UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 19-cv-61350-ALTMAN/HUNT

In re: Citrix Data Breach Litigation

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Lee Milligan, on behalf of himself and his minor son, Lindsey Howard, Kristi Jackson, Michelle Ramus, Charles Ramus, Brandon Sargent, and Natalie Young (collectively "Plaintiffs"), individually and on behalf of all persons similarly situated (the "Class" or "Class members"), bring this Consolidated Class Action Complaint against Defendant Citrix Systems, Inc. ("Defendant" or "Citrix"), based upon personal knowledge with respect to themselves, and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE CASE

1. Citrix is a global technology provider of virtualization services, including server and desktop virtualization, networking, software-as-a-service and cloud technologies. Roughly 400,000 organizations nationwide use Citrix's services, including the U.S. Department of Defense. In 2018, Citrix reported net revenues of nearly $3 billion.

2. On March 8, 2019, Citrix disclosed that hackers gained access to its internal networks. At that time, Citrix stated only that "it appears that the hackers may have accessed and downloaded business documents. The specific documents that may have been accessed, however, are currently unknown." Citrix was reportedly completely unaware of the attack until March 6, 2019, when the FBI informed it that up to 10 terabytes of its data had been stolen.

3. In April 2019, Citrix acknowledged that the hackers "removed information relating to certain individuals who are current and former employees, as well as certain beneficiaries and dependents. Beginning on October 13, 2018 and continuing through March 8, 2019, hackers exploited glaring vulnerabilities in the Citrix's network to steal valuable employee data. This information may have included, for example, names, Social Security numbers, and financial information" (the "Data Breach").

4. As a matter of course, and on an ongoing basis, Citrix collected its employees' sensitive personal and financial information, including names, addresses, Social Security numbers, bank account numbers, and other personal and financial information ("Personal Information") as a condition of their employment. Accordingly, Citrix had an obligation to secure that information by implementing reasonable and appropriate safeguards compliant with industry-standard data security practices.

5. Citrix has now acknowledged that hackers were able to access its networks using a basic and well-known technique known as "password spraying" that exploits weak passwords. Citrix's failure to implement and maintain reasonable safeguards to protect against these types of attacks was and is contrary to the representations made in its employee handbook and its express and implied agreements with its employees. In addition to Citrix's failure to prevent the Data Breach, Citrix also failed to detect the breach, allowing hackers to access its networks and exfiltrate data over a period of more than four months.

6. As a result of Citrix's failure to protect the information with which it was entrusted to safeguard, Plaintiffs and Class members have already suffered harm and have been exposed to a significant risk of identity theft, financial fraud, and other identity-related fraud for years to come.

JURISDICTION AND VENUE

7. This Consolidated Complaint is intended to serve as a superseding complaint as to all other complaints consolidated in this litigation, and to serve for all purposes as the operative pleading for the Classes defined below. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from Citrix. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

8. This Court has jurisdiction over Citrix as maintains its corporate headquarters in this District. Defendant is authorized to and conducts business in this District and is subject to general personal jurisdiction in this state.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, Citrix maintains its headquarters within this District, and Citrix has caused harm to Class members residing in this District.

PARTIES

10. Defendant Citrix Systems, Inc. is a Delaware corporation with its principal place of business located in Ft. Lauderdale, Florida.

11. Plaintiff Lee Milligan and his minor son are residents and citizens of Cumming, Georgia. Plaintiff Milligan is a former employee of Citrix.

12. Plaintiff Lindsey Howard is a resident and citizen of Coral Springs, Florida, and former employee of Citrix.

13. Plaintiff Kristi Jackson is a resident and citizen of Florida, and former employee of Citrix.

14. Plaintiff Michelle Ramus is a resident and citizen of Tampa, Florida, and former employee of Citrix.

15. Plaintiff Charles Ramus is a resident and citizen of Tampa, Florida and was listed in Michelle Ramus's employment records as her beneficiary.

16. Plaintiff Brandon Sargent is a resident and citizen of Goldsboro, North Carolina, and former employee of Citrix.

17. Plaintiff Natalie Young is a resident and citizen of Parkland, Florida, and former employee of Citrix.

STATEMENT OF FACTS

A. Citrix Knew it was a Target of Cyber-Threats

18. Citrix is a major technology company specializing in "delivering digital workspace, networking, and analytics solutions that help customers drive innovation and be productive anytime, anywhere."[1] Citrix employed 8,200 employees as of the end of 2018.

19. Citrix represents that "more than 100 million users across 400,000 organizations – including 99% of the Fortune 500 – trust Citrix to power a better way to work."[2] Chief amongst its most well-known products and services is its Virtual Desktop solutions, which allows users to remotely access their desktops and applications from anywhere. Citrix's holdings include its

[1] Citrix Systems, Inc., 2018 Form 10-K ("Citrix 2018 Form 10-K"), https://d18rn0p25nwr6d.cloudfront.net/CIK-0000877890/5a296e8b-c25a-4a37-a5df-ceb29faed950.pdf (last visited July 26, 2019).

[2] Citrix, *About Us*, https://www.citrix.com/about/ (last visited July 26, 2019).

wholly-owned "GoTo family of service offerings" consisting of GoToMeeting, GoToWebinar, GoToTraining, GoToMyPC, GoToAssist, Grasshopper and OpenVoice.[3]

20. Consistent with its position at the vanguard of technology companies, Citrix is well aware of the risks associated with failing to protect its information systems and the Personal Information contained therein. Specifically, Citrix's public filings state:

> ***Actual or perceived security vulnerabilities in our solutions and services or cyberattacks on our networks could have a material adverse impact on our business, results of operations and financial condition***.
>
> Use of our solutions and services may involve the transmission and/or storage of data, including in certain instances customers' business, financial and personal data. Thus, **maintaining the security of our solutions, computer networks and data storage resources is important as security breaches could result in solution or service vulnerabilities and loss of and/or unauthorized access to confidential information**. We aim to engineer secure solutions and services, enhance security and reliability features in our solutions and services, deploy security updates to address security vulnerabilities and seek to respond to known security incidents in sufficient time to minimize any potential adverse impact. We have in the past, and may in the future, discover vulnerabilities in our solutions or underlying technology, which could expose our operations and our customers to risk until such vulnerabilities are addressed. In addition, to the extent we are diverting our resources to address and mitigate these vulnerabilities, it may hinder our ability to deliver and support our solutions and customers in a timely manner.
>
> As a more general matter, **unauthorized parties may attempt to misappropriate or compromise our confidential information or that of third parties, create system disruptions, product or service vulnerabilities or cause shutdowns**. These perpetrators of cyberattacks also may be able to develop and deploy viruses, worms, malware and other malicious software programs that directly or indirectly attack our products, services or infrastructure (including third party cloud service providers – such as Microsoft Azure and Amazon Web Services and Google Cloud Platform – upon which we rely).

Citrix 2018 Form 10-K at 15 (second and third emphasis added).

36. Citrix was further aware of its need to attract and retain talented employees:

> Our success depends, in large part, on our ability to attract, engage, retain, and integrate qualified executives and other key employees throughout all areas of our

[3] Citrix 2018 Form 10-K at 3.

> business. Identifying, developing internally or hiring externally, training and retaining highly-skilled managerial, technical, sales and services, finance and marketing personnel are critical to our future, and competition for experienced employees can be intense.
>
> ***
>
> Competition for qualified personnel in our industry is intense because of the limited number of people available with the necessary technical skills and understanding of solutions in our industry. The loss of services of any key personnel, the inability to retain and attract qualified personnel in the future or delays in hiring may harm our business and results of operations.

Citrix 2018 Form 10-K at 14-15.

