STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DOUBET CONSULTING, LLC and GL2 PARTNERS, INC., individually and on behalf of others similarly situated,

Plaintiffs,

-against-

RACKSPACE TECHNOLOGY, INC.,

Defendant.

Civil Action No.:

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiffs DOUBET CONSULTING, LLC ("Doubet") and GL2 PARTNERS, INC. ("GL2") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this Class Action Complaint against Defendant RACKSPACE TECHNOLOGY, INC. ("Rackspace" or "Defendant"), based upon their individual experiences and personal information, and investigation by their counsel.

INTRODUCTION

1. Plaintiffs, individually and on behalf of all others similarly situated, brings this class action suit against Defendant because of its failure to properly secure and safeguard Plaintiffs' and Class Members' personally identifiable information ("PII") and/or other proprietary and/or highly confidential data (collectively, "Sensitive Data") stored within Defendant's information network, to properly maintain its Hosted Exchange environment so as to provide continuous email service, and/or notify Plaintiffs and Class Members of outages so as to not unreasonably interfere with their access to their Sensitive Data.

2. Launched in 1998, Rackspace touts itself on its website (www.rackspace.com/about) as "multicloud solutions experts" and a leading provider of expertise and managed services across all the major public and private cloud technologies, assisting business customers in over 120

countries. Rackspace is the world's largest managed cloud provider and provides access to such cloud offerings as Amazon Web Services, Microsoft Azure, and OpenStack.

3. According to Defendant, at some point prior to 2:49 AM EST on or about December 2, 2022, Defendant discovered "an issue [that affected its Hosted Exchange Environments]."

4. According to Defendant, at approximately 2:49 AM EST, it was investigating the issues, but provided no further information to Plaintiffs and Class Members. As of that time, Defendant had allegedly already received "reports of connectivity issues" to its Exchange environments, admitting (albeit much later and insufficiently) that users "may experience an error upon accessing the Outlook Web App (Webmail) and syncing their email clients."

5. According to Defendant, over the next several hours, it continued its investigation regarding these connectivity and login issues, admitting (although much later) that users "may experience an error upon attempting to access OWA (Webmail) & sync mail to their email client" or "a prompt [to] re-enter their password."

6. Over the course of the following day, Defendant's investigation continued, with Defendant acknowledging that these "connectivity and login issues greatly impact its clients.

7. According to statements made later on its website, Defendant recognized, and then apologized, for the "major disruption" these issues caused its clients.

8. According to statements made later that evening, Defendant again acknowledged that this "significant failure" in its environment was impacting its clients "greatly." At that time, it directed its clients' account administrators to "manually set up each individual user" on clients' accounts, actions that would require significant time and expense to those clients. During that recommended process, Defendant acknowledged that its clients would be "unable to connect to the Hosted Exchange service to sync new email or send mail using [the] Hosted Exchange." Defendant

further encouraged "admins to configure and set up their users accounts on Microsoft 365 so they can begin sending and receiving mail immediately."

9. According to Defendant, as of December 3, 2022, at 1:57 AM EST, Defendant had determined, and later acknowledged, that the forgoing events were the result of a "security incident".

10. While Defendant claims to have discovered the disruption as early as December 2, 2022, Defendant did not inform victims of the Security Incident other than via an incident report/summary subsequently posted on its website. Indeed, Plaintiffs and Class Members were wholly unaware of the Security Incident, if at all, until their email accounts became unusable and/or they contacted Defendant directly to inquire as to the disruption.

11. Prior to the Security Incident, and in the normal course and scope of performing services for Plaintiffs and Class Members, Defendant acquired, collected and/or stored Plaintiffs' and Class Members' Sensitive Data. Therefore, at all relevant times, Defendant knew, or should have known, that Plaintiffs and Class Members would use Defendant's services to store and/or share Sensitive Data.

12. By obtaining, collecting, using, and deriving a benefit from storing and/or facilitating access to Plaintiffs' and Class Members' Sensitive Data, Defendant assumed legal and equitable duties to those individuals/businesses. These duties arise from state and federal statutes and regulations, as well as common law principles.

13. The confidential information that was compromised in the Security Incident can be used to gain unlawful access to online accounts of present and former clients, carry out identity theft, or commit other fraud and can be disseminated on the internet, available to those who broker and traffic in stolen PII and Sensitive Data .

14. The illegal access to PII and Sensitive Data of minors is particularly nefarious, as awareness of such access is typically delayed for a much longer period of time in the case of children as opposed to adults, giving perpetrators more time to use the PII and Sensitive Data for illegal purposes before detection.

15. While the sophistication of the methods employed in effectuating the Security Incident is not publicly known, it is certain that the Security Incident could have been avoided through basic security measures, encrypting, authentications, and training.

16. At all relevant times, Defendant promised and agreed in various documents to safeguard and protect Personal Identifiable Information (PII) and Sensitive Data in accordance with federal, state, and local laws, and industry standards, including the New York General Business Law, the New York SHIELD Act, and the Texas Deceptive Trade Practices – Consumer Protection Act. Defendant made these promises and agreements on their websites and other written notices.

17. Contrary to these promises, and despite the fact that the threat of a data breach or other security incident has been a well-known risk to Defendant, especially due to the valuable and sensitive nature of the data Defendant collects, stores and maintains, Defendant failed to take reasonable steps to adequately protect the PII and Sensitive Data of current and former clients. The Security Incident was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII and Sensitive Data.

18. As a result of Defendant's failure to take reasonable steps to adequately protect the PII and Sensitive Data of current and former clients, Plaintiffs' and Class Members' PII and Sensitive Data is now on the internet for anyone and everyone to acquire, access, and use for unauthorized purposes for the foreseeable future.

19. Defendant's failure to implement and follow basic security procedures has resulted

in ongoing harm to Plaintiffs and Class Members, who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss and loss of privacy, as well as disruption of their business operations, loss of hosted exchange services and permanent loss of countless e-mails and other stored data.

20. Accordingly, Plaintiffs seek to recover damages and other relief resulting from the Security Incident, including but not limited to, compensatory damages, reimbursement of costs that Plaintiffs and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this incident.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; the number of Members of the proposed Class exceeds 100, and diversity exists because some of the Plaintiffs and Class Members and Defendant are citizens of different states. Subject matter jurisdiction is also based upon the Federal Trade Commission Act (FTCA). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

22. This Court has personal jurisdiction over Defendant as it routinely conducts business in the State where this District is located, conducts substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in the Security Incident was likely stored and/or maintained in accordance with practices emanating from this District.

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.