IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

Q INDUSTRIES, INC., JOHN MOSER, and DANA MOSER WILKINSON, individually and on behalf of all others similarly situated,	**Case No.: 22-cv-01322**
Plaintiffs,	**CLASS ACTION COMPLAINT**
v.	
RACKSPACE TECHNOLOGY, INC.	**JURY TRIAL DEMANDED**
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff Q Industries, Inc., John Moser, and Dana Moser Wilkinson ("Plaintiffs"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Rackspace Technology, Inc. ("Rackspace" or "Defendant"). Based upon personal knowledge as well as information and belief, Plaintiffs specifically allege as follows:

NATURE OF THE ACTION

1. This is a class action for damages brought by Q Industries, John Moser, and Dana Moser on behalf of themselves and all others similarly situated against Rackspace Servicing, LLC, for its failure to exercise reasonable care in securing and safeguarding the sensitive, proprietary data of its customers, and its failure to exercise reasonable care to maintain the stable, reliable cloud computing services its customers rely on in conducting their respective businesses.

2. Rackspace's business is predicated on provision of secure and resilient email and cloud storage services because of the sensitivity of the information stored within its hosted Exchange environment, as well as the messaging and calendaring features that make up its core business functions.

3. Plaintiffs and Class members relied on these services to conduct their business and other related matters.

4. On or around December 2, 2022, unauthorized parties gained access to Rackspace's servers, disrupting its cloud services and exfiltrating sensitive customer data, including sensitive proprietary information belonging to Plaintiffs (the "Data Breach").

5. As of the filing of this Complaint, Plaintiffs and Class members are still unable to access their business email account or propriety data stored on Rackspace's servers, nor do they know when they will be able to access their email or data. Moreover, there has been no assurance offered from Rackspace that the compromised Private Information has been recovered or destroyed.

6. Rackspace only offered its impacted customers free access to Microsoft Exchange Plan 1 licenses on Microsoft 365 for the duration of the Data Breach, which does not guarantee security of Plaintiffs' Private Information and, as Rackspace itself warned, would make it difficult to preserve data for those with hybrid environments as archives would not be available.

7. Accordingly, Plaintiffs assert claims for negligence, gross negligence, negligent misrepresentation, breach of express contract, breach of implied contract, breach of confidence, breach of implied covenant of good faith and fair dealing, unfair and deceptive trade practices, breach of implied warranty of merchantability, breach of express warranty of merchantability, unjust enrichment, and declaratory relief.

PARTIES

A. Plaintiff Q Industries

8. Plaintiff Q Industries is a Nevada corporation with its principal place of business in Phoenix, Arizona. Q Industries brings this action in its individual capacity and on behalf of all others similarly situated.

9. Q Industries manufactures air compressors and related products, such as hoses, for retail.

10. Q Industries is a Rackspace customer and uses Rackspace services in the usual course of its business, including to communicate by way of email with its current and potential customers and business partners. Q Industries also uses Rackspace to store important, proprietary information on Rackspace cloud servers.

11. Now that it cannot access Rackspace services, Plaintiff Q Industries and similarly situated Class members are unable to conduct their respective businesses. Based on Rackspace's own representations, Q Industries anticipates being unable to do so for at least another sixteen weeks.

12. Moreover, the Data Breach has resulted in the compromise of Plaintiff Q Industries' Private Information (defined below) by cybercriminals. Other harms may not materialize for years after the Data Breach, rendering Defendant's limited communications to date regarding the Data Breach woefully inadequate to prevent the harms to Plaintiff Q Industries' business that will continue to occur as a result of the Data Breach.

B. Plaintiff John Moser

13. Plaintiff John Moser is a resident of Phoenix, Arizona and brings this lawsuit on behalf of himself and all others similarly situated.

14. Mr. Moser is the president of Q Industries. He has been impacted by the Data Breach both as president and in his personal capacity, since highly sensitive information about him personally has almost certainly been exfiltrated as a result of the Data Breach.

C. Plaintiff Dana Moser Wilkinson

15. Plaintiff Dana Moser Wilkinson is a resident and citizen of Phoenix, Arizona and brings this lawsuit on her behalf and on behalf of all others similarly situated.

16. Ms. Wilkinson is the chief operating officer (COO) of Q industries. She has been affected by the Data Breach both as COO and in her personal capacity, since highly sensitive information about her personally has almost certainly been exfiltrated as a result of the Data Breach.

D. Defendant

17. Defendant Rackspace Technology, Inc. is a San Antonio, Texas based cloud computing company, with a principal place of business at 1 Fanatical Place, San Antonio, Texas.

18. All of Plaintiffs' claims stated herein are asserted against Rackspace and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

19. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

14. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is in this District.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(1), because Defendant maintains its principal place of business in this District and therefore is a resident in this District pursuant to 28 U.S.C. § 1391(c)(2).

FACTS

16. On or before December 2, 2022, an unauthorized actor conducted a ransomware attack against Rackspace, gaining access to Rackspace's network and the Private Information (defined below) stored thereon. Rackspace's network hosts email and cloud computing services for its customers, including Plaintiffs and the Class, and contains innumerable types of highly sensitive and confidential customer data, including but not limited to, business related correspondence, technical plans, software products, proprietary information, and more (defined herein as the "Private Information").