37. Citrix also maintains a "Code of Business Conduct" which "sets out Citrix's expectations for the Citrix community (including its employees, directors, partners, suppliers and contractors)."[4] Under the heading "Protect Personal Information," Citrix directs its community to: "Always protect the privacy of our employees, customers, and partners."[5]

38. Moreover, Citrix directs its community to: "Handle personal information in a manner that will avoid accidental loss or alteration or unauthorized access" and "[n]ever disclose personal information to anyone outside of Citrix without specific authorization from your manager and the local Legal representative in your region."[6]

39. Citrix knew that it could not retain and attract qualified employees if it did not adequately invest in data security and adopt measures to protect their Personal Information. But despite recognizing these information security risks, and acknowledging its crucial need to attract and retain qualified employees, Citrix failed to take necessary precautions to ensure their Personal Information was secure.

---

[4] Citrix Code of Business Conduct June 2018, at 3, https://www.citrix.com/content/dam/citrix/en_us/documents/about/code-of-business-conduct.pdf (last visited July 26, 2019).

[5] *Id.* at 13.

[6] *Id.*

40. At all relevant times, Citrix was aware, or should have been aware, that the Personal Information it collected, maintained and stored in its systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud. Indeed, Citrix observed frequent public announcements of employee-related data breaches affecting technology companies, healthcare companies, retailers, and restaurant chains, and knew that personal and financial information of the type stored by Citrix is highly coveted and a frequent target of hackers.

41. In fact, in the years prior to the Data Breach, Citrix itself has been a frequent target of hackers across the globe. For example, in October 2015, an "altruistic" Russian hacker known as "w0rm" – who is infamous for attacks on a number of high profile targets including CNET, Adobe, and Bank of America – stated in a blog post that he was able to gain access to Citrix's content management system via an insecure password. From there, w0rm "was able to exploit a series of security holes to gain access to the company's administrative system including the remote assistance system."[7]

42. Cyberint, a cyber-security intelligence company based in Israel, said it identified the hack in October 2015 and promptly tried to notify Citrix. According to Elad Ben-Meir, vice president of marketing at Cyberint, the company made repeated efforts to notify Citrix, but received no response. In addition, the hacker w0rm tweeted Citrix with a link to its blog posting on October 25, 2015, and said it received no response.[8]

43. According to Ben-Meir, an analysis of w0rm's attack showed that it had gained access to all of Citrix's customers through the administrative system. This would have enabled

[7] *See* Tom Reeve, *I hacked Citrix, says Russian hacker w0rm*, SC Magazine UK (Jan. 11, 2016), https://www.scmagazineuk.com/i-hacked-citrix-says-russian-hacker-w0rm/article/1477764 (last visited July 26, 2019).

[8] *Id.*

an attacker potentially to bypass customers' security systems and upload malware undetected. "Citrix offer[s] a platform for remote assistance – [w0rm] could if he wanted to – but he didn't actually use it, but if he wanted to he could penetrate every endpoint of Citrix customers out there," said Ben-Meir. "Essentially if he had wanted to, he could have put malware into every end user of every Citrix customer which then would allow it to either keylog the things the people type, he could steal sensitive information from those end points, or he could use those endpoints as a botnet to run DDos attacks. A hacker that gains access to that amount of PCs is basically really powerful."[9]

44. The hacker told media outlets that its goals were actually altruistic, and that the hack was driven by a desire to upgrade internet security: "By targeting high-profile sites, the group says it can raise awareness about security flaws."[10]

45. In response to the report, Citrix's Chief Security Officer, Stan Black, issued a statement acknowledging that while Citrix's content management system was accessed, the "server under question did not contain any customer, employee or other sensitive or confidential information."[11] The statement further noted that "**we have no evidence that this threat actor has accessed systems other than the single content management server.** We will continue to monitor the environment for unauthorized access and changes."[12]

---

[9] *Id.*

[10] Alasdair Gilchrist, *W0rm hackers hit Citrix in show of power*, ITProPortal (Jan. 12, 2016), https://www.itproportal.com/2016/01/12/w0rm-hackers-hit-citrix-show-power/ (last visited July 26, 2019).

[11] Stan Black, *No Access to Sensitive Info; No Broad Network Access*, Citrix.com (Jan. 18, 2016), https://www.citrix.com/blogs/2016/01/12/no-access-to-sensitive-info-no-broad-network-access-4/ (last visited July 26, 2019).

[12] *Id.* (emphasis in original).

46. The 2015 hack by w0rm is not the only breach Citrix has experienced in recent years. In June 2016, GoToMyPC, a popular remote desktop software owned by Citrix, required all users to reset their passwords after disclosing it was "targeted by a very sophisticated password attack." A Citrix representative stated at the time that "the recent incident was a password re-use attack, where attackers used usernames and passwords leaked from other websites to access the accounts of GoToMyPC users. At this time, the response includes a mandatory password reset for all GoToMyPC users. Citrix encourages customers to visit the GoToMyPC status page to learn about enabling two-step verification, and to use strong passwords in order to keep accounts as safe as possible."[13]

47. In December 2018, Citrix forced a password reset for users of its secure file sharing and transfer service known as Sharefile. In response to questions by security industry personnel as to the reasons for the password reset, Citrix spokesperson Jamie Buranich claimed, "This is not in response to a breach of Citrix products or services." But at the time this statement was made, hackers had *already* gained access to Citrix's networks.

48. Also in December 2018, Citrix published a blog post touting the importance of data security in a world that has a "staggering" number of data breaches:

> 2018 has seen an unprecedented number of records breached by hackers. According to the Breach Level Index, in just the first half of 2018, more records were compromised than in all of 2017. The number of records compromised in 2018 is in the multi billions. It's staggering.
>
> With the credentials harvested from these attacks, and the bad guys knowing that people will use the same password for multiple systems and websites, "credential stuffing" – a type of cyber-attack where stolen emails and passwords obtained through these types of breaches are used to try and gain unauthorized access to other systems – has become a serious threat facing businesses and individuals.

[13] Brian Krebs, *Citing Attack, GoToMyPC Resets All Passwords*, KrebsOnSecurity (June 20, 2016), https://krebsonsecurity.com/2016/06/citing-attack-gotomypc-resets-all-passwords/ (last visited July 26, 2019).

> Late last week, not long after new high profile security breaches were revealed, in the course of our ongoing security monitoring, we saw incidences in ShareFile that had some of the characteristics of credential stuffing. After further analysis, we became very concerned that indeed perpetrators were using credentials obtained from breaches unrelated to ShareFile to attempt to gain access to individual accounts.
>
> We made an immediate decision to limit the risk to our ShareFile customers by forcing a password reset. We knew the timing over the weekend was not ideal, but felt it far more important to help our customers by fundamentally stopping the credential stuffing effort. We acknowledge it has been inconvenient to customers, and regret the inconvenience, but we were acting in our customers' best interests. It was the most expeditious way to end the attack, and proactively help our customer protect their data.[14]

49. Yet, despite Citrix's stated desire to protect its *customer* information and its knowledge of what it called "unprecedented data breaches," Citrix failed to implement reasonable safeguards to protect its own *employees*' information stored by the company.

50. As Citrix acknowledges, the rise in the number of data breaches is attributable to the fact that information of the type exposed in the Data Breach is highly-coveted and valuable on underground markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web" – exposing impacted individuals to identity theft and fraud for years to come.

