Plaintiff,

v.

AMAZON WEB SERVICES, INC. and **JOHN DOE**, In Possession of Stolen SalusCare, Inc. Confidential Information, Thereby Injuring SalusCare, Inc. and Its Customers, Clients, and Vendors,

Defendants.

VERIFIED COMPLAINT AND DEMAND FOR JURY TRIAL
INJUNCTIVE RELIEF REQUESTED

Plaintiff SalusCare,Inc. ("SalusCare" or "Plaintiff") hereby complains and alleges against Amazon Web Services, Inc. ("Amazon") and John Doe ("John Doe"), as follows:

NATURE OF THE ACTION

1. This is a civil action for injunctive relief and damages against Defendant John Doe and for injunctive relief against Amazon arising under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Computer Abuse and Recovery Act, Section 668.801, et seq. Florida Statutes. As further alleged below, Defendant John Doe wrongfully accessed SalusCare's computer systems and extracted SalusCare's confidential business and patient financial and health-related information and other

sell the stolen information on the "dark web" where it will likely be used to promote identity theft and possible online disclosure—any of which would cause substantial, imminent, and irreparable harm to Plaintiff.

THE PARTIES

2. Plaintiff SalusCare is a not-for-profit mental health and substance abuse service provider headquartered in Fort Myers, Florida. Incorporated in 2013, following the merger of Lee Mental Health Center and Southwest Florida Addiction Services (SWFAS), it is the most comprehensive provider of behavioral healthcare services in Southwest Florida.

3. Amazon is a Delaware corporation which provides information storage services to individuals and companies. Amazon is the owner of the server containing the buckets of stolen information. Amazon routinely contracts with entities for such data storage services throughout the United States and the world, including the State of Florida. Amazon is headquartered in and a resident of the State of Washington.

4. Defendant John Doe controls two web-based storage sites, or "buckets," which it has created under contract with Amazon, in which the stolen information has been stored. SalusCare is informed and believes and thereupon alleges that John

will amend this Complaint to allege the true name and capacity of Defendant John Doe when ascertained. Plaintiff has exercised due diligence and will continue to exercise due diligence to determine Defendant John Doe's true name(s), capacity, and contact information, and to effect service on that Defendant.

5. On information and belief, the fictitiously named Defendant is responsible for the occurrences herein alleged, and SalusCare's injuries as herein alleged were proximately caused by such Defendant.

6. On information and belief, the actions and omissions alleged herein to have been undertaken by Defendant and their agents were actions that Defendant authorized, controlled, directed, or had the ability to control, direct, and/or were actions and omissions Defendant assisted, participated in, or otherwise encouraged, and are actions for which Defendant is liable.

JURISDICTION AND VENUE

7. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, as the action arises under the federal Computer Fraud and Abuse Act (18 U.S.C. § 1030) ("CFAA"). This Court has subject-matter jurisdiction under 28 U.S.C. § 1367 over the claims for violation of Florida's Computer Abuse and

the Defendant's unauthorized access into, and misappropriation of information from, a "protected computer" as defined in 18 U.S.C. § 1030(e)(2)(B) that is used for commerce and communication with persons and entities in Florida, and also as a result of Defendant's wrongful conduct causing injurious effect in Florida.

9. This Court has personal jurisdiction over Defendant Amazon because Amazon, through its web-based information storage business, provides web-storage services extensively to individuals and businesses which transmit data and payment therefore from Florida. Accordingly, Amazon operates, conducts, carries on, and a business or business venture in Florida, and is engaged in substantial and not isolated activity in this state.

10. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b). A substantial part of the events or omissions giving rise to SalusCare's claims occurred in this judicial district.

FACTS

11. On or about March 16, 2021, SalusCare learned of the unauthorized access to and exfiltration of its data when issues of "slowness" were detected in its computer network. A prompt forensic inspection revealed that the data had been

12. The breached machines, or computers, are "protected computers" under 18 U.S.C. § 1030(e)(2)(B), which defines a "protected computer" as a computer

> which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications to the United States.

The breached computers are used for interstate and foreign commerce or communication.

13. After discovering the incident, SalusCare acted promptly in contacting Amazon requesting that the buckets of stolen data be "locked." Amazon responded that the bucket accounts had been "suspended." However, Amazon has given no assurance of how long they will remain suspended. SalusCare, in spite of its forensic investigation, has yet been unable to determine the identity of the intruder, the precise scope of the intrusion, and the extent of the damages. This investigation is ongoing.

14. Plaintiff has already been irreparably harmed by Defendant John Doe's illegal misappropriation of SalusCare's data. To date, Plaintiff has been forced to spend a substantial sum of money (in excess of $12,000.00) to investigate 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.