17. The unauthorized actor installed ransomware, a form of malicious software that copies and encrypts the contents of a server, rendering it inaccessible to the intended user.

18. At some point on or around December 2, 2022, Plaintiffs and Class members were locked out of their Rackspace email and cloud services accounts due to a services outage arising from the Data Breach.

19. On December 2, 2022, at or around 2:49 a.m., Rackspace announced that it was "investigating an issue that is affecting [its] Hosted Exchange environments." It provided no further details.

20. At or around 6:36 a.m. that same day, Rackspace announced that, "Users may experience an error upon attempting to access OWA (Webmail) & sync mail to their email client, or a prompt to re-enter a password."

21. At or around 8:19 p.m., Rackspace announced that it would be providing its customers with a stopgap measure while it sought to solve the issue: Microsoft Exchange Plan 1 licenses on Microsoft 365.

22. On December 3, 2022, at or around 1:57 a.m., Rackspace announced that these problems were the result of a "security incident." It did not provide any details about the incident, nor did it provide any assurances that services would resume in a timely manner.

23. As of the filing of this Complaint, Plaintiffs and Class members remain locked out of their Rackspace services.

24. On information and belief, Plaintiffs and Class members have been told that limited services will be restored eight weeks after their repair request tickets are accepted by Rackspace's IT services contractor, with full functionality restored eight more weeks after that. However, as of December 9, 2022, Plaintiffs' tickets had not yet been accepted. Therefore, the only promise of full restoration of their services Plaintiffs have received is one of sixteen weeks from an unspecified future date, without any recompense by Defendant for the harms Plaintiffs are suffering as a result of this shocking and devastating disruption to their business.

25. As detailed herein, the Breach occurred because Defendant failed to take reasonable measures to protect its network and the Private Information it collected and stored on its network. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the tech industry about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

26. Defendant disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class members' PII 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 a result, the Private Information of Plaintiffs and Class members was compromised through unauthorized access by an unknown third party and Plaintiffs and Class members continue to experience a devastating services outage. Plaintiffs and Class members have a continuing interest in ensuring that their Private Information is and remains safe and that extended services outages such as this never occur again.

A. Rackspace's Services and Privacy Promises

27. Rackspace describes itself as "the multicloud solutions experts" and "a leading provider of expertise and managed services across all the major public and private cloud technologies." [1]

28. Founded in 1998, Rackspace markets itself as particularly devoted to customer service and network security. Describing its history, Rackspace has said, "We were a tiny player looking for a way to differentiate ourselves — to serve business customers better than the big telecom companies and other competitors did. So we hired smart people who were deeply committed to serving customers. We began providing end-to-end customer service and branded it Fanatical Support®. We developed specialized expertise in technologies such as Linux and Windows and network security."[2]

[1] https://www.rackspace.com/about

[2] *Id.*

29. Rackspace claims to provide a superior product compared to other larger services such as Amazon because of its comprehensive support of business customers and expertise in cutting edge technology. It refers to its product as "managed cloud services." [3]

30. Reliability and security are a crucial part of any cloud computing service, but especially so for a boutique, business-focused service that holds itself out as a high-quality alternative to leading technology corporations.

31. In fact, Rackspace promises its business customers that it will provide data protection for them "anytime and everywhere," acknowledging that data disruptions like the one arising from the Data Breach here "can slow down your business and adversely impact customer experiences."[4] Further, Rackspace promises its business customers "the highest levels of data protection."[5]

32. Because of these claims of reliability, quality, and data protection, Plaintiffs and Class members employed Rackspace to provide vital business cloud services.

33. In other words, Plaintiffs and Class members staked their own reputation on Rackspace's reputation. Now, without access to their email and proprietary data, Plaintiffs and Class members would appear to their own customers and clients to be unreliable, untrustworthy, or incompetent, when this is simply not the case.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures as Promised to its Customers

34. Ransomware attacks are not an unknown threat to the cloud services industry, and

[3] *Id.*

[4] https://www.rackspace.com/security/data-privacy-protection.

[5] *Id*.

any reasonable cloud services provider should take adequate steps to protect against them. Rackspace failed to do so here.

35. The U.S. Government has placed businesses such as Rackspace on notice of data security threats. In 2021, the FTC updated its consumer information Safeguards Rule, requiring non-banking financial institutions to develop, implement, and maintain comprehensive security systems to keep their customer's information safe. Against the backdrop of a rapid increase in cybersecurity incidents related to consumer financial information, Samuel Levine, the director of the FTC's Bureau of Consumer Protection stated that "Financial institutions and other entities that collect sensitive consumer data have a responsibility to protect it."[6]

36. As a cloud services provider and self-described network security expert, Rackspace has an even-higher duty than non-technology companies to protect the data entrusted to it. Rackspace acknowledges this duty in its Privacy Notice, in which it affirms its commitment "to providing [its business customers] with the best overall experience in all of [its] products and services" and "protecting [their] privacy."[7] Rackspace also promises to "not sell, retain, use or disclose Personal Information for any purpose other than as set out in an agreement with our customer or as otherwise permitted or required by the CCPA."[8]

37. Almost half of the data breaches globally are caused by internal errors, either human mismanagement of sensitive information, or system errors.[9] Cybersecurity firm

[6] *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches*, https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data

[7] https://www.rackspace.com/information/legal/privacystatement

[8] *Id*.

