UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

GARRETT STEPHENSON, GATEWAY RECRUITING, LLC, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

RACKSPACE TECHNOLOGY, INC.,

Defendant.

Case No. 5:22-cv-01296

CLASS ACTION

COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **BREACH OF CONFIDENCE;**
3. **BREACH OF IMPLIED CONTRACT;**
4. **BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING;**
5. **DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT (TEXAS BUS. & COM. CODE §§ 17.41, *ET SEQ.)***

[JURY TRIAL DEMANDED]

Representative Plaintiffs allege as follows:

INTRODUCTION

1. Representative Plaintiffs Garrett Stephenson and Gateway Recruiting, LLC ("Representative Plaintiffs") bring this class action against Defendant Rackspace Technology, Inc. ("Defendant") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' personally identifiable information ("PII")[1] and/or other proprietary and/or highly confidential data (collectively, "Sensitive Data") stored within Defendant's information network, maintain its Hosted Exchange environment so as to provide continuous email service and/or notify Representative Plaintiffs and Class Members of outages so as to not unreasonably interfere with their access to their Sensitive Data.

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused, and will continue to cause, Representative Plaintiffs and thousands of others similarly situated persons in the massive and preventable security incident purportedly discovered by Defendant on or about December 2, 2022 (the "Security Incident").

3. Representative Plaintiffs further seek to hold Defendant responsible for not ensuring that its Hosted Exchange environment was maintained in a manner consistent with industry and other relevant standards.

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

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

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

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

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

9. According to statements made later that evening, Defendant again acknowledged that this "significant failure" in its environment was impacting its clients "greatly." At that time, it directed its clients' account administrators to "manually set up each individual user" on clients' accounts–actions which would require significant time and expense to those clients. During that recommended process, Defendant acknowledged that its clients would be "unable to connect to

the Hosted Exchange service to sync new email or send mail using [the] Hosted Exchange." Defendant further encouraged "admins to configure and set up their users accounts on Microsoft 365 so they can begin sending and receiving mail immediately."

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

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

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

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

14. Despite these obligations, Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently: failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' Sensitive Data was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, failing to prevent the unavailability of the Sensitive Data of Representative Plaintiffs and Class Members, disrupting Representative Plaintiffs' and Class Members' business operations, and failing to follow applicable, required and appropriate

protocols, policies and procedures regarding the protection of Sensitive Data. As a result, the Sensitive Data of Representative Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

15. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member is a citizen of a state different from Defendant.

16. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

17. Defendant is headquartered and routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

18. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiffs' claims took place within this District, and Defendant does business in this Judicial District.

PLAINTIFFS

19. Representative Plaintiff Garrett Stephenson is an adult individual and, at all relevant times herein, a resident and citizen of Texas. Representative Plaintiff Garrett Stephenson is a victim of the Security Incident.

20. Representative Plaintiff Gateway Recruiting, LLC is an executive recruiting firm and was, at all relevant times herein, based in New Braunfels, Texas. Representative Plaintiff Gateway Recruiting, LLC is a victim of the Security Incident. Representative Plaintiff Garrett Stephenson is the President of Gateway Recruiting, LLC.

21. Both Representative Plaintiffs contracted with Defendant to receive email hosting among other services.

22. Defendant received, stored and/or was provided access by Representative Plaintiffs of their Sensitive Data in connection with the support services it provides. As a result, Representative Plaintiffs' information was among the data accessed by an unauthorized third party and/or made unavailable during the Security Incident.

23. Representative Plaintiffs received services—and were "consumers" for purposes of obtaining services from Defendant within this state.

24. At all times herein relevant, Representative Plaintiffs are and were members of each of the Classes.

25. As required in order to obtain services from Defendant, Representative Plaintiffs and Class Members provided Defendant with Sensitive Data.

26. Representative Plaintiffs' and Class Members' Sensitive Data was exposed in the Security Incident because Defendant stored and/or shared their Sensitive Data. Their Sensitive Data was within the possession and control of Defendant at the time of the Security Incident.

