. The compromised Personal and Medical Information at issue includes (i) patient contact information (such as patient name, guarantor name, address, email address, gender, and date of birth); (2) Social Security number, driver's license number, state identification number, and/or financial account information; (3) health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, medical record numbers, diagnosis, prescription information, physician names, referring doctor names, and Medical Record Numbers); and (5) billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by the patient's provider).[5] Specifically, Plaintiff's

9. Defendants' misconduct – failing to timely implement adequate and reasonable measures to protect Plaintiff's Personal and Medical Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that they did not have adequate security practices in place to safeguard the Personal and Medical Information, failing to honor their promises and representations to protect Plaintiff's and Class members' Personal and Medical Information,

[5] *See* https://www.hipaajournal.com/memorial-health-system-confirms-216k-patients-affected-by-august-2021-ransomware-attack/#:~:text=MedQuest%20Pharmacy%20Data%20Breach%20Affects,detected%20on%20November%2018%2C%202021.

and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and Class members across the United States.

10. Due to Defendants' negligence and failures, cybercriminals obtained and now possess everything they need to commit personal and medical identity theft and wreak havoc on the financial and personal lives of nearly 40,000 individuals for decades to come.

11. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that their Personal and Medical Information has been released into the criminal cyber domains, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal and Medical Information. Additionally, Plaintiff and Class members have already lost time and money responding to and mitigating the impact of the Data Breach.

12. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages, statutory damages, punitive damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendants' data security systems and protocols), reasonable attorney fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems proper.

THE PARTIES

Plaintiff James T. Buechler

13. Plaintiff James T. Buechler is a citizen and resident of Maryland.

14. Plaintiff is a patient of MedQuest.

15. Plaintiff received a letter from MedQuest dated December 23, 2021, informing him that his first and last name, date of birth, mailing address, email address, telephone number,

gender, Social Security number, driver's license number, medical record number, health information (including prescription information), referring doctor, date(s) of treatment, health insurance policy information or policy number (including Medicare number, if applicable), health insurance claim number or claim or appeal information, internal MedQuest identification number, financial account or payment card information (including expiration date, access code, and CVV), and account login credentials were or could have been compromised in the Data Breach. *See* **Exhibit 1**, the "Notice."

16. Plaintiff was required to provide Defendants with highly sensitive personal, health, and insurance information, including his Personal and Medical Information compromised in the Data Breach. Plaintiff believes this is a standard practice required of all Defendants' patients.

17. Because of Defendants' negligence leading to the Data Breach, Plaintiff's Personal and Medical Information is now in the hands of cyber criminals and Plaintiff is now under imminent risk of identity theft and fraud, including medical identity theft and medical fraud.

18. The imminent risk of medical identity theft and fraud that Plaintiff now faces is substantial, certainly impending, and continuous and ongoing because of the negligence of Defendants, which negligence led to the Data Breach. Plaintiff has already been forced to spend time and money responding to the Data Breach in an attempt to mitigate the harms of the Breach and determine how best to protect himself from identity theft and medical information fraud. These efforts are continuous and ongoing.

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.