51. Legitimate organizations and the criminal underground alike recognize the value of personal information contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. At all relevant times, Citrix knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable

[14] Stan Black, *Citrix forces password reset to protect against credential stuffing*, Citrix.com (Dec. 7, 2018), https://www.citrix.com/blogs/2018/12/04/citrix-forces-password-reset-to-protect-against-credential-stuffing/ (last visited July 26, 2019).

consequences of a breach of its data security system, including, specifically, the significant costs that would be imposed on its employees as a result of a breach.

52. In this case, Citrix was at all times fully aware of its obligation to protect the Personal Information of its employees. Citrix was also aware of the significant repercussions if it failed to do so because Citrix collected data from thousands of employees and knew that this data, if compromised, would result in injury to its employees and their beneficiaries and dependents. Unfortunately, despite its recognition of the risks of inadequate data security practices, Citrix failed to adopt reasonable safeguards to protect against known and obvious cyber-threats.

B. The Data Breach and Password Spraying

53. In its March 8, 2019, public announcement, Citrix disclosed that it had been contacted by the Federal Bureau of Investigation ("FBI") and advised that "they had reason to believe that international cyber criminals gained access to the internal Citrix network."[15] Even at that early time, however, the "FBI ha[d] advised that the hackers likely used a tactic known as password spraying, a technique that exploits weak passwords. Once they gained a foothold with limited access, they worked to circumvent additional layers of security."[16]

54. On April 4, 2019, Citrix revealed the following additional information:

> We are devoting significant resources to manage this incident with painstaking deliberateness and thoroughness. We have brought on board multiple leading cyber security firms to assist our internal team with the work, and we continue to be engaged with the FBI.
>
> Based on where we are in the investigation at this point:

[15] Stan Black, *Citrix investigating unauthorized access to internal network*, Citrix.com (Mar. 8, 2019), https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/ (last visited July 26, 2019).

[16] *Id.*

- We identified password spraying, a technique that exploits weak passwords, as the likely method by which the threat actors entered our network.
- We have taken measures to expel the threat actors from our systems. Additionally, we've performed a forced password reset throughout the Citrix corporate network and improved internal password management protocols.
- We have found no indication that the threat actors discovered and exploited any vulnerabilities in our products or services to gain entry.
- Based upon the investigation to date, there is no indication that the security of any Citrix product or service was compromised by the threat actors.[17]

55. Citrix ultimately notified Plaintiffs and Class members of the Data Breach by letter dated April 29, 2019 (the "Notice Letter").[18] The Notice Letter confirmed that hackers had not only accessed Citrix's network between October 13, 2018 and March 8, 2019, but also "removed files from [Citrix's] systems, which may have included files containing information about our current and former employees and, in limited cases, information about beneficiaries and/or dependents."[19] The Notice Letter further acknowledged that the stolen information could have included names, Social Security numbers, and financial information for current and former employees, including potentially their dependents and beneficiaries.[20]

56. The Notice Letter recommended that affected individuals "remain vigilant for incidents of fraud and identity theft by, for example, regularly reviewing your account statements and regularly monitoring your credit reports. If you discover any suspicious or unusual activity

[17] Eric Armstrong, *Citrix provides update on unauthorized internal network access*, Citrix.com (Apr. 4, 2019), https://www.citrix.com/blogs/2019/04/04/citrix-provides-update-on-unauthorized-internal-network-access/ (last visited July 26, 2019).

[18] *See* Citrix Sample Notice of Data Breach Letter provided to California Attorney General, https://oag.ca.gov/system/files/CX1%20US%20LTR%20%28no%20MA%20or%20CT%29_0.pdf (last visited July 26, 2019).

[19] *Id*.

[20] *Id*.

on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions."[21]

57. Unfortunately, Citrix's notification to affected individuals was severely deficient in numerous respects. First, Citrix failed to disclose exactly who was affected and what information was compromised, instead using vague phrasing "information relating to certain individuals who are current and former employees, as well as certain beneficiaries and dependents" and giving non-exhaustive examples including "names, Social Security numbers, and financial information." But employers like Citrix routinely store all sorts of other employee information, including full names and addresses, e-mail addresses, employee system passwords, tax information, W-2 and other IRS forms, insurance information that may include the personal information of dependents and family members, and payroll records, among others. Consequently, Plaintiffs and Class members remain in the dark regarding what information was actually stolen.

58. Citrix's failure to specify what information was stolen is important because affected individuals may take different precautions depending on what type of information was compromised. For example, if W-2 information, tax information, or payroll records were compromised, affected individuals may need to contact the Internal Revenue Service or their accountants to place fraud alerts on their accounts. If the breach included Social Security numbers or other identifiable information, the impacted individuals may need to enroll in credit monitoring, contact their financial institutions or credit bureaus to freeze their accounts, or take other additional measures. By failing to identify exactly who was affected or what information was compromised, Citrix has prevented its current and former employees from taking

[21] *Id.*

meaningful, proactive, and targeted mitigation measures that could help protect them from years of financial harm.

59. In addition to lacking the necessary safeguards to secure Personal Information, Citrix did not have adequate monitoring systems and controls in place to detect the unauthorized infiltration after it occurred. Citrix, like any company its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to thousands of employee files. In this case, Citrix only learned of the breach after the FBI warned Citrix its systems were compromised months after they were initially accessed.

60. Moreover, the Data Breach was entirely preventable given that password spraying is a well-known tactic of cyber attackers. As explained by the Department of Homeland Security ("DHS") in a March 2018 alert:

> In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow three to five bad attempts during a set period of time. During a password-spray attack (also known as the "low-and-slow" method), the malicious actor attempts a single password against many accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.
>
> Password spray campaigns typically target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols. An actor may target this specific protocol because federated authentication can help mask malicious traffic. Additionally, by targeting SSO applications, malicious actors hope to maximize access to intellectual property during a successful compromise.
>
> Email applications are also targeted. In those instances, malicious actors would have the ability to utilize inbox synchronization to (1) obtain unauthorized access to the organization's email directly from the cloud, (2) subsequently download user mail to locally stored email files, (3) identify the entire company's email

address list, and/or (4) surreptitiously implements inbox rules for the forwarding of sent and received messages.[22]

61. DHS also described the typical "tactics, techniques, and procedures (TTPs)" of a password-spray attack, which include:

- Using social engineering tactics to perform online research (i.e., Google search, LinkedIn, etc.) to identify target organizations and specific user accounts for initial password spray
- Using easy-to-guess passwords (e.g., "Winter2018", "Password123!") and publicly available tools, execute a password spray attack against targeted accounts by utilizing the identified SSO or web-based application and federated authentication method
- Leveraging the initial group of compromised accounts, downloading the Global Address List (GAL) from a target's email client, and performing a larger password spray against legitimate accounts; and
- Using the compromised access, attempting to expand laterally (e.g., via Remote Desktop Protocol) within the network, and performing mass data exfiltration using File Transfer Protocol tools such as FileZilla.[23]

62. DHS also detailed the indicators of a password spray attack, which include:

- A massive spike in attempted logons against the enterprise SSO portal or web-based application;
    - Using automated tools, malicious actors attempt thousands of logons, in rapid succession, against multiple user accounts at a victim enterprise, originating from a single IP address and computer (e.g., a common User Agent String).
    - Attacks have been seen to run for over two hours.
- Employee logons from IP addresses resolving to locations inconsistent with their normal locations.[24]

[22] U.S. Dep't of Homeland Security, *Alert (TA18-086A): Brute Force Attacks Conducted by Cyber Actors* (Mar. 27, 2018, last revised March 28, 2018), *available at*: https://www.us-cert.gov/ncas/alerts/TA18-086A (last visited July 26, 2019).

[23] *Id*.

[24] *Id*.