27. As a result, Representative Plaintiffs and Class Members spent significant time and costs dealing with the consequences of the Security Incident, which included and continues to include, time spent verifying the legitimacy and impact of the Security Incident, discussing the incident with Defendant's representative(s), migrating Representative Plaintiffs' data (including the confidential information of their clients) to a new platform, exploring credit monitoring and identity theft insurance options, self-monitoring their accounts and seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Security Incident. This time has been lost forever and cannot be recaptured.

28. Representative Plaintiffs and Class Members suffered lost time, annoyance, interference, and inconvenience as a result of the Security Incident and have anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling their Sensitive Data.

29. Representative Plaintiffs and Class Members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Sensitive Data.

30. Representative Plaintiffs and Class Members have a continuing interest in ensuring that their Sensitive Data, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches. At present, Representative Plaintiffs and Class Members lack full access to substantial portions, if any, of their Sensitive Data, resulting in significant personal and business interruption/losses.

DEFENDANT

31. Defendant Rackspace Technology, Inc. has a principal place of business in San Antonio, Texas.

32. Launched in 1998, Rackspace touts itself as the "multicloud solutions experts" and a leading provider of expertise and managed services across all the major public and private cloud technologies, assisting business customers in over 120 countries.[2] Rackspace is the world's largest managed cloud provider, and provides access to such cloud offerings as Amazon Web Services, Microsoft Azure and OpenStack.

33. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when the identities become known.

[2] https://www.rackspace.com/about (last accessed December 4, 2022)

CLASS ACTION ALLEGATIONS

34. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves(s)/itself and the following classes:

> **Nationwide Class:**
> "All individuals within the United States of America whose PII and/or proprietary data was rendered unavailable and/or exposed to unauthorized third-parties as a result of the Data security incident announced on or about December 3, 2022."
>
> **Texas Subclass:**
> "All individuals within the State of Texas whose PII and/or proprietary data was rendered unavailable and/or exposed to unauthorized third-parties as a result of the Data security incident announced on or about December 3, 2022."

35. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

36. Also, in the alternative, Representative Plaintiffs request additional Subclasses as necessary based on the types of Sensitive Data that were compromised.

37. Representative Plaintiffs reserve the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

38. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is in the thousands of individuals. Membership in the classes will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Classes to exercise due care in collecting, storing, using and/or safeguarding their Sensitive Data;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Security Incident to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

6) Whether Defendant adequately, promptly, and accurately informed Representative Plaintiffs and Class Members that their Sensitive Data had been compromised;

7) How and when Defendant actually learned of the Security Incident;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Sensitive Data of Representative Plaintiffs and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Security Incident to occur;

10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Sensitive Data of Representative Plaintiffs and Class Members;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiff Classes. Representative Plaintiffs and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiffs in this class action are adequate representatives of each of the Plaintiff Classes in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

39. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes in their entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Classes in their entirety, not on facts or law applicable only to Representative Plaintiffs.

40. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Sensitive Data of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

41. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

The Security Incident

42. In the course of the Security Incident, one or more unauthorized persons and/or entities accessed Class Members' Sensitive Data. Representative Plaintiffs were among the individuals/entities whose data was accessed in the Security Incident.

43. As of the filing of this Complaint, Defendant had reported on its site, *inter alia*, the following announcements and disruption updates:

> **02:31 PM EST**
> **12/03/22**
> Our security and operations teams continue to work both internally and closely with outside experts to determine the full scope and impact of the issue involving our Hosted Exchange environment.
>
> Since our last update, we have assisted numerous customers to open replacement Microsoft 365 accounts so they can resume sending and receiving emails. This remains our topmost priority. Our support teams across the company continue working to assist customers in all hands-on deck effort during this time. We are working diligently to source additional resources to help our customers over the weekend. If you need assistance, please contact our support team via our usual support channels.
>
> Please continue to monitor our status page for the latest updates and FAQs: https://status.apps.rackspace.com/index/viewincidents?group=2.
>
> Again, thank you for your patience.

> **01:57 AM EST**
> **12/03/22**
> What happened?
>
> On Friday, Dec 2, 2022, we became aware of an issue impacting our Hosted Exchange environment. We proactively powered down and disconnected the Hosted Exchange environment while we triaged to understand the extent and the severity of the impact. After further analysis, we have determined that this is a security incident.
>
> The known impact is isolated to a portion of our Hosted Exchange platform. We are taking necessary actions to evaluate and protect our environments.
>
> Has my account been affected?
>
> We are working through the environment with our security teams and partners to determine the full scope and impact. We will keep customers updated as more information becomes available.
>
> Has there been an impact to the Rackspace Email platform?
>
> We have not experienced an impact to our Rackspace Email product line and platform.