[9] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.

Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[10] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[11]

38. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[12]

39. To prevent and detect unauthorized access, including the systems changes that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

[10] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.

[11] *Id.*

[12] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

40. To prevent and detect unauthorized access to its systems, including the unauthorized access that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet

for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[13]

41. To prevent the unauthorized access that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  Apply the latest security updates
  Use threat and vulnerability management
  Perform regular audit; remove privilege credentials;
- **Thoroughly investigate and remediate alerts**
  Prioritize and treat commodity malware infections as potential full compromise
- **Include IT Pros in security discussions**
  Ensure collaboration among [security operations], [security admins], and

[13] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

[information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  Monitor for adversarial activities
  Hunt for brute force attempts
  Monitor for cleanup of Event Logs
  Analyze logon events
- **Harden infrastructure**
  Use Windows Defender Firewall
  Enable tamper protection
  Enable cloud-delivered protection
  Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[14]

42. These are basic, common-sense data security measures that every business, not only those who handle sensitive personal information, should be doing. Rackspace, as a sophisticated cloud computing services provider holding itself out as a reliable service for businesses, should have been doing this and even more. By adequately taking these common-sense solutions, Rackspace could have prevented the Data Breach from occurring.

43. Charged with handling the sensitive Private Information of Plaintiffs and the Class, Rackspace knew, or should have known, the importance of safeguarding its customers' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Class members as a result of a breach. Rackspace failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

44. With respect to training, Rackspace specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters,

[14] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

posters, login alerts, email alerts, and team-based discussions;

- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

45. The PII was also maintained on Rackspace's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's negligently maintained systems. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiffs' and Class members' PII was a known risk to Rackspace, and Rackspace was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. Rackspace Failed to Comply with FTC Guidelines

46. Rackspace was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

47. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[15]

[15] *Start With Security: A Guide for Business*, FED. TRADE. COMM'M (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

48. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[16] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

49. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[17]

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. Rackspace failed to properly implement basic data security practices. Rackspace's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[16] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.
[17] *Start with Security*, *supra* note 31.

52. Rackspace was at all times fully aware of its obligation to protect the Private Information of customers because of its position as a trusted student loans services provider. Rackspace was also aware of the significant repercussions that would result from its failure to do so.

D. Damages to Plaintiffs and the Class

53. Plaintiffs and the Class have been damaged by Rackspace's failure to provide reasonably reliable services.

54. Plaintiffs, like other members of the Class, relies upon Rackspace data storage and email services in the regular course of its business.

55. Specifically, Q Industries, as well as many other Class members, relies on email services to connect with its own customers, interface with business partners, and drive sales.

56. Often, sales are initiated, negotiated, and agreed upon entirely through email. This makes the store of previously sent and received emails an invaluable business asset.

57. Plaintiffs and Class members are now locked out of their primary sales vehicle – their email account – during the 2022 December holiday shopping season. The holidays are an incredibly important time for retailers, retail suppliers, and other businesses, and the loss of vital business services during this time is a substantial blow to annual sales volume.

58. Additionally, Plaintiffs and Class members cannot access their proprietary data stored on Rackspace cloud servers. This represents an incalculable loss of business function, as many Class members reasonably relied on Rackspace to safeguard data that they regularly use for their business. This includes data used every day, as well as long-term storage of sensitive material.

59. This loss of business function has already led to lost business opportunities for Plaintiffs and Class members, and will lead to many more still (without any assurance by Defendant that it will compensate Plaintiffs for such losses). It also entails less concrete, but no less grave, reputational damage. Plaintiffs and Class members have staked their reputations as reliable businesses, business partners, and service providers on the security of the cloud services that Rackspace provides. Without access to the cloud, and without a way to guarantee the safety of information about their own customers and clients held on the cloud, Plaintiffs and Class members are left holding the bag for Rackspace's own security failures.

60. Rackspace's stopgap offer of Microsoft 365 services is grossly insufficient, since it does not restore access to the correspondence and proprietary data that Plaintiffs and Class members stored on Rackspace's servers in the first place.

61. In addition, Microsoft 365 is a mass market product, not the high quality, business-oriented comprehensive service that Rackspace's customers, Plaintiffs, and Class members bought and paid for.

62. Moreover, as a result of the Data Breach, Plaintiffs' and Class members' Private Information has almost certainly been compromised by cybercriminals.

63. The ramifications of Rackspace's failure to keep its customers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Proprietary information of businesses, such as technical designs or digital products, can be copied, stolen, and used around the world without permission. Consumer victims of data breaches, such as employees, are more likely to become victims of identity fraud.[18]

[18] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

64. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

65. Defendant further owed and breached its duty to Plaintiffs and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

66. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

67. Plaintiffs and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

68. Plaintiffs and Class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with Rackspace. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

69. Plaintiffs and Class members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

70. Plaintiffs and members of the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

71. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiffs and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

72. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

73. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class members' Private Information.

74. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they

otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

75. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[19]

76. Defendant's failure to adequately protect Plaintiffs' and Class members' Private Information has resulted in Plaintiffs and Class members having to take action to protect themselves from multifarious, vague risks, since they do not know what data was taken or by whom. This requires extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the Breach. Instead, as Rackspace's limited communications with its business customers indicate, it is putting the burden on Plaintiffs and Class members to deal with the devastating impacts the services outage and compromise of Private Information are having on Plaintiffs' and Class members' businesses and personal lives.