63. Importantly, *months before* the initial intrusion at Citrix began, DHS detailed both the typical victim environment for password spray attacks, and the methods to prevent such an intrusion:

> **Typical Victim Environment**
>
> The vast majority of known password spray victims share some of the following characteristics:
>
> - Use SSO or web-based applications with federated authentication method
> - Lack multifactor authentication (MFA)
> - Allow easy-to-guess passwords (e.g., "Winter2018", "Password123!")
> - Use inbox synchronization, allowing email to be pulled from cloud environments to remote devices
> - Allow email forwarding to be setup at the user level
> - Limited logging setup creating difficulty during post-event investigations
>
> ***
>
> **Solution**
>
> **Recommended Mitigations**
>
> To help deter this style of attack, the following steps should be taken:
>
> - Enable MFA and review MFA settings to ensure coverage over all active, internet facing protocols.
> - Review password policies to ensure they align with the latest NIST guidelines and deter the use of easy-to-guess passwords.
> - Review IT helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts. IT helpdesk password procedures may not align to company policy, creating an exploitable security gap.

- Many companies offer additional assistance and tools [that] can help detect and prevent password spray attacks, such as the Microsoft blog released on March 5, 2018.[25]

64. In fact, following the Data Breach, Citrix even posted on its website a blog post entitled "*Security best practices: Multi-factor authentication*"[26] that advised its *clients* on the risks of password spraying and the best ways to combat such attacks:

> WHAT IS PASSWORD SPRAYING?
>
> Password spraying is a technique in which cyber criminals use passwords from previous breaches, or generated password lists, to attempt access to an environment. Slowly testing against many user accounts, from a variety of source networks, these attacks are hard to identify since many do not trigger threshold alarms.
>
> HOW DO YOU PROTECT YOURSELF FROM PASSWORD SPRAYING?
>
> Multi-factor authentication (MFA) and user education are the most traditional, and in many cases, the most effective deterrents. We will focus on these two protections in this article, but there are additional protections that can be layered in to provide added security. Increased audit, analytics, and defining a secure digital perimeter also help detect and protect against attacks.
>
> The weakest link determines the ultimate strength of your security system. Often, this link is your users' passwords. As a result, our most common security recommendation is to enforce MFA for all external entry points.
>
> ***
>
> USER EDUCATION
>
> As passwords are the key to unlocking your environment, your end users play a key role in ensuring their passwords deter rather than enable criminals. However, some users don't fully understand, or aren't aware of, security policies and best practices around password development. Therefore, user education is an important step in fortifying your systems' password security. Too often we rely on password length and complexity requirements to enforce our password policy. What looks like a complex password scheme leads to a simple password that is trivial for a computer to crack. In addition, some organizations go further by periodically testing users' passwords against known vulnerable passwords and discouraging users from using repeatable, easy patterns.

---

[25] *Id.* (footnotes omitted).

[26] Hector Lima, *Security best practices: Multi-factor authentication*, Citrix.com (April 4, 2019), https://www.citrix.com/blogs/2019/04/04/security-best-practices-multi-factor-authentication/ (last visited July 26, 2019).

> IN CLOSING
>
> Security safeguards and attacks against them are continually evolving. In light of new attack methods we've seen in recent months, multi-factor authentication and user education around passwords have become two important steps that every organization can take to help deter cyber criminals from gaining entry to their environment.[27]

65. But despite Citrix's recommendation that its clients implement multi-factor authentication "for all external entry points" and acknowledgement that "multi-factor authentication and user education around passwords" are "important steps that every organization can take to help deter cyber criminals from gaining entry to their environment" – Citrix failed to heed its own security advice for safeguarding the Personal Information of its employees.[28]

66. On July 24, 2019, Citrix president and CEO, David Henshall posted on Citrix's website a blog post entitled "*Citrix concludes investigation of unauthorized internal network access*."[29] In the post, Citrix confirmed that "the cyber criminals gained access to our internal network through password spraying, a technique that exploits weak passwords. Once in our network, the cyber criminals intermittently accessed and, over a limited number of days between October 13, 2018, and March 8, 2019, principally stole business documents and files from a company shared network drive that has been used to store current and historical business documents, as well as a drive associated with a web-based tool used in our consulting practice."[30]

67. Citrix further acknowledged that the "cyber criminals also may have accessed the individual virtual drives and company email accounts of a very limited number of compromised

---

[27] *Id*.

[28] *Id*.

[29] David Henshall, *Citrix concludes investigation of unauthorized internal network access*, Citrix.com (July 24, 2019), https://www.citrix.com/blogs/2019/07/19/citrix-concludes-investigation-of-unauthorized-internal-network-access/ (last visited July 26, 2019).

[30] *Id*.

users and launched without further exploitation a limited number of internal applications." It stated that "[a]s part of an extensive e-discovery process, experts are carefully reviewing documents and files that may have been accessed or were stolen in this incident. We have notified, or shortly will notify, the limited number of customers who may need to consider additional protective steps."[31]

68. Regarding remediation measures, Citrix asserted that "we have taken significant actions to safeguard our systems and improve protocols. We performed a global password reset, improved our internal password management, and strengthened password protocols. Further, we improved our logging at the firewall, increased our data exfiltration monitoring capabilities, and eliminated internal access to non-essential web-based services along with disabling non-essential data transfer pathways. We also deployed [third party security vendor] FireEye's endpoint agent technology across our systems to provide an additional layer of defense. These protective agents perform continuous monitoring across the enterprise permitting us to quickly contain any detected issues."[32]

69. Under the heading "Moving Forward," Henshall stated that he is "focused on fostering a security culture at Citrix that prioritizes prevention and also ensures that we detect and respond effectively to any future incidents. The improvements to our security culture will extend to the highest levels of our company" including implementing a "cybersecurity committee" to "become a permanent part of our governance model."[33] But rather than apologize to those individuals who were impacted, Henshall instead thanked them for their "support":

> Finally, I want to express my sincerest appreciation to the employees and customers that have been impacted by this incident for their understanding and

[31] *Id.*

[32] *Id.*

[33] *Id.*

> support. Throughout the investigation, we have endeavored to be as transparent as possible with key findings and lessons learned, but we recognize that is not enough. And while we have made meaningful strides towards improving our cyber security defenses, we live in a dynamic threat environment that requires a culture of continuous improvement. I want to assure you that we are fully committed to continuing to foster such a culture, and we are doing everything possible to ensure this type of incident cannot happen again.[34]

70. Unfortunately, the data security measures that Citrix is now putting into place – such as implementing multi-factor authentication and strengthening password requirements – are measures that any reasonable company (and especially technology company) should have implemented years ago. Had Citrix heeded the DHS's guidelines or followed its own advice to its clients, the Data Breach could have been prevented entirely.

C. Citrix Failed to Comply With FTC Requirements

71. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[35]

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[36] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no

---

[34] *Id*.

[35] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 26, 2019).

[36] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 26, 2019).

longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[37]

73. Additionally, the FTC recommends that companies limit access to sensitive 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.[38]

74. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect Personal Information, 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 ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[39]

75. As a technology company, Citrix understood the risks and consequences of inadequate data security, but nevertheless operated network systems with outdated operating systems and software, and failed to detect the hackers' presence for months, notice the massive

[37] *Id*.

[38] FTC, *Start With Security*, *supra* note 35.

[39] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 26, 2019).

amounts of data that were being exfiltrated from its databases, or take any steps to investigate the numerous other red flags that should have warned the company about what was happening.

76. Citrix's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

D. Plaintiffs' Employment with Citrix and Discovery of Breach

77. Plaintiffs are, or were, all employed by Citrix and provided their Personal Information as a condition of that employment, and/or are family members of those employed or formerly employed by Citrix whose information was obtained by Citrix as a result of their family members' employment.