At this time, Hosted Exchange accounts are impacted, and not Rackspace Email.

When will I be able to access my Hosted Exchange account?

We currently do not have an ETA for resolution. We are actively working with our support teams and anticipate our work may take several days. We will be providing information on this page as it becomes available, with updates at least every 12 hours.

As a result, we are encouraging admins to configure and set up their users accounts on Microsoft 365 so they can begin sending and receiving mail immediately. If you need assistance, please contact our support team. We are available to help you set it up.

Is there an alternative solution?

At no cost to you, we will be providing access to Microsoft Exchange Plan 1 licenses on Microsoft 365 until further notice.

To activate, please use the below link for instructions on how to set up your account and users.

https://docs.rackspace.com/support/how-to/how-to-set-up-O365-via-your-cloud-office-control-panel

Please note that your account administrator will need to manually set up each individual user on your account. Once your users have been set up and all appropriate DNS records are configured, their email access will be reactivated, and they will start receiving emails and can send emails. Please note, that DNS changes take approximately 30 minutes to provision and in rare cases can take up to 24 hours.

IMPORTANT: If you utilize a hybrid Hosted environment (Rackspace Email and Exchange on a single domain) then you will be required to move all mailboxes (Rackspace Email and Exchange) to M365 for mail flow to work properly. To preserve your data, it is critical that you do not delete your original mailboxes when making this change.

I don’t know how to setup Microsoft 365. How can I get help?

Please leverage our support channels by either joining us in chat or by calling +1 (855) 348-9064. (INTL: +44 (0) 203 917 4743).

Can I access my Hosted Exchange inbox from before the service was brought offline?

If you access your Hosted Exchange inbox via a local client application on your laptop or phone (like Outlook or Mail), your local device is likely configured to store your messages. However, while the Hosted Exchange environment is down, you will be unable to connect to the Hosted Exchange service to sync new mail or send mail using Hosted Exchange.

If you regularly access your inbox via Outlook Web Access (OWA), you will not have access to Hosted Exchange via OWA while the platform is offline.

As a result, we are encouraging admins to configure and set up their user’s accounts on Microsoft 365 so they can begin sending and receiving mail immediately. If you need assistance, please contact our support team. We are available to help you set it up.

Will I receive mail in Hosted Exchange sent to me during the time the service has been

shut down?

Possibly. We intend to update further as we get more information.

As a result, we are encouraging admins to configure and set up their user's accounts on Microsoft 365 so they can begin sending and receiving mail immediately. If you need assistance, please contact our support team. We are available to help you set it up.

08:19 PM EST
12/02/22
To our valued customers,

First and foremost, we appreciate your patience as we are working through the issue with your Hosted Exchange account, which we know impacted you greatly today. We experienced a significant failure in our Hosted Exchange environment. We proactively shut down the environment to avoid any further issues while we continue work to restore service. As we continue to work through the root cause of the issue, we have an alternate solution that will re-activate your ability to send and receive emails.

At no cost to you, we will be providing you access to Microsoft Exchange Plan 1 licenses on Microsoft 365 until further notice.

To activate, please use the below link for instructions on how to set up your account and users.

https://docs.rackspace.com/support/how-to/how-to-set-up-O365-via-your-cloud-office-control-panel

Please note that your account administrator will need to manually set up each individual user on your account. Once your users have been set up and all appropriate DNS records are configured, their email access will be reactivated, and they will start receiving emails and can send emails. Please note, that DNS changes take approximately 30 minutes to provision and in rare cases can take up to 24 hours.

IMPORTANT: If you utilize a hybrid Hosted environment (Rackspace Email and Exchange on a single domain) then you will be required to move all of your mailboxes (Rackspace Email and Exchange) to M365 in order for mail flow to work properly. To preserve your data, it is critical that you do not delete your original mailboxes when making this change.

Again, we apologize that this has been a major disruption to you, but we hope this will allow you to resume regular business as soon as possible.