77. Plaintiffs and Class members have been damaged in several other ways as well. Plaintiffs and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiffs and Class members have also purchased credit monitoring and other identity protection services, purchased

[19] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class members also suffered a loss of the inherent value of their Private Information.

78. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost sales associated with the disruption of the functionality of Defendant's product and services;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and

f. Anxiety and distress resulting fear of misuse of their Private Information and loss of business opportunities.

79. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

80. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

81. Plaintiffs bring this action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23.

82. Plaintiff proposes the following "Nationwide Class" and "Arizona Subclass" definitions subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Nationwide Class and Arizona Subclass (collectively, the "Class"):

> **Nationwide Class**
>
> All persons, including business entities, whose Private Information became inaccessible and/or was viewed by unauthorized third parties as a result of the Data Breach discovered on or about December 3, 2022.
>
> **Arizona Subclass**
>
> All persons, including business entities, residing in Arizona whose Private Information became inaccessible and/or was viewed by unauthorized third parties as a result of the Data Breach discovered on or about December 3, 2022.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

83. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

84. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the hundreds of thousands.

85. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and

predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant's data security practices and systems prior to and during the Data Breach complied with applicable data security laws and regulations;

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant properly implemented its purported security measures to protect Plaintiffs' and Class members' Private Information from outages, unauthorized capture, dissemination, and/or misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

e. Whether Defendant disclosed Plaintiffs' and Class members' Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Private Information;

g. Whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and Class member's Private Information;

h. Whether Defendant failed to timely notify Plaintiffs and Class members' of the outage of its systems and networks and that such outage resulted from the Data Breach;

i. Whether Defendant was unjustly enriched by its actions and inactions; and

j. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

86. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

87. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the outage and resulting Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

88. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

89. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

90. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On Behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

91. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

92. Upon Defendant's accepting and storing the Private Information of Plaintiffs and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that highly confidential and sensitive proprietary information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected.

93. In light of this special relationship between them, Defendant owed a duty of care to its customers, including Plaintiffs and Class members, not to subject their Private Information

to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

94. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

95. Defendant also breached its duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' Private Information without their consent and in violation of Defendant's own Privacy Notice.

96. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant, as a cloud computing company, knew or should have known about numerous well-publicized data breaches and the danger of ransomware attacks.

97. Defendant knew, or should have known, that its data systems and networks could not adequately safeguard Plaintiffs' and Class members' Private Information.

98. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class members' Private Information and avoid a prolonged outage of services.

99. Because Defendant knew that a breach of their systems would damage thousands of its customers, including Plaintiffs and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

100. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach and resulting outage of services.

101. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

102. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

103. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs' and Class members' Private Information; (2) comply with industry standard

security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

104. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class members' Private Information, and by failing to provide timely, detailed notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class members' Private Information and prevent a prolonged services outage;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Plaintiffs' and Class members' Private Information;

d. Failing to detect in a timely manner that Plaintiffs' and Class members' Private Information had been compromised; and

e. Failing to timely notify Plaintiffs and Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for business losses and misuse of their Private Information.

105. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security to prevent a devastating services outage and failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care

to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendant's possession and control.

106. Defendant's conduct was grossly negligent, as further set forth below, and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiffs and Class members with timely and detailed notice that their Private Information had been compromised.

107. Neither Plaintiffs nor the other Class members contributed to the Data Breach, resulting outage of services, nor the subsequent loss of business opportunities as described in this Complaint.

108. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged throughout this Complaint.

109. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; and (ii) submit to future annual audits of those systems and monitoring procedures.

COUNT II
Gross Negligence
(On Behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

110. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

111. Defendant created a series of circumstances which, together, constituted an imminent or clear and present danger amounting to more than the usual peril.

112. Defendant was aware of the imminent danger. Specifically, Defendant was aware that its data and network security practices, procedures, and protocols were not properly sufficient in light of applicable law and industry standards to protect Plaintiffs' and Class members Private

Information from compromise. Nor were they sufficient to prevent an extended outage severely impacting Plaintiffs' and Class members' respective businesses.

113. Defendant has failed to provide an effective alternative means for Plaintiffs and Class members to continue running their respective businesses while its product and accompanying services remain down.

114. Defendant's omissions occurred in a manner which demonstrates a conscious disregard for the consequences. Defendant's omissions were an extreme departure from the standard of care that is required in the industry. Defendant has effectively abandoned its business customers during one of the busiest and most productive sales periods of the year.

115. Defendant's grossly negligent and conscious disregard of its duty to protect its customers' Private Information and provide them with the ability to continue running their businesses effectively is the direct and proximate cause of the damages suffered by Plaintiffs and Class members, which damages will be determined at trial.

COUNT III
Negligent Misrepresentation
(On Behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

116. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

117. Rackspace, through its actions and advertisements, undertook to provide and did provide a platform for data storage and email services.

118. Rackspace provided false information in association with its ability to maintain the privacy and security of the Private Information Plaintiffs and Class members entrusted to it as part of their business relationship. Further, Rackspace knew or had reason to believe that its data and

network security practices, procedures, and protocols would not be able to prevent the Data Breach and resulting services outage.