1. Plaintiff Lee Milligan

78. Plaintiff Lee Milligan and his minor son are citizens of Georgia. Plaintiff Milligan was employed by Citrix from 2013 to 2018. As a condition of his employment, Plaintiff Milligan provided Citrix with significant amounts of his personal and financial information, including his name and address, Social Security number, bank and financial account information, insurance information, and payroll and tax information, as well as information pertaining to his beneficiaries and dependents.

79. In a letter dated April 24, 2019, Plaintiff Milligan was notified by Citrix that his Personal Information may have been compromised in the Data Breach. On July 16, 2019, Plaintiff Milligan received a follow-up letter from Citrix's Chief Privacy and Digital Risk Officer Peter Lefkowitz confirming that the Personal Information of Plaintiff Milligan's nine-year-old son was exfiltrated in the Data Breach. The letter stated that "we are providing this notice so that you or your dependent can take the steps you deem appropriate."

80. As a result of the Data Breach, Plaintiff Milligan has spent time and effort researching the Data Breach, monitoring his financial accounts to detect potential fraud, and intends to purchase identity theft monitoring services on behalf of his family and minor son.

2. Plaintiff Lindsey Howard

81. Plaintiff Howard was hired by Citrix as a contractor in early 2006 and served in that role until approximately August 2007. From August 2007 through May 2018, Plaintiff Howard was a full-time employee of Citrix, holding roles as a billing maintenance representative, consulting services billing associate, and accounts receivable representative, among others. Plaintiff Howard left Citrix in May 2018 to pursue other opportunities.

82. As a condition of her employment, Plaintiff Howard provided Citrix with significant amounts of her personal and financial information, including her name and address, Social Security number, bank and financial account information, insurance information, and payroll and tax information. Plaintiff Howard also provided Citrix with Personal Information relating to her spouse and three minor children who were her beneficiaries and dependents.

83. After receiving the Notice Letter dated April 29, 2019, Plaintiff Howard became fearful for the safety of herself and her family. As recommended by Citrix, Plaintiff Howard has taken and continues to take steps to mitigate against possible harm, including daily monitoring of her and her family's credit reports and financial accounts. Plaintiff Howard also pays a monthly fee to enroll in identity theft protection and credit monitoring services through Complete ID to help discover and protect against instances of identity theft or fraud.

84. Plaintiff Howard subsequently received an alert notifying her that her Personal Information was located on illegal internet sites on the dark web. Plaintiff Howard has suffered

stress and anxiety worrying about the safety and financial well-being of her family and three minor children.

3. Plaintiff Kristi Jackson

85. Plaintiff Kristi Jackson was employed by Citrix from 1998 to 2003. As a condition of her employment, Plaintiff Jackson provided Citrix with significant amounts of her personal and financial information.

86. After receiving a letter from Citrix notifying her that her Personal Information was stolen, Plaintiff Jackson spent time and effort putting a credit freeze in place and is currently paying for credit monitoring.

87. Plaintiff Jackson also had to file a police report because she is receiving phishing attempts at her current job. The phishing attempts sought to have Plaintiff Jackson's current human resources department route her direct deposit to a fraudulent account.

4. Plaintiff Michelle Ramus

88. Plaintiff Michelle Ramus was employed by Citrix from April 2017 to April 2019. Her husband, Plaintiff Charles Ramus, was listed in her employment records as her beneficiary.

89. On or around April 29, 2019, Ms. Ramus received a letter from Citrix informing her that her Personal Information was stolen.

90. Later, on June 5, 2019, Ms. Ramus received an email from Citrix's human resources offering two years of credit monitoring, which was also extended to her beneficiaries, including her husband, Plaintiff Charles Ramus. The email also informed Ms. Ramus that Citrix was working on a revised letter to its current and former employees regarding the Data Breach.

91. As a result of the Data Breach, Plaintiff Michelle Ramus has spent time and effort contacting her credit card companies and monitoring her financial accounts to detect fraudulent activity.

5. Plaintiff Charles Ramus

92. Plaintiff Charles Ramus is married to Plaintiff Michelle Ramus and was included in her Citrix employment records as her beneficiary.

93. Beginning on approximately March 15, 2019, Plaintiff Ramus started receiving notifications from his credit card companies, banks, and online accounts – including Paypal, Amazon, and eBay – that an unauthorized person(s) was constantly attempting to access his accounts and passwords related to those accounts. Plaintiff Ramus has about 12 accounts. For each account, Plaintiff Ramus was asked to reset his password numerous times, and even after the reset, he had to reset them again, for at least an additional three times. To date, there have been approximately 30 hacking attempts to Plaintiff Ramus' financial accounts and online accounts.

94. As a result of these hacking attempts, Plaintiff Ramus had to spend additional time and effort to implement two-factor authentication on his accounts. However, even with the implementation of two-factor authentication, Plaintiff Ramus still experienced attempted hacking issues to his accounts. For example, Plaintiff Ramus received texts asking if he requested access to an account and requested a change to his password. This has happened approximately 10 times since Plaintiff Ramus added two-factor authentication to his accounts.

95. As a result of the Data Breach, Plaintiff Charles Ramus has spent time and effort, and continues to spend time and effort, researching and monitoring his financial and online accounts in an effort to detect and prevent any further misuse.

6. Plaintiff Brandon Sargent

96. Plaintiff Brandon Sargent is a citizen of North Carolina. Plaintiff Sargent was employed by Citrix from 2015 to 2019. As a condition of his employment, Plaintiff Sargent provided Citrix with significant amounts of his personal and financial information.

97. Citrix collected, stored and used Plaintiff Sargent's Personal Information. Following the Data Breach, Plaintiff had fraudulent charges to his debit card and was forced to freeze the account. While his account was frozen, Plaintiff Sargent's vehicle broke down and he was unable to pay for repairs, until he got his new card a week later. Plaintiff has also received fraudulent phone calls and other identity theft attempts that have caused him to waste countless hours mitigating the damage from this breach.

7. Plaintiff Natalie Young

98. Plaintiff Natalie Young was employed by Citrix from March 4, 2019 through July 1, 2019. As a condition of her employment with Citrix, Plaintiff Young was required to provide Citrix with her personal and financial information, including her Social Security number, bank and financial account information, such as routing and checking account numbers, tax information, and her name and address. Plaintiff Young also provided Citrix with personal information relating to her beneficiaries.

99. On or around April 8, 2019, Plaintiff Young received a fraud notice from her bank informing her that her financial accounts were locked. Plaintiff Young's bank informed her that her bank routing number and checking account numbers and Social Security number were compromised, and that her financial account was completely emptied. As a result, Plaintiff Young lost use of her funds, which she needed for her daily living necessities, among other

things. Plaintiff Young's bank also informed her that she was not the first Citrix employee to have had their financial account hacked since the announcement of the Data Breach.

100. On the evening of April 8, 2019, at 7:14 p.m., Plaintiff Young informed Citrix's Human Resources Department and Citrix's Security Department of what happened to her financial account. That same evening, on or around 9:00 p.m., Citrix's Human Resources personnel, Peggy Way, called Plaintiff Young and told her that she spoke with the Director of Global Security Risk Services, Jeff Dean, about what had happened. Rather than taking the matter seriously, Mr. Dean told Plaintiff Young: "Don't you think if anyone's accounts are going to be hacked it would be an executive versus a sales person?"

101. On or around April 9, 2019, Mr. Dean responded to Plaintiff Young's note by simply directing her to the FTC website regarding identity theft (www.identitytheft.gov/steps) without any information concerning the Data Breach that would help Plaintiff Young take proactive, meaningful, and targeted mitigation measures to protect herself from further financial headache and harm.