Our support team is available to assist you via our usual support channels. Please reach out and continue to monitor our status page for further updates. Link to incident: https://status.apps.rackspace.com/index/viewincidents?group=2

Thanks again for your patience in this matter, we appreciate your business as a valued customer.

04:51 PM EST
12/02/22
To all of our valued customers, we understand the connectivity and login issues in our Cloud Office environments are greatly impacting you. We are working diligently to

resolve the issue and it is currently our highest priority. Please continue to monitor our status page for the latest updates. Again, thank you for your patience, as we work to provide you a resolution soon.

04:01 PM EST
12/02/22
We are aware of an issue impacting our Hosted Exchange environments. Our Engineering teams continue to work diligently to come to a resolution. At this time we are still in the investigation phase of this incident and will update our status page as more information becomes available.

01:54 PM EST
12/02/22
We are aware of an issue impacting our Hosted Exchange environments. Our Engineering teams continue to work diligently to come to a resolution. At this time we are still in the investigation phase of this incident and will update our status page as more information becomes available.

09:38 AM EST
12/02/22
All hands are on the deck & right resources have been engaged and are actively working on the issue. All new updates will be posted here as they become available.

06:36 AM EST
12/02/22
We continue to investigate the connectivity and login issues to our Exchange environments. Users may experience an error upon attempting to access OWA (Webmail) & sync mail to their email client, or a prompt to re-enter their password.

We will provide further information as this becomes available.

04:39 AM EST
12/02/22
We continue to investigate the connectivity issues to our Exchange environments. We will provide further updates as they become available.

04:32 AM EST
12/02/22
We continue to investigate the connectivity issues to our Exchange environments. We will provide further updates as they become available.

03:02 AM EST
12/02/22
We are investigating reports of connectivity issues to our Exchange environments. Users may experience an error upon accessing the Outlook Web App (Webmail) and syncing their email client(s).

We will provide further updates as they become available.

02:49 AM EST
12/02/22
We are investigating an issue that is affecting our Hosted Exchange environments. More details will be posted as they become available.

Defendant's Failed Response to the Security Incident

44. Upon information and belief, unauthorized persons and/or entities gained access to Representative Plaintiffs' and Class Members' Sensitive Data with the intent of engaging in misuse of the Sensitive Data, including potential marketing and selling Representative Plaintiffs' and Class Members' Sensitive Data.

45. Representative Plaintiffs and Class Members were required to provide their Sensitive Data to Defendant in order to receive email and/or other support services. As part of providing such services, Defendant created, collected, and stored Representative Plaintiffs' and Class Members' Sensitive Data with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

46. Despite this, Defendant failed to adequately inform Representative Plaintiffs and Class Members of the Security Incident properly, resorting to only subsequently providing opaque announcements as to this incident on its website and/or responding (albeit briefly and insufficiently) to Class Members' concerns if they affirmatively contacted Defendant. Further, despite their payments for secure and ongoing access to Representative Plaintiffs' and Class Members' Sensitive Data, Defendant permitted the Sensitive Data to become inaccessible for a prolonged period of time in what it has described as a "security incident," further exacerbating Representative Plaintiffs' and Class Members' concerns over the integrity of such information, and/or to make significant efforts and incur significant costs to protect that data and/or migrate their data to an altogether different email platform. Defendant has, heretofore, made no real effort, nor has it announced any intention, to reimburse Representative Plaintiffs or Class Members for the costs associated with migration of their Sensitive Data to these alternate email platforms. At present, Representative Plaintiffs and Class Members remain in the dark as to

whether their Sensitive Data will ever be fully accessible yet continue to pay Defendant for its services.

47. What's more, despite the foregoing, Representative Plaintiffs and Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their Sensitive Data going forward. Representative Plaintiffs and Class Members are, thus, left to speculate as to where their Sensitive Data ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Security Incident and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further incidents.

48. Representative Plaintiffs' and Class Members' Sensitive Data may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Sensitive Data for targeted marketing without the approval of Representative Plaintiffs and/or Class Members. Either way, unauthorized individuals can now easily access the Sensitive Data of Representative Plaintiffs and Class Members.

Defendant Collected/Stored Class Members' Sensitive Data

49. Defendant acquired, collected, and stored and assured reasonable security over Representative Plaintiffs' and Class Members' Sensitive Data.