119. Rackspace failed to use reasonable care and competence in obtaining and communicating information to its customers, including Plaintiffs and the Class, about its inadequate data and network security practices.

120. Rackspace had a direct pecuniary interest in its customers and/or users continuing to utilize its product for data storage and email communications without knowledge of Rackspace's faulty data and network security practices.

121. The information, including representations of Rackspace's enhanced data storage capabilities and commitment to maintaining the privacy of Plaintiffs' and Class members' Private Information was false.

122. The conduct of Defendant as set forth herein was a direct, proximate and/or contributing cause of the injuries suffered by Plaintiffs and the Class.

COUNT IV
Breach of Express Contract
(On Behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

123. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

124. Plaintiffs and other Class members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other Class members agreed to provide payment and their Private Information to Defendant, and Defendant agreed to (a) provide cloud storage and email services; (b) implement adequate data security practices, procedures, and protocols sufficient to prevent outages and provide Plaintiffs and Class members uninterrupted

access to their highly sensitive proprietary and other personal information; and (c) protect Plaintiffs and the Class members' Private Information from unauthorized access.

125. These contracts include the Privacy Notice on Defendant's website.

126. To the extent Defendant's obligation to protect Plaintiffs' and other Class members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class members' Private Information, including in accordance with federal, state and local laws, and industry standards. Plaintiffs and Class members would not have entrusted their Private Information to Defendant and entered into these contracts with Defendant without an understanding that their Private Information, including highly sensitive proprietary information, would not only be safeguarded and protected from unauthorized access, but that Plaintiffs and Class members would have uninterrupted access to it, as necessary. Nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures

127. A meeting of the minds occurred, as Plaintiffs and Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information and provide uninterrupted access to such Private Information so that Plaintiffs and Class members could continue to effectively run their businesses.

128. The protection of Plaintiffs' and Class members' Private Information and the provision of uninterrupted access to the highly sensitive Private Information stored on Defendant's network were material aspects of Plaintiffs' and Class members' contracts with Defendant.

129. Defendant's promises and representations described above relating to industry practices, and about Defendant's purported concern about their clients' privacy rights became terms of the contracts between Defendant and their clients, including Plaintiffs and Class members. Defendant breached these promises by failing to comply with federal law and reasonable industry practices.

130. Plaintiffs and Class members read, reviewed, and/or relied on statements made by or provided by Rackspace and/or otherwise understood that Rackspace would protect its Private Information if that information were provided to Rackspace.

131. Plaintiffs and Class members fully performed their obligations under these express contracts with Defendant; however, Defendant did not.

132. As a result of Defendant's breach of these terms, Plaintiffs and Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; not receiving the benefit of their bargain with Defendant; losing the difference in the value of the secure, uninterrupted access to their highly sensitive Private Information Defendant promised and the lack of network and data security that was actually received; and the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives and businesses, including, inter alia, the lost business opportunities resulting from the Data Breach.

133. Plaintiffs and Class members are therefore entitled to damages, including restitution, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT V
Breach of Implied Contract
(On Behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

134. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

135. Plaintiffs bring this breach of implied contract claim in the alternative to their breach of express contract claim.

136. Through their course of conduct, Defendant, Plaintiffs, and Class members entered into implied contracts for the provision of data security adequate to (a) provide Plaintiffs with access to their proprietary information without extended outages, and (b) safeguard and protect the privacy of such highly sensitive information.

137. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when they first entered purchased the product and accompanying services from Defendant.

138. These valid and enforceable implied contracts include Defendant's promise to protect nonpublic Private Information entrusted to Defendant.

139. When Plaintiffs and Class members provided their Private Information to Defendant in exchange for Defendant's product and services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

140. Defendant solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class members accepted Defendant's offers and provided their Private Information to Defendant to store on its network.

141. When entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

142. Class members who have paid money to Defendant reasonably believe and expect that Defendant will use part of those funds to obtain adequate data security. Defendant has failed to do so.

143. Under implied contracts, Defendant promised and was obligated to: (a) provide cloud storage and email services to Plaintiffs and Class members; (b) implement adequate data security practices, procedures, and protocols sufficient to prevent outages and provide Plaintiffs and Class members uninterrupted access to their highly sensitive proprietary and other personal information; and (c) protect Plaintiffs and the Class members' Private Information from unauthorized access. In exchange, Plaintiffs and members of the Class agreed to pay money for these services, and to turn over their Private Information to Defendant.

144. Both the provision of a product and its accompanying services and the protection of Plaintiffs and Class members' Private Information were material aspects of these implied contracts.

145. These implied contracts, which include the contractual obligations to maintain the privacy of Plaintiffs' and Class members' Private Information – are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

146. Defendant's express representations, including but not limited to the express representations found in its Privacy Notice, memorialize and embody the implied contractual

obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and protect the privacy of Plaintiffs and Class members' Private Information.

147. Plaintiffs and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information, including highly sensitive proprietary information, would not only be safeguarded and protected, but that Plaintiffs and Class members would have uninterrupted access to it, as necessary. Nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

148. A meeting of the minds occurred, as Plaintiffs and Class members agreed and provided their Private Information to Defendant and paid for, amongst other things, both the provision of the product and services and the protection of their Private Information.