102. On May 17, 2019, Plaintiff Young received an email from Citrix stating that her "current user account password has been identified as a ***compromised password***" and to "change [her] password **immediately**." (Emphasis in original).

103. As a result of the Data Breach, Plaintiff Young's banking has become complicated. Each time Plaintiff Young is paid her wages, she must go, in-person, to her bank to transfer her money into her checking account so she can access and use her funds.

104. During the process of working with her bank to resolve the fraud, Plaintiff Young's electronic bill payments have been repeatedly denied, resulting in late fees to her. Plaintiff Young experienced late fees as recently as July 2019.

105. Plaintiff Young has also suffered additional damages, including the loss of use of her funds for approximately four days.

106. Moreover, as a result of the Data Breach, Plaintiff Young has spent time and money driving to the bank to handle and manage her financial affairs, has incurred late fees due to bill payments having been repeatedly denied, and has spent countless hours attempting to fix her financial account. Plaintiff Young continues to spend time and effort researching and monitoring her financial accounts in an effort to detect and prevent any further misuse and unauthorized access.

E. The Citrix Data Breach Caused Harm and Will Result in Additional Fraud

107. Without detailed disclosure to Citrix's employees and others impacted, affected individuals including Plaintiffs and Class members have been left exposed, unknowingly and unwittingly, for months, to continued misuse and ongoing risk of misuse of their Personal Information without being able to take necessary precautions to prevent imminent harm.

108. The ramifications of Citrix's failure to keep Plaintiffs' and Class members' data secure are severe.

109. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." *Id*.

110. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have

personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[40]

111. Identity thieves can use personal information, such as that of Plaintiffs and Class members, which Citrix failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or medical treatment; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

112. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and

[40] Federal Trade Commission, *Warning Signs of Identity Theft* (May 2015), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 26, 2019).

> monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[41]

113. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[42]

114. In fact, Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[43]

---

[41] Federal Trade Commission, *Combating Identity Theft A Strategic Plan* (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited July 26, 2019).

[42] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), *available at*: http://www.ssa.gov/pubs/10064.html (last visited July 26, 2019).

[43] Javelin Research, *2016 Identity Fraud: Fraud Hits an Inflection Point* (Feb. 2, 2016), *available at:* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited July 26, 2019).

115. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[44]

116. There may also be a significant time lag between when personal information is stolen and when it is actually misused. 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.[45]

117. Moreover, Plaintiffs and Class members place significant value in data security. Had they known their employer would not adequately protect and secure their Personal Information, they would have refused to provide such information or sought alternative employment.

F. Plaintiff and Class Members Suffered Damages

118. The Personal Information of Plaintiffs and Class members is private and sensitive in nature and was left inadequately protected by Citrix. Citrix did not obtain Plaintiffs' and Class members' consent to disclose their Personal Information to any other person as required by applicable law and industry standards.

---

[44] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Sept. 2015, revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 26, 2019).

[45] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited July 26, 2019).

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

120. Citrix had the resources to prevent a breach. Citrix made significant expenditures to market its products and tout its prowess in the technology field, but neglected to adequately invest in data security, despite the growing number of intrusions and several years of well-publicized data breaches.

121. Had Citrix remedied the deficiencies in its systems, followed DHS guidelines, and adopted security measures recommended by experts in the field, Citrix would have prevented or discovered the intrusion into its network and systems and, ultimately, the theft of its current and former employees' Personal Information.

122. As a direct and proximate result of Citrix's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time, which they otherwise would have dedicated to other life demands, such as work, to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports.

123. Citrix's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. identity theft and fraud resulting from the theft of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to address and mitigate the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals and/or misused via sale on the Internet black market;

h. damages to and diminution in value of their Personal Information entrusted to Citrix for the sole purpose of working for Citrix; and

i. the loss of Plaintiffs' and Class members' privacy.

124. Citrix continues to hold Personal Information of its current and former employees, including Plaintiffs and Class members. Particularly because Citrix has demonstrated an inability to prevent a breach, or stop one from continuing even after detection, Plaintiffs and Class

members have an undeniable interest in ensuring that their Personal Information is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

125. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Rule 23(a), (b)(2), (b)(3) and/or (c)(4), Fed. R. Civ. P., Plaintiffs seek certification of a nationwide class defined as follows:

> All individuals residing in the United States whose Personal Information was compromised in the data breach initially disclosed by Citrix in or about March 2019 (the "Class" or "Nationwide Class").

126. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs Howard, Jackson, Michelle Ramus, Charles Ramus, and Young assert claims under the law of Florida on behalf of a separate statewide subclass, defined as follows:

> All individuals residing in Florida whose Personal Information was compromised in the data breach initially disclosed by Citrix in or about March 2019 (the "Florida Subclass").

127. Pursuant to Rule 23, Plaintiffs Milligan (on behalf of himself), Howard, Jackson, Michelle Ramus, Sargent, and Young assert claims on behalf of a separate employee subclass, defined as follows:

> All current and former employees of Citrix whose Personal Information was compromised in the data breach initially disclosed by Citrix in or about March 2019 (the "Citrix Employee Subclass").

128. Excluded from each of the above Classes are all persons who make a timely election to be excluded from the Class; government entities; and the judge(s) to whom this case is assigned and their immediate family and court staff.

129. Plaintiffs hereby reserve the right to amend or modify the class definition(s) with greater specificity or division after having had an opportunity to conduct discovery.

130. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

131. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class includes potentially tens of thousands of individuals whose Personal Information was compromised in the Data Breach. Class members may be identified through objective means, including by and through Citrix's business records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

132. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Citrix had a duty to protect Personal Information;

b. Whether Citrix knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Citrix's security measures to protect its systems were reasonable in light of known legal requirements, such as the FTC data security recommendations, and industry standards;

d. Whether Citrix was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Citrix's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether Citrix's conduct constituted unfair or deceptive trade practices;

g. Whether Citrix'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 Personal Information of Plaintiffs and Class members;

h. Whether Plaintiffs and Class members were injured and suffered damages or other losses because of Citrix's failure to reasonably protect its systems and data network; and,

i. Whether Plaintiffs and Class members are entitled to relief.

133. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs are current and former employees (or dependents or beneficiaries of current and former employees) whose Personal Information was in Citrix's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seek relief consistent with the relief of the Class.

134. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Citrix to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation.

Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

135. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 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 purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Citrix, and thus, individual litigation to redress Citrix's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the 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, economies of scale, and comprehensive supervision by a single court.

136. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

137. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Citrix owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Citrix's security measures to protect is systems were reasonable in light of known legal requirements, such as the FTC data security recommendations, and industry standards;

c. Whether Citrix failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiff and the Class members; and,

d. Whether adherence to FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

138. Finally, all members of the proposed Class are readily ascertainable. Citrix has access to information regarding which of its employees, former employees, and their beneficiaries and dependents were affected by the Data Breach. Using this information, the members of the Class can be identified through objective means.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE FLORIDA SUBCLASS)

139. Plaintiffs restate and re-allege paragraphs 1 through 138 as if fully set forth herein.

140. Citrix owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class members' Personal Information within its control from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty includes, among other things, designing,

maintaining and testing Citrix's security systems to ensure that Plaintiffs' and Class members' information in Citrix's possession was adequately secured and protected.

141. Citrix owed a duty of care to Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the Personal Information of its current and former employees.

142. Citrix owed a duty of care to Plaintiffs and members of the Class because they were foreseeable and probable victims of any inadequate security practices. Citrix knew or should have known of the inherent risks in collecting and storing the Personal Information of its employees and their beneficiaries and dependents and the critical importance of adequately securing such information.