50. As a condition of its relationships with Representative Plaintiffs and Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with their Sensitive Data. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Security Incident.

51. By obtaining, collecting, and storing Representative Plaintiffs' and Class Members' Sensitive Data, Defendant assumed legal and equitable duties and knew, or should have known, that they were thereafter responsible for protecting Representative Plaintiffs' and Class Members' Sensitive Data from unauthorized disclosure.

52. Representative Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Sensitive Data. Representative Plaintiffs and Class Members relied on Defendant to keep their Sensitive Data confidential and securely maintained, and to make only authorized disclosures of this information.

53. Defendant could have prevented the Security Incident, which began as early as December 2, 2022, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' Sensitive Data.

54. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' Sensitive Data is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

55. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated corporation with the resources to put adequate data security protocols in place.

56. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' Sensitive Data from being compromised.

Defendant Had an Obligation to Protect the Sensitive Data

57. Defendant's failure to adequately secure Representative Plaintiffs' and Class Members' Sensitive Data arises from statutory and common law.

58. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "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).

59. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Sensitive Data in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Representative Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Sensitive Data of Representative Plaintiffs and Class Members.

60. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the Sensitive Data in its possession was adequately secured and protected.

61. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Sensitive Data in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

62. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems and inform Representative Plaintiffs and Class Members thereof in a timely manner.

63. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

64. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Sensitive Data from theft because such an inadequacy would be a material fact in the decision to entrust this Sensitive Data to Defendant.

65. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

66. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' Sensitive Data and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

67. The type of Sensitive Data at issue in this litigation is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites.

68. The high value of Sensitive Data to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[3] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[4] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[5]

69. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

70. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying

---

[3] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[4] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[5] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

71. Identity thieves can use PII and financial information, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

72. The ramifications of Defendant's failure to keep secure Representative Plaintiffs' and Class Members' Sensitive Data are long lasting and severe. Once Sensitive Data is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the Sensitive Data of Representative Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the Sensitive Data for that purpose. The fraudulent activity resulting from the Security Incident may not come to light for years.

73. There may be a time lag between when harm occurs versus when it is discovered, and also between when Sensitive Data is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[6]

[6] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).

74. And data breaches are preventable.[7] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[8] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[9]

75. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs.[10]

76. Here, Defendant knew of the importance of safeguarding Sensitive Data and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' Sensitive Data was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

77. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' Sensitive Data, (iii) failing to take standard and reasonably available steps to prevent the Security Incident, (iv) concealing the existence and extent of the Security Incident for an unreasonable

---

[7] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[8] *Id.* at 17.
[9] *Id.* at 28.
[10] *Id.*

duration of time and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Security Incident.

Representative Plaintiffs' Notice and Response to the Security Incident

78. At approximately 3:00 AM (CT) on December 3, 2022, Representative Plaintiff Stephenson observed that no emails were arriving on his Defendant-hosted email account(s). Though a series of steps to troubleshoot the situation, Representative Plaintiff Stephenson first changed his password, to no avail. Upon reviewing the status of the Rackspace server, Representative Plaintiff Stephenson noted that the Hosted Exchange was off-line, with no other provided updates other than that the Exchange was having issues.

79. At approximately 3:30 AM (CT) and, again, at 4:00 AM (CT) on December 3, 2022, Representative Plaintiff Stephenson telephoned, reached and spoke to a representative of Defendant. During the second contact at 4:00 AM (CT), Defendant's representative told Representative Plaintiff Stephenson that Defendant had suffered a security "breach" and that no other notice (beyond the website information) had been made available about it to the public.

80. Thereafter, Representative Plaintiff Stephenson tried again reach a support representative but has been unsuccessful since Defendant's technical support telephone number simply rings for hours and Defendant has shut down its support chat feature.