149. Defendant materially breached its contractual obligations to provide uninterrupted access to the information it stored, and to protect the nonpublic Private Information it gathered when the outage occurred and the information was accessed and exfiltrated as a result of the Data Breach. Plaintiffs still do not have access to the highly sensitive information stored on Defendant's network.

150. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiffs' and Class members' Private Information as evidenced by its notifications of the Data Breach to the public, including Plaintiffs and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of

the FTCA, or otherwise protect Plaintiffs' and Class members' Private Information as set forth above.

151. The Data Breach and services outage were reasonably foreseeable consequences of Defendant's actions and inactions in breach of these implied contracts.

152. As a result of Defendant's failure to fulfill its data security protection and other obligations promised in these contracts, Plaintiffs and Class members did not receive full benefit of the bargain and, instead, received services that were of a diminished value to that described in the contracts. Plaintiffs and Class members therefore were damaged in an amount at least equal to the difference in the value of the services with data security protection and full access to their stored information (which services they bargained and paid for) and the services they actually received.

153. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard data security measures, neither the Plaintiffs, Class members, nor any reasonable person would have done business with Defendant.

154. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation, lost access and use of the Private Information impacted by the Data Breach, the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses and the loss of business opportunities, as well as the loss of the benefit of the bargain they struck with Defendant.

155. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

156. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT VI
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

157. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

158. In light of the special relationship between the parties, as alleged herein, Defendant has a duty of good faith and fair dealing with respect to its dealings with Plaintiffs. The implied covenant of good faith and fair dealing supplements the express and/or implied contractual terms between the parties to prevent a contracting party from engaging in conduct that frustrates the other party's rights to the benefits of the agreement. Thus, the implied covenant of good faith and fair dealing prevents either party from engaging in any action which would frustrate the other party's right to the benefit of the contract.

159. Plaintiffs complied with and performed all conditions of their contracts with Defendant. Defendant, however, breached the implied covenant of good faith and fair dealing by (a) failing to maintain adequate computer systems, networks, and data security practices sufficient to safeguard Plaintiffs' and Class members Private Information from unauthorized disclosure, (b) failing to timely and accurately disclose the Data Breach, (c) failing to timely resolve the outage of services resulting from the Data Breach, and (d) continuing to accept and store Plaintiffs' and Class members' Private Information after Defendant knew, or should have known, of the security vulnerabilities that were exploited in the Data Breach.

160. Defendant's bad-faith conduct described herein is a violation of its covenant of good faith and fair dealing in numerous respects, including but not limited to, Defendant having engaged in a course of conduct that is unreasonable, arbitrary, capricious, malicious, and oppressive, evidenced by Defendant's violations of the FTC Act and industry standards.

161. The effects of Defendant's violations have injured and destroyed Plaintiffs' rights to receive the benefit of the bargain as originally intended by the parties, thereby causing them injury in an amount to be fully determined at trial.

COUNT VII
Breach of Confidence
(On Behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

162. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

163. Plaintiffs and Class members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by Defendant and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

164. Defendant, in taking possession of this highly sensitive information, has a special relationship with its customers, including Plaintiffs and the Class. As a result of that special relationship, Defendant was provided with and stored private and valuable information belonging to Plaintiffs and the Class, which Defendant was required by law and industry standards to maintain in confidence.

165. Plaintiffs and the Class provided such information to Defendant under both the express and/or implied agreement of Defendant to limit and/or restrict completely the use and disclosure of such Private Information without Plaintiffs' and Class members' consent.

166. Defendant had a common law duty to maintain the confidentiality of Plaintiffs' and Class members' Private Information.

167. Defendant owed a duty to Plaintiffs and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

168. Plaintiffs and Class members have a privacy interest in their personal and proprietary matters and Defendant had a duty not to disclose such confidential information.

169. As a result of the parties' relationship of trust, Defendant had possession and knowledge of the confidential Private Information of Plaintiffs and Class members.

170. Plaintiffs' and Class members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiffs and Class members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

171. Defendant breached the duty of confidence it owed to Plaintiffs and Class members when Plaintiffs' and Class members' Private Information was disclosed to unknown criminal hackers by way of Defendant's own acts and omissions, as alleged herein.

172. Defendant breached its duties of confidence by failing to safeguard Plaintiffs' and Class members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement

information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) storing PII and other proprietary information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs and the Class members' Private Information to a criminal third party.

173. But for Defendant's wrongful breach of its confidence owed to Plaintiffs and Class members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

174. As a direct and proximate result of Defendant's breach of Plaintiffs' and Class members' confidence, Plaintiffs and Class members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality in their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their proprietary information and/or financial accounts; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts; the imminent and certainly impending injury flowing from the

increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and/or mental anguish accompanying the loss of confidences and disclosure of their confidential Private Information.

175. Additionally, Defendant received payments from Plaintiffs and Class members for the product and accompanying services with the understanding that Defendant would uphold its responsibilities to maintain the confidences of Plaintiffs' and Class members' Private Information.

176. Defendant breached the confidence of Plaintiffs and Class members when it made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendant to retain the benefits it has received at Plaintiffs' and Class members' expense.

177. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VIII
Arizona Consumer Fraud Act
(Ariz. Rev. Stat. Ann. §§ 44-1521, *et seq.*)
(On Behalf of Plaintiffs and the Arizona Subclass)

178. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

179. Plaintiffs bring this claim under the Arizona Consumer Fraud Act (the "CFA"), which makes it unlawful to commit "any deception, deceptive act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission[.]" Ariz. Rev. Stat. § 44-1522(A).

