Exhibit A
to
Notice of Removal

Filing # 134054313 E-Filed 09/03/2021 05:30:50 PM

IN THE CIRCUIT COURT FOR THE FIFTH JUDICIAL CIRCUIT IN AND FOR LAKE COUNTY, FLORIDA

CHRYSTAL HOLMES, on behalf of herself and all others similarly situated, Plaintiff, vs. THE VILLAGES TRI-COUNTY MEDICAL CENTER, INC. d/b/a UF HEALTH CENTRAL FLORIDA, LEESBURG REGIONAL MEDICAL CENTER, INC. d/b/a UF HEALTH CENTRAL FLORIDA, and CENTRAL FLORIDA HEALTH, INC. d/b/a UF HEALTH CENTRAL FLORIDA, Defendants.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Chrystal Holmes ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against The Villages Tri-County Medical Center, Inc. d/b/a UF Health Central Florida, Leesburg Regional Medical Center, Inc. d/b/a UF Health Central Florida ("Leesburg Hospital"), and Central Florida Health, Inc. d/b/a UF Health Central Florida (collectively, "Defendants"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personal identifiable information that they acquired from their patients. Defendants required this information from their patients or recorded this information for their

patients as a condition or result of medical treatment, including without limitation, names, addresses, dates of birth, and/or Social Security numbers (collectively, "personal identifiable information" or "PII") as well as health insurance information, medical record numbers, patient account numbers, and/or limited treatment information (collectively, "protected health information" or "PHI").

2. Defendants are the registered owners of the fictious name "UF Health Central Florida" ("UFHCF") and individually and collectively operate under this fictitious name.

3. UFHCF is a health care system that "care[s] for patients in Lake, Sumter, and Marion counties through inpatient acute hospital services at UF Health The Villages® Hospital and UF Health Leesburg Hospital, inpatient rehabilitation services at UF Health The Villages® Rehabilitation Hospital, adult inpatient psychiatric services at the UF Health Leesburg Hospital Senior Behavioral Health Center and diagnostic laboratory services at several locations."[1]

4. In order to obtain medical treatment, Plaintiff and other patients of UFHCF entrust and provide to UFHCF an extensive amount of PII. UFHCF also records an extensive amount of PHI regarding its patients, including treatment information. UFHCF retains this information on computer hardware—even long after the treatment relationship ends. UFHCF acknowledges that it understands the importance of protecting information.

5. On or around May 29 to May 31, 2021, an unauthorized actor obtained unauthorized access to UFHCF's computer network as part of a ransomware attack (the "Cybersecurity Event").

6. The unauthorized actor may have accessed the PII and PHI of UFHCF's current and former patients, including Plaintiff and Class Members.

[1] *See* "About Us", https://www.centralfloridahealth.org/ (last visited Aug. 30, 2021).

7. In a "Notice to Our Patients of Cybersecurity Event" posted on its website (the "Website Notice"), UFHCF advised that it was informing its current and former patients of the Cybersecurity Event and mailing them letters.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, UFHCF assumed legal and equitable duties to those individuals. UFHCF admits that the unencrypted PII and PHI exposed to "unauthorized activity" included names, addresses, dates of birth, and/or Social Security numbers as well as health insurance information, medical record numbers, patient account numbers, and/or limited treatment information.

9. The exposed PII and PHI of UFHCF's current and former patients can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. UFHCF's current and former patients face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

10. This PII and PHI was compromised due to UFHCF's negligent and/or careless acts and omissions and the failure to protect PII and PHI of UFHCF's current and former patients.

11. Until notified of the breach, Plaintiff and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

12. Plaintiff bring this action on behalf of all persons whose PII and/or PHI was compromised as a result of UFHCF's failure to: (i) adequately protect the PII and PHI of UFHCF's current and former patients; (ii) warn UFHCF's current and former patients of UFHCF's inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities

and incidents. UFHCF's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of UFHCF's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Cybersecurity Event, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in UFHCF's possession and is subject to further unauthorized disclosures so long as UFHCF fails to undertake appropriate and adequate measures to protect the PII and PHI, and at the very least, are entitled to nominal damages .

14. UFHCF disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that UFHCF's current and former patients' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

15. Plaintiff Chrystal Holmes is a citizen of Florida residing in Lake County, Florida. On or around July 30, 2021, Plaintiff Holmes received UFHCF's letter notifying her of the

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.