143. Plaintiffs and members of the Class entrusted Citrix with their Personal Information on the premise and with the understanding that Citrix would safeguard their information, and Citrix was in a position to protect against the harm suffered by Plaintiffs and members of the Class as a result of the Data Breach.

144. Citrix's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Personal Information. Citrix's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard data 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.

145. Citrix knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its systems, and the importance of adequate security. Citrix knew about numerous, well-publicized data breaches within the technology industry including those targeting its own company.

146. Citrix breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiffs and Class members.

147. Because Citrix knew that a breach of its systems would damage tens of thousands of current and former Citrix employees, including Plaintiffs and Class members, Citrix had a duty to adequately protect its data systems and the Personal Information contained thereon.

148. Citrix had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Citrix with their Personal Information as a condition of employment was predicated on the understanding that Citrix would take adequate security precautions to protect their Personal Information.

149. Citrix also had independent duties under state and federal laws that required Citrix to reasonably safeguard Plaintiffs' and Class members' Personal Information and promptly notify them about the Data Breach.

150. Citrix breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiffs and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' Personal Information both before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiffs' and Class members' Personal Information had been improperly acquired or accessed.

151. The law further imposes an affirmative duty on Citrix to timely disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class so that Plaintiffs and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information.

152. Citrix breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting to notify Plaintiffs and Class members and then by failing to provide Plaintiffs and Class members sufficient information regarding the breach, including disclosing what information was compromised and who was affected. To date, Citrix has not provided sufficient information to Plaintiffs and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

153. Through Citrix's acts and omissions described in this Complaint, including Citrix's failure to provide adequate security and its failure to protect Personal Information of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Citrix unlawfully breached its duty to use reasonable care to adequately protect and secure Personal Information of Plaintiffs and Class members during the time it was within Citrix's possession or control.

154. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Citrix prevented Plaintiffs and Class members from taking meaningful, proactive, and targeted measures to mitigate against potential harm.

155. Citrix improperly and inadequately safeguarded the Personal Information of Plaintiffs and Class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Citrix's failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiffs and Class members.

156. Citrix's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Personal Information; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Personal Information of Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive Personal Information had been compromised.

157. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

158. As a direct and proximate cause of Citrix's conduct, Plaintiffs and Class members have suffered and will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit

reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Citrix possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE FLORIDA SUBCLASS)

159. Plaintiffs restate and re-allege paragraphs 1 through 138 as if fully set forth herein.

160. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Citrix, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

161. The FTC publications and orders described above also form part of the basis of Citrix's duty in this regard.

162. Citrix violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Citrix's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach at a company as large as Citrix, including, specifically, the immense damages that would result to Plaintiff and Class members.

163. Citrix's violation of Section 5 of the FTC Act constitutes negligence *per se*.

164. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

165. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

166. Moreover, Florida law requires that covered entities "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. § 501.171(2).

167. "Covered entity" in includes any "commercial entity that acquires, maintains, stores, or uses personal information." Fla. Stat. § 501.171(1)(b).

168. "Personal information" means "[a]n individual's first name or first initial and last name in combination with" several additional data elements for that individual, including, social security number; driver license or identification card number; and/or financial account number or credit or debit card number. Fla. Stat. § 501.171(1)(g).

169. Citrix violated § 501.171(2) by failing to take reasonable measures to protect and secure Plaintiffs' and Class Member's Personal Information.

170. The harm that occurred as a result of the Data Breach is the type of harm section 501.171(2) was intended to guard against, and Plaintiffs and the Class are in the class of persons the section was intended to protect.

171. Citrix's violation of § 501.171(2) constitutes negligence *per se*.

172. As a direct and proximate result of Citrix's negligence *per se*, Plaintiffs and Class members have suffered and will suffer injury and damages, including but not limited to: (i) the

loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Citrix possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT III
VIOLATIONS OF THE OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq.*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE FLORIDA SUBCLASS)

173. Plaintiffs restate and re-allege paragraphs 1 through 138 as if fully set forth herein.

174. Citrix engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

175. As alleged herein this Complaint, Citrix engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard Personal Information;

b. failure to make only authorized disclosures of employees' Personal Information;

c. failure to timely and accurately disclose the Data Breach to Plaintiffs and Class members;

d. failure to disclose that its computer systems and data security practices were inadequate to safeguard Personal Information from theft; and

e. failure to timely and accurately disclose the Data Breach to Plaintiffs and Class members.

176. Citrix's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Citrix engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to its current and former employees.

177. In committing the acts alleged above, Citrix engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to its current and former employees that it did not follow industry best practices for the collection, use, and storage of Personal Information.

178. As a direct and proximate result of Citrix's conduct, Plaintiffs and other members of the Class have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs

associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

179. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

180. Also as a direct result of Citrix's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

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

B. Ordering that Citrix engage third-party security auditors and internal personnel to run automated security monitoring;

C. Ordering that Citrix audit, test, and train its security personnel regarding any new or modified procedures;

D. Ordering that Citrix segment Personal Information by, among other things, creating firewalls and access controls so that if one area of Citrix is compromised, hackers cannot gain access to other portions of Citrix systems;

E. Ordering that Citrix purge, delete, and destroy in a reasonable secure manner Personal Information not necessary for its provisions of services;

F. Ordering that Citrix conduct regular database scanning and securing checks;

G. Ordering that Citrix routinely and continually conduct 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; and

H. Ordering Citrix to meaningfully educate its employees about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps Citrix employees must take to protect themselves.

COUNT IV
BREACH OF CONTRACT
(ON BEHALF OF THE CITRIX EMPLOYEE SUBCLASS)

181. Plaintiffs Milligan (on behalf of himself), Howard, Jackson, Michelle Ramus, Sargent, and Young ("Plaintiffs," for purposes of this Count), bring this cause of action on behalf of the Citrix Employee Subclass and re-state and re-allege paragraphs 1 through 138 as if fully set forth herein.

182. Citrix's Code of Business Conduct is an agreement between Citrix, including its management and directors, and its employees, including Plaintiffs and Class members.

183. Citrix's Code of Business Conduct states, among other things, that Citrix and its employees are required to (a) "Always protect the privacy of our employees, customers, and partners"; (b) "Handle personal information in a manner that will avoid accidental loss or alteration or unauthorized access"; and (c) "Never disclose personal information to anyone outside of Citrix without specific authorization[.]"

184. Plaintiffs and class members fully performed their obligations under Citrix's Code of Business Conduct.

185. Citrix, on the other hand, breached its agreement with Plaintiffs and Class members by: (a) failing to protect the privacy of its employees; (b) failing to handle Plaintiffs' and Class members' Personal Information in a manner that would avoid accidental loss or alteration or unauthorized access; and (c) disclosing Plaintiffs' and Class members' Personal Information to unauthorized individuals outside of Citrix.

186. As a direct and proximate result of Citrix's breach of contract, Plaintiffs and Class members have suffered and will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Citrix possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT V
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF THE CITRIX EMPLOYEE SUBCLASS)

187. Plaintiffs Milligan (on behalf of himself), Howard, Jackson, Michelle Ramus, Sargent, and Young ("Plaintiffs," for purposes of this Count), bring this cause of action on behalf of the Citrix Employee Subclass, and assert this claim in the alternative to their breach of contract claim to the extent necessary, and re-state and re-allege paragraphs 1 through 138 as if fully set forth herein.

188. Plaintiffs and Class members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, beneficiary information, and other personal information to Citrix for tax purposes and to receive employment and benefits.