180. Plaintiffs and Defendant qualify as "persons" as contemplated by Section 44-1521(6) of the CFA.

181. As alleged herein, Defendant engaged in false, misleading, or deceptive acts or practices in the conduct of consumer transactions, in violation of the CFA, including but not limited to:

a. Representing that its product and accompanying services were of a particular standard or quality that it knew or should have known were of another;

b. Advertising goods or services with the intent not to sell them as advertised;

c. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Private Information, which was a direct and proximate cause of the Data Breach and services outage;

d. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach and services outage;

e. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45 and other statutory duties pertaining

to the security and privacy of Plaintiffs' and Class members' Private Information, which was a direct and proximate cause of the Data Breach and services outage;

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' Private Information, including by implementing and maintaining reasonable security measures;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45 and other statutory duties pertaining to the security and privacy of consumer data, which was a direct and proximate cause of the Data Breach.

182. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy and security of Defendant's network, the accessibility of the product and services being offered by Defendant, and Defendant's ability to protect the confidentiality of its customers' Private Information.

183. In addition, Defendant's failure to secure consumers' Private Information violated the FTCA (and other statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including duties also imposed by the FCRA, 15 U.S.C. § 1681e and the GLBA, 15 U.S.C. § 6801, *et seq*.) and therefore violates the CFA.

184. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiffs and Class members, deter hackers, detect a breach within a reasonable time, and prevent an extended outage, and that the risk of a data breach was highly likely.

185. The aforesaid conduct constitutes a violation of the CFA in that it is a restraint on trade or commerce.

186. These violations have caused financial injury to Plaintiffs and the Class.

187. Defendant's violations of the CFA have an impact of great and general importance on the public, including Arizonans. Many Arizona residents are customers of Rackspace, an appreciable number of whom have been impacted by the Data Breach.

188. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including economic damages, damages for mental anguish, treble damages for each act committed intentionally or knowingly, court costs, reasonably and necessary attorneys' fees, injunctive relief, and any other relief which the Court deems proper.

COUNT IX
Breach of Implied Warranty of Merchantability
(On behalf of the Nationwide Class or, alternatively, the Arizona Subclass)

189. Plaintiffs fully incorporate by reference all of the above paragraphs as though set fully set forth herein.

190. Defendant sold and maintained its hosted Exchange environment to Plaintiffs and the Class so as to provide continuous email and other services to Class members under implied warranties of merchantability and fitness. Defendant impliedly warranted the product to be merchantable, fit for the ordinary purposes for which it was intended to be used (including the guarantee that the product would provide a safe and non-defective condition relating to data

security, storage, and access, for use by their purchasers for the ordinary purpose for which they were intended and were not otherwise injurious).

191. Defendant is under a duty to design, manufacture, label, and test the product to make it suitable for the ordinary purposes of its use.

192. Defendant breached these implied warranties by failing to disclose that the product did, in fact, contain very serious data security inadequacies which led to the compromise of the security of the product and Plaintiffs' and Class members' Private Information stored therein, as set forth in detail herein. As a result of this breach of the express warranty, Plaintiffs and other consumers experienced an extended outage of services and the compromise of their Private Information and thus did not receive the product or services as warranted by Defendant.

193. Defendant has been on notice of these material omissions and/or misrepresentations through its own internal research and development process, and through the many data breaches similar to this one that have occurred within the cloud services and technology industry in recent years, as explained, *supra*. Defendant has had the opportunity to correct the misrepresentations pertaining to privacy and data security but has chosen not to do so. Moreover, Plaintiffs have sent a notice letter to Defendant seeking a remedy for the material omissions and/or misrepresentations alleged herein. Defendant has not yet remedied the harms and damages resulting from the omissions and/or misrepresentations.

194. As a direct and proximate result of Defendant's breach of the implied warranty of merchantability and fitness for a particular purpose, Plaintiffs and Class members did not receive the benefit of their bargains.

195. Plaintiffs and Class members are entitled to damages and other legal and equitable relief, including the purchase and ongoing payment price of the product, overpayment, and/or loss of the benefit of the bargain.

COUNT X
Breach of Express Warranty of Merchantability
(On behalf of the Nationwide Class or, alternatively, the Arizona Subclass)

196. Plaintiffs fully incorporate by reference all of the above paragraphs as though set forth herein.

197. Defendant extended, by way of product descriptions and representations as to the product's qualities and characteristics on its website and via Product advertisements, certain express warranties to Plaintiffs and Class members that the Product was safe to use and that such usage would not be disrupted for extended periods of time. These promises and representations became part of the basis of the bargain between the parties and, thus, constituted an express warranty.

198. Defendant sold the product and accompanying services, and Plaintiffs and Class members pay for the product and accompanying services, in reliance upon these representations and express warranties.

199. However, Defendant breached these express warranties in that the product did, in fact, contain very serious data security inadequacies which led to the compromise of the security of the product and Plaintiffs' and Class members' Private Information stored therein, as set forth in detail herein. As a result of this breach of the express warranty, Plaintiffs and other consumers experienced an extended outage of services and the compromise of their Private Information and thus did not receive the product or services as warranted by Defendant.