81. As additional interim steps, Representative Plaintiff Stephenson, so as to maintain operability of co-Representative Plaintiff Gateway Recruiting, LLC, for his/its own benefit, and for the benefit of his/their numerous clients (not to mention so as to maintain the confidential nature of these Representative Plaintiffs' and their clients' Sensitive Data), spent considerable time (i.e., no less than 30 hours) responding to the Security Incident. These steps included calling employees and asking them to come into the office so as to proactively back up what data existed on their local machines, advising them to change all passwords, moving to a Microsoft 365 hosting solution, repointing the company's domain away from Rackspace to Microsoft, etc. Indeed, the cost (employee time, loss of data, etc.) was extraordinary and the incurrence of such and other costs will continue as Representative Plaintiffs continue to discover the full scope of

the loss/inaccessible data. At present, it appears that years of data (and associated work to accumulate it) has been lost.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class and the Texas Subclass)

82. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein

83. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their Sensitive Data and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the Sensitive Data of Representative Plaintiffs and Class Members in its computer systems and on its networks.

84. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Sensitive Data in its possession;

b. to protect Representative Plaintiffs' and Class Members' Sensitive Data using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Security Incident and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiffs and Class Members of any security incident, or intrusion that affected, or may have affected, their Sensitive Data.

85. Defendant knew that the Sensitive Data was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

86. Defendant knew, or should have known, of the risks inherent in collecting and storing Sensitive Data, the vulnerabilities of its data security systems, and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

87. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' Sensitive Data.

88. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the Sensitive Data that Representative Plaintiffs and Class Members had entrusted to it.

89. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Sensitive Data of Representative Plaintiffs and Class Members.

90. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the Sensitive Data contained therein.

91. Representative Plaintiff(s)' and Class Members' willingness to entrust Defendant with their Sensitive Data was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the Sensitive Data it stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

92. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' Sensitive Data and promptly notify them about the Security Incident. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or the remaining Class Members.

93. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Sensitive Data of Representative Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Representative Plaintiff(s)' and Class Members' Sensitive Data had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the Sensitive Data by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Sensitive Data;

d. by failing to provide adequate supervision and oversight of the Sensitive Data with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Sensitive Data of Representative Plaintiffs and Class Members, misuse the Sensitive Data and intentionally disclose it to others without consent;

e. by failing to adequately train its employees to not store Sensitive Data longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff(s)' and the Class Members' Sensitive Data;

g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. by failing to encrypt Representative Plaintiffs' and Class Members' Sensitive Data and monitor user behavior and activity in order to identify possible threats.

94. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

95. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

96. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Sensitive Data to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their Sensitive Data.

97. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by unreasonably waiting after learning of the Security Incident to notify Representative Plaintiffs and Class Members (if and when it notified them at all) and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

98. By notifying Representative Plaintiffs and Class Members that the disruption of service was a "security incident," and offering little more, Representative Plaintiffs and Class Members reasonably elected to treat the incident as a data breach, such that they took steps to change passwords, notify clients and/or otherwise took steps to protect the integrity of their Sensitive Data. These steps required Representative Plaintiffs and Class Members to incur significant costs and time.

99. Further, through its failure to provide timely and clear notification (if any notification at all) of the Security Incident to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking all available meaningful and proactive steps to secure their Sensitive Data.

100. There is a close causal connection between Defendant's failure to implement security measures to protect the Sensitive Data of Representative Plaintiffs and Class Members and the harm suffered, or risk of imminent harm suffered by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' Sensitive Data was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Sensitive Data by adopting, implementing, and maintaining appropriate security measures.

101. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

102. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will suffer, were and are the direct and proximate result of Defendant's grossly negligent conduct.

103. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and financial information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

104. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect Sensitive Data and not complying with applicable industry standards, as described in

detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Data it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

105. Defendant had a further duty to employ reasonable security measures and otherwise protect the Sensitive Data of Representative Plaintiffs and Class Members pursuant to Texas law.

106. Defendant, through its actions and/or omissions, unlawfully breached its duty to Representative Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Representative Plaintiffs' and Class Members' Private Information within Defendant's possession.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to Representative Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Representative Plaintiffs' and Class Members' Sensitive Data.

108. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Representative Plaintiffs and Class Members that the Sensitive Data within Defendant's possession might have been compromised and precisely the type of information compromised.

109. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their Sensitive Data is used, (iii) the compromise, publication, and/or theft of their Sensitive Data, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Sensitive Data, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Security Incident, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their Sensitive Data, which may remain in Defendant's possession and is subject to further

unauthorized disclosures, so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' Sensitive Data in its continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Data compromised as a result of the Security Incident for the remainder of the lives and/or business operations of Representative Plaintiffs and Class Members.

110. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

111. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Sensitive Data, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Data in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Confidence
(On behalf of the Nationwide Class and the Texas Subclass)

112. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth therein.

113. At all times during Representative Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the Sensitive Data that Representative Plaintiffs and Class Members provided it.

114. As alleged herein and above, Defendant's relationship with Representative Plaintiffs and the Class Members was governed by promises and expectations that Representative Plaintiffs and Class Members' Sensitive Data would be collected, stored, and protected in confidence, and would not be 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.

115. Representative Plaintiffs and Class Members provided their respective Sensitive Data to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Sensitive Data to be 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.

116. Representative Plaintiffs and Class Members also provided their Sensitive Data to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their Sensitive Data from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

117. Defendant voluntarily received, in confidence, Representative Plaintiffs' and Class Members' Sensitive Data with the understanding that the Sensitive Data would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by the public or any unauthorized third parties.

118. Due to Defendant's failure to prevent, detect, and avoid the Security Incident from occurring by, *inter alia*, not following best information security practices to secure Representative Plaintiffs' and Class Members' Sensitive Data, Representative Plaintiffs' and Class Members' Sensitive Data was 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 beyond Representative Plaintiffs' and Class Members' confidence, and without its express permission.

119. As a direct and proximate cause of Defendant's actions and/or omissions, Representative Plaintiffs and Class Members have suffered damages, as alleged herein.

120. But for Defendant's failure to maintain and protect Representative Plaintiffs' and Class Members' Sensitive Data in violation of the parties' understanding of confidence, their Sensitive Data 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. The Security Incident was the direct and legal cause of the misuse of Representative Plaintiffs' and Class Members' Sensitive Data, as well as the resulting damages.

121. The injury and harm Representative Plaintiffs and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Representative Plaintiffs' and Class Members' Sensitive Data. Defendant knew its data systems and protocols for accepting and securing Representative Plaintiffs' and Class Members' Sensitive Data had security and other vulnerabilities that placed Representative Plaintiffs' and Class Members' Sensitive Data in jeopardy.

122. As a direct and proximate result of Defendant's breaches of confidence, Representative Plaintiffs and Class Members have suffered and will suffer injury, as alleged herein, including, but not limited to, (a) actual identity theft, (b) the compromise, publication, and/or theft of their Sensitive Data, (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Data, (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Security Incident, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft, (e) the continued risk to their Sensitive Data, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' Sensitive Data in its continued possession, (f) future costs in terms of time, effort, and money that will be expended as result of the Security Incident for the remainder of the lives and/or business operations of Representative Plaintiffs and Class Members, (g) the diminished value of Representative Plaintiffs' and Class Members' Sensitive Data and (h) the diminished value of Defendant's services for which Representative Plaintiffs and Class Members paid and received.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Nationwide Class and the Texas Subclass)

123. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth therein.

124. Through its course of conduct, Defendant, Representative Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' Sensitive Data.

125. Defendant required Representative Plaintiffs and Class Members to provide and entrust their Sensitive Data as a condition of obtaining Defendant's services.

126. Defendant solicited and invited Representative Plaintiffs and Class Members to provide their Sensitive Data as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers and provided their Sensitive Data to Defendant.

127. As a condition of being direct customers/employees of Defendant, Representative Plaintiffs and Class Members provided and entrusted their Sensitive Data to Defendant. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Representative Plaintiffs and Class Members if their data had been breached and compromised or stolen.

128. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide their Sensitive Data to Defendant, in exchange for, amongst other things, the protection of their Sensitive Data.

129. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

130. Defendant breached the implied contracts it made with Representative Plaintiffs and Class Members by failing to safeguard and protect their Sensitive Data and by failing to

provide timely and accurate notice to them that their Sensitive Data was compromised as a result of the Security Incident.

131. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (c) loss of the confidentiality of the stolen confidential data, (d) the illegal sale of the compromised data on the dark web, (e) lost work time and (f) other economic and non-economic harm.

FOURTH CLAIM FOR RELIEF
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class and the Texas Subclass)

132. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth therein.

133. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

134. Representative Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

135. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Sensitive Data, failing to timely and accurately disclose the Security Incident to Representative Plaintiffs and Class Members and continued acceptance of Sensitive Data and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Security Incident.

136. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

FIFTH CLAIM FOR RELIEF
Deceptive Trade Practices—Consumer Protection Act
(Texas Bus. & Com. Code §§ 17.41, *et seq.*
(On behalf of the Texas Subclass)

137. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth therein.

138. Representative Plaintiffs bring this claim under the Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), which makes it unlawful to commit "[f]alse, misleading, or deceptive acts or practices in the conduct of any trade or commerce." Tex. Bus. & Com. Code § 17.46.

139. Defendant is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

140. Representative Plaintiffs and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

141. Defendant advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

142. Defendant engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

143. Defendant's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Representative Plaintiffs and Texas Subclass members' Sensitive Data, which was a direct and proximate cause of the Security Incident;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Security Incident;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiffs and Texas Subclass

members' Sensitive Data, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Security Incident;

d. Misrepresenting that it would protect the privacy and confidentiality of Representative Plaintiffs and Texas Subclass members' Sensitive Data, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Representative Plaintiffs and Texas Subclass members' Sensitive Data, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq*., and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Representative Plaintiffs and Texas Subclass members' Sensitive Data; and

g. 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 Representative Plaintiffs and Texas Subclass members' Sensitive Data, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

144. Defendant intended to mislead Representative Plaintiffs and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

145. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data/network security and ability to protect the confidentiality of consumers' Sensitive Data.

146. Had Defendant disclosed to Representative Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as a responsible company that could be trusted with valuable Sensitive Data regarding thousands of consumers, including Representative Plaintiffs and the Texas Subclass. Defendant accepted the responsibility of being a steward of that Sensitive Data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself out as such, Representative

Plaintiffs and the Texas Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

147. Defendant had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the Sensitive Data in its possession, and the generally accepted professional standards in its industry.

148. Defendant engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendant engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

149. Consumers, including Representative Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in Defendant's data security because this information was known exclusively by Defendant. Consumers also lacked the ability, experience, or capacity to secure the Sensitive Data in Defendant's possession or to fully protect their interests with regard to their data. Representative Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to Defendant's systems in order to evaluate its security controls. Defendant took advantage of its special skill and access to Sensitive Data to hide its inability to protect the security and confidentiality of Representative Plaintiffs and Texas Subclass members' Sensitive Data.

150. Defendant intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Defendant's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Security Incident, which resulted from Defendant's unconscionable business acts and practices, exposed Representative Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their Sensitive Data and the security of their identities, financial information or PII, and worked a substantial hardship on a significant and unprecedented number of consumers. Representative Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the Security Incident.

151. Defendant acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Representative Plaintiffs and Texas Subclass members' rights.

152. As a direct and proximate result of Defendant's unconscionable and deceptive acts or practices, Representative Plaintiffs and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Data. Defendant's unconscionable and deceptive acts or practices were a producing cause of Representative Plaintiffs' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

153. Defendant's violations present a continuing risk to Representative Plaintiffs and Texas Subclass members as well as to the general public.

154. Representative Plaintiffs and the Texas Subclass 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.

JURY DEMAND

155. Representative Plaintiffs, individually, and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demand a trial by jury for all issues triable by jury.

PRAYER

WHEREFORE, Representative Plaintiffs, on behalf of himself/themselves and each member of the proposed National Class and the Texas Subclass, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' Sensitive Data, and from refusing to issue prompt, complete, and accurate disclosures to Representative Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge the Sensitive Data of Representative Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' Sensitive Data;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' Sensitive Data on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Sensitive Data, as well as protecting the Sensitive Data of Representative Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings, and determinations identified and sought herein.

Respectfully submitted,

/s/ Scott Edward Cole

Scott Edward Cole, Esq. (CA S.B. #160744)
(*pro hac vice* forthcoming)
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, California 94607
510.891.9800 / 510.891.7030 (fax)
sec@colevannote.com

Ronald W. Armstrong, II, Esq. (S.B. #24059394)
THE ARMSTRONG FIRM, PLLC
310 S. Saint Mary's, Suite 2700
San Antonio, Texas 78205
210.277.0542 / 210.277.0548 (fax)
rwaii@tafpllc.com

Attorneys for Representative Plaintiffs
and the Plaintiff Class(es)