

EXHIBIT A

IN THE CIRCUIT COURT FOR THE TWELFTH JUDICIAL
CIRCUIT IN AND FOR SARASOTA COUNTY, FLORIDA

STEVEN K. FARMER,

on behalf of himself and all others
similarly situated,

Plaintiff,

v.

HUMANA INC.,
a Delaware corporation,

and

COTIVITI, INC.,
a Delaware corporation,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Steven K. Farmer ("Plaintiff") brings this Class Action Complaint against Humana Inc. ("Humana") and Cotiviti, Inc. ("Cotiviti") (collectively, "Defendants"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his 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 and sensitive information that Cotiviti, with Humana's authorization and approval, collected from medical providers, including, without limitation, full Social Security numbers, partial Social Security numbers, names, dates of birth, addresses, cities, states, zip codes, phone numbers, email addresses, member identification numbers, subscriber identification numbers, dates of services, and/or dates of death (collectively, "personal identifiable information" or "PII") as well as provider names, medical record numbers, treatment related information, and/or

actual images (x-ray, photographs, etc.) (collectively, “protected health information” or “PHI”). Plaintiff also alleges Defendants failed to provide timely, accurate, and adequate notice to Plaintiff and similarly situated current and former members of Humana (collectively, “Class Members”) that their PII and PHI had been exposed and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. Humana provides medical benefit plans to approximately 17 million members. Humana’s members entrust Humana, either directly or through medical providers, with an extensive amount of their PII and PHI. Humana asserts that it understands the importance of protecting such information.

3. On or before December 22, 2020, Humana learned that PII and PHI for approximately 62,000 of its members had been exposed to unauthorized individuals through a personal “Google Drive” account (the “Data Breach”).

4. Humana determined that the Data Breach occurred because Cotiviti, with Humana’s authorization and approval, collected the PII and PHI from medical providers and then shared the PII and PHI with a subcontractor, “Visionary,” which, from October 12, 2020 through December 16, 2020, disclosed the PII and PHI to unauthorized individuals to promote a personal business endeavor.

5. More than two months later, in a “Notice of Privacy Incident,” dated March 1, 2021, Humana advised Plaintiff of the Data Breach.

6. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Humana admits that the unencrypted PII and PHI exposed to unauthorized individuals included names, Social

Security numbers, dates of birth, treatment related information, and/or actual images (x-ray, photographs, etc.

7. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and dates of birth.

8. This PII and PHI was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members. In addition to Defendants' failure to prevent the Data Breach, after discovering the breach, Defendants waited more than two months to report it to the states' Attorneys General and affected individuals.

9. As a result of this delayed response, 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.

10. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) ensure that the PII and PHI of Plaintiff and Class Members would be adequately safeguarded from misuse or exposure to unauthorized individuals whenever Defendants shared it with third parties. Defendants' conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendants'

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 Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

12. Defendants 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 the PII and PHI of Plaintiff and Class Members 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

13. Plaintiff Steven Farmer ("Farmer") is a Citizen of Florida residing in Sarasota County, Florida. Mr. Farmer received Humana's *Notice of Privacy Incident*, dated March 1, 2021, on or about that date.¹ The notice stated that Plaintiff's full Social Security number, partial Social Security number, name, date of birth, address, city, state, zip code, phone number, email address,

¹ Ex. 1.



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.