200. Defendant has been on notice of these material omissions and/or misrepresentations through its own internal research and development process, and through the many data breaches similar to this one that have occurred within the cloud services and technology industry in recent years, as explained, *supra*. Defendant has had the opportunity to correct the misrepresentations pertaining to privacy and data security but has chosen not to do so. Moreover, Plaintiffs have sent a notice letter to Defendant seeking a remedy for the material omissions and/or misrepresentations alleged herein. Defendant has not yet remedied the harms and damages resulting from the omissions and/or misrepresentations.

201. As a direct and proximate result of Defendant's breach of the express warranty of merchantability and fitness for a particular purpose, Plaintiffs and Class members did not receive the benefit of their bargains.

202. Plaintiffs and Class members are entitled to damages and other legal and equitable relief, including the purchase and ongoing payment price of the product, overpayment, and/or loss of the benefit of the bargain.

COUNT XI
Unjust Enrichment
(On behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

203. Plaintiffs fully incorporate by reference all of the above paragraphs as though set forth herein.

204. To the extent there is any determination made by the Court that Plaintiffs do not have standing to assert any contractual or warranty claims asserted against Defendant on the alleged basis of an absence of contractual privity or otherwise, this claim is asserted in the alternative.

205. By its wrongful acts and omissions described herein, including the sale of a product and services with numerous data security flaws that led to the outage and resulting Data Breach (without alerting purchasers, including Plaintiffs and the Class, to the existence of such flaws), Defendant was unjustly enriched at the expense of Plaintiffs and the Class.

206. Considering the very serious nature of the data security vulnerabilities of Defendant's systems and networks, which vulnerabilities were never revealed to Plaintiffs or Class members, Plaintiffs and Class members either (i) purchased a product and services they otherwise would not have purchased, or (ii) paid more for a product and services than they otherwise would have paid, and are thus left with a product and services of diminished value and utility because of the data security vulnerabilities such product and services contained at the time of purchase. Meanwhile, Defendant has sold more of the product and services than it otherwise would have and charged higher prices for such than it otherwise could have, thereby unjustly enriching itself.

207. Thus, Plaintiffs and the Class conferred benefits upon Defendant by paying for the product and services at their full price. Under the circumstances, it would be inequitable for Defendant to retain the profits, benefits, and other compensation obtained through its wrongful conduct in marketing and selling the product and services to Plaintiffs and Class members based on misrepresentations and/or omissions that the product was non-defective as it relates to data security practices, protocols, and procedures.

208. Plaintiffs and Class members are entitled to damages in the amount Defendant was unjustly enriched, to be determined at trial.

COUNT XII
Declaratory Relief
(On Behalf of the Nationwide Class or, Alternatively, the Arizona Subclass)

209. Plaintiffs fully incorporate by reference all of the above paragraphs as though fully set forth herein.

210. Under the Declaratory Judgment Act, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

211. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs and Class members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information and cause outages that restrict their use of Defendant's offered product and services. Plaintiffs and the Class remain at imminent risk that further outages and compromises of their Private Information will occur in the future.

212. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumer Private Information and avoid similar outages of services in the future.

213. Defendant still possesses the Private Information of Plaintiffs and the Class.

214. Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

215. Defendant has made no substantive announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

216. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Rackspace. The risk of another such breach is real, immediate, and substantial.

217. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Rackspace, Plaintiffs and Class members will likely continue to be subjected to more service outages, unauthorized disclosure of their Private Information, actual and/or substantial risk of fraudulent misuse of such Private Information, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

218. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Rackspace, thus eliminating the additional injuries that would result to Plaintiffs and Class members.

219. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Rackspace implement and maintain reasonable data security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Rackspace's systems on a periodic basis, and ordering Rackspace to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. conducting regular database scans and security checks; and

f. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to its inadequate networks and systems, lax data security practices, misuse and/or disclosure of Plaintiffs' and Class members' Private Information to unauthorized third parties, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety; to disclose

with specificity the type of PII compromised during the Data Breach; and to routinely and continually conduct training to inform internal security personnel how to prevent, identify, and contain a breach, and how to appropriately respond;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

F. For an award of punitive damages, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

Date: December 12, 2022

Respectfully submitted,

THE HERRERA LAW FIRM, INC.
1800 W. Commerce Street
San Antonio, Texas 78207
Telephone: (210) 224-1054
Facsimile: (210) 228-0887

BY: /s/ - JORGE A. HERRERA
JORGE A. HERRERA
State Bar No. 24044242
Email: *jherrera@herreralaw.com*
JAVIER L. HERRERA
State Bar No. 24075498
Email: *javier@herreralaw.com*
LAURA E. GUTIERREZ TAMEZ
State Bar No. 00793869
Email: *ltamez@herreralaw.com*
FRANK HERRERA, JR.
State Bar No. 09531000
Email: *fherrera@herreralaw.com*

JASON S. RATHOD*
jrathod@classlawdc.com
NICHOLAS A. MIGLIACCIO*
nmigliaccio@classlawdc.com
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

Robert Mackey, Esq.*
Law Offices of Robert Mackey
P.O. Box 279
Sewickley PA 15143
Tel: 412-370-9110
bobmackeyesq@aol.com

**Pro Hac Vice Applications Forthcoming*

Attorneys for Plaintiffs and the Putative Class

ClassAction.org