189. Implicit in the employment agreement between the Citrix and its employees was the obligation that Citrix would use the Personal Information of its employees for business purposes only and not make unauthorized disclosures of the information or allow unauthorized access to the information.

190. Additionally, Citrix implicitly promised to retain this Personal Information only under conditions that kept such information secure and confidential and therefore Citrix had a duty to reasonably safeguard and protect the Personal Information of Plaintiffs and Class members from unauthorized disclosure or access.

191. Plaintiffs and Class members fully performed their obligations under the implied contract with Citrix. Citrix did not.

192. Citrix breached the implied contract with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' Personal Information, which was compromised as a result of the Data Breach.

193. Citrix's acts and omissions have materially affected the intended purpose of the implied contact, which required Plaintiffs and Class members to provide their Personal Information in exchange for employment, compensation, and benefits.

194. As a direct and proximate result of Citrix breach of implied contract, Plaintiffs and Class members have suffered and will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Citrix possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT VI
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF THE CITRIX EMPLOYEE SUBCLASS)

195. Plaintiffs Milligan (on behalf of himself), Howard, Jackson, Michelle Ramus, Sargent, and Young ("Plaintiffs," for purposes of this Count), bring this cause of action on behalf of the Citrix Employee Subclass and re-state and re-allege paragraphs 1 through 138 as if fully set forth herein.

196. In light of the special relationship between Citrix and its employees, whereby Citrix required Plaintiffs and Class Members to provide highly sensitive, confidential, personal and financial information as a condition of their employment, Citrix was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including Plaintiffs and Class members, for the safeguarding of employees' Personal Information.

197. Citrix had a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their employer/employee relationship, and in particular Citrix had a fiduciary duty to keep secure the Personal Information of its current and former employees.

198. Citrix breached its duty to Plaintiffs and Class members to ensure that their Personal Information was not disclosed without authorization or used for improper purposes by failing to provide adequate protections to the information and by disclosing the information to an unknown and unauthorized third party.

199. As a direct and proximate cause of Citrix's breach of fiduciary duty, Plaintiffs and members of the Citrix Employee Subclass have suffered and will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft,

tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Citrix possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT VII
BREACH OF CONFIDENCE
(ON BEHALF OF THE CITRIX EMPLOYEE SUBCLASS)

200. Plaintiffs Milligan (on behalf of himself), Howard, Jackson, Michelle Ramus, Sargent, and Young ("Plaintiffs," for purposes of this Count), bring this cause of action on behalf of the Citrix Employee Subclass and re-state and re-allege paragraphs 1 through 138 as if fully set forth herein.

201. At all times during Plaintiffs' and Class members' interactions with Citrix, Citrix was fully aware of the confidential and sensitive nature of Plaintiffs' and Class members' Personal Information that Plaintiffs and Class members provided to Citrix.

202. As alleged herein and above, Citrix's relationship with Plaintiffs and Class' members was governed by expectations that Plaintiffs' and Class members' Personal Information

would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

203. Plaintiffs and Class members provided their respective Personal Information to Defendant with the explicit and implicit understandings that Citrix would protect and not permit their sensitive Personal Information to be disseminated to any unauthorized parties.

204. Plaintiffs and Class members also provided their respective Personal Information to Defendant with the explicit and implicit understanding that Citrix would take precautions to protect that Personal Information from unauthorized disclosure, such as following industry-standard information security practices.

205. Defendant voluntarily received in confidence Plaintiffs' and Class members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

206. Due to Citrix's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow industry-standard information security practices to secure Plaintiffs' and Class members' Personal Information, Plaintiffs' and Class members' Personal Information was disclosed to and misappropriated by unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

207. But for Citrix's disclosure of Plaintiffs' and Class members' Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' Personal Information, as well as the resulting damages.

208. As a direct and proximate cause of Citrix's actions and/or omissions, Plaintiffs and Class members have suffered damages as alleged herein.

209. The injuries and harm Plaintiffs and Class members suffered were the reasonably foreseeable result of Citrix's unauthorized disclosure of Plaintiffs' and Class members' Personal Information. Citrix knew its computer systems and technologies for accepting and securing Plaintiffs' and Class members' Personal Information had security vulnerabilities because Citrix knew it was failing to observe industry standard information security practices.

210. As a direct and proximate cause of Citrix's breaches of confidence, Plaintiffs and members of the Citrix Employee Subclass have suffered and will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Citrix possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and

repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT VIII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

211. Plaintiffs restate and re-allege paragraphs 1 through 138 as if fully set forth herein.

212. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the state and federal statutes described in this Complaint.

213. An actual controversy has arisen in the wake of the Data Breach regarding Citrix's present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Citrix is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Personal Information. Plaintiffs allege that Citrix's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future

214. Citrix still possesses Personal Information pertaining to Plaintiffs and Class members, which means the Personal Information remains at risk of further breaches.

215. Accordingly, Citrix has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Citrix's lax approach towards data security has

become public; the Personal Information in its possession is more vulnerable than it was prior to announcement of the Data Breach.

216. Actual harm has arisen in the wake of the Data Breach regarding Citrix's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

217. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that (a) Citrix's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Citrix must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Citrix's systems on a periodic basis, and ordering Citrix 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. segmenting Personal Information by, among other things, creating firewalls and access controls so that if one area of Citrix is compromised, hackers cannot gain access to other portions of Citrix systems;

e. purging, deleting, and destroying in a reasonable secure manner Personal Information not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. 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; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Citrix customers must take to protect themselves.

REQUEST FOR RELIEF

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

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class and Citrix Employee Subclass, or in the alternative the separate Florida Subclass and Citrix Employee Subclass;

b. For equitable relief enjoining Citrix from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

c. For equitable relief compelling Citrix to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of Personal Information compromised;

d. For an award of damages, including nominal damages, as allowed by law in an amount to be determined;

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

f. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: July 29, 2019

/s/ John A. Yanchunis
John A. Yanchunis (Fla. Bar No. 324681)
Patrick A. Barthle II (Fla. Bar No. 99286)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com
pbarthle@ForThePeople.com

/s/ J. Austin Moore
Norman E. Siegel (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Telephone: (816) 714-7100
Facsimile: (816) 714-7101
siegel@stuevesiegel.com
moore@stuevesiegel.com

Attorneys for Plaintiffs Lindsey Howard, Lee Milligan and His Minor Son

/s/ Gayle M. Blatt
Gayle M. Blatt (*pro hac vice* to be filed)
David S. Casey, Jr. (*pro hac vice* to be filed)
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD LLP

110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
gmb@cglaw.com
dcasey@cglaw.com

/s/ Herman J. Russomanno III
Herman J. Russomanno (Fla. Bar No. 240346)
Robert J. Borrello (Fla. Bar No. 764485)
Herman J. Russomanno III (Fla. Bar No. 21249)
RUSSOMANNO & BORRELLO, P.A.
Museum Tower – Penthouse 2800
150 West Flagler Street
Miami, Florida 33130
Telephone: (305) 373-2101
Facsimile: (305) 373-2103
hrussomanno@russomanno.com
rborrello@russomanno.com
herman2@russomanno.com

Attorneys for Plaintiffs Kristi Jackson and Brandon Sargent

/s/ Rosemary M. Rivas
Rosemary M. Rivas (*pro hac vice*)
Rosanne L. Mah (*pro hac vice*)
LEVI & KORSINSKY LLP
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 373-1671
Facsimile: (415) 484-1294
rrivas@zlk.com
rmah@zlk.com

Attorneys for Plaintiffs Michelle Ramus, Charles Ramus, and Natalie Young

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing was filed and served on all counsel of record via the Court's CM/ECF electronic filing system.

/s/ *John A. Yanchunis*