**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF FLORIDA**
**FORT LAUDERDALE DIVISION**

| | |
|---|---|
| **JESSICA CAREY**, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>**CITRIX SYSTEMS, INC.,** and **COMCAST CABLE COMMUNICATIONS, LLC d/b/a XFINITY,**<br><br>Defendants. | Civil Action No.: 0:24-cv-60008<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Jessica Carey ("Plaintiff"), individually and on behalf of herself and all others similarly situated, alleges the following against Citrix Systems, Inc. ("Citrix") and Comcast Cable Communications, LLC d/b/a Xfinity ("Comcast") (collectively "Defendants"). The following allegations are based upon Plaintiff's personal knowledge with respect to herself and her own acts, and on information and belief as to all other matters.

## I. INTRODUCTION

1. Plaintiff and Class Members bring this class action against Citrix and Comcast for their failures to properly secure and safeguard Plaintiff's and similarly situated individuals' Private Information, including but not limited to names, mailing addresses, telephone numbers, dates of birth, portions of Social Security numbers, usernames, passwords in encrypted form, and security question prompts and answers.

2. Citrix is a multinational cloud computing company that provides technology services to thousands of organizations. Their services include but are not limited to server technologies, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing technologies. Citrix claims to have over 16 million cloud users.

3. Comcast is an telecommunications business that markets a range of consumer products including cable television, internet, telephone, and wireless services.

4. This class action is brought on behalf of all citizens of all states in the United States who are the victims of a targeted cyberattack on Defendants that occurred on or around October 16, 2023 ("the Data Breach").

5. On or about December 18, 2023, Comcast began mailing a Notice of Data Security Incident to Plaintiffs and other Class Members. According to the Notice of Data Security Incident, "[o]n October 10, 2023, one of Xfinity's software providers, Citrix, announced a vulnerability in one of its products used by Xfinity and thousands of other companies worldwide." As a result of Defendants' inability to properly secure Plaintiff and the Class Members' Private Information, data thieves were able to access and obtain the Private Information of Plaintiff and Class Members on or around October 16, 2023.

6. On December 18, 2023, Comcast posted a copy of its Notice of Data Security Incident to its website.[1] The Notices sent directly to Plaintiff and other Class Members and the Notice posted on Comcast's website were essentially identical and will be collectively referred to as the "Notice."

[1] *Notice to Customers of Data Security Incident*, *available at* https://assets.xfinity.com/assets/dotcom/learn/_Data_Incident.pdf.

7. The Notice failed to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed the Class Members' Private Information, what Citrix product contained the vulnerability, and whether the breach was a system-wide breach or limited to a certain subset of customers.

8. The Notice also failed to provide details on how many people were impacted by the Data Breach. In a filing with the Maine Attorney General's Office, Comcast stated that the Data Breach affected 35.8 million people.

9. Defendants knowingly collected the Private Information of customers in confidence, and have a resulting duty to secure, maintain, protect, and safeguard that Private Information against unauthorized access and disclosure through reasonable and adequate security measures.

10. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses, including, but not limited to, a loss of potential value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendants, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff and Class Members entrusted their Private Information to Defendants, their officials, and agents. That Private Information was subsequently compromised, unlawfully accessed, and stolen due to the Data Breach.

12. Plaintiff brings this class action lawsuit on behalf of herself and all others similarly situated to address Defendants' inadequate safeguarding of Plaintiff's and Class Members' Private Information, for failing to provide adequate notice to Plaintiff and other Class Members of the

unauthorized access to their Private Information by a cyber attacker, and for failing to provide adequate notice of precisely what information was accessed and stolen.

13. Defendants breached their duties to Plaintiff and Class Members by maintaining Plaintiff's and the Class Members' Private Information in a negligent and reckless manner.

14. Upon information and belief, the means of the Data Breach and potential risk for improper disclosure of Plaintiff's and Class Members' Private Information were known and foreseeable to Defendants. Thus, Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left the Private Information in a dangerous and vulnerable condition.

15. Defendants failed to properly monitor the computer network and systems housing the Private Information.

16. Had Defendants properly monitored their property, they would have discovered the intrusion sooner or been able to wholly prevent it.

17. Exacerbating an already devastating privacy intrusion, Plaintiff's and Class Members' identities are now at a heightened risk of exposure because of Defendants' negligent conduct since the Private Information that Defendants collected and stored is now in the hands of data thieves.

18. Armed with the Private Information accessed in the Data Breach, data thieves can now use the Private Information obtained from Defendants to commit a variety of crimes, including credit/debit card fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's

licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

19. As a direct result of the Data Breach, Plaintiff and Class Members have suffered fraud and will continue to be exposed to a heightened and imminent risk of fraud and identity theft, potentially for the rest of their lives. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

20. Plaintiff and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

21. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiff and Class Members have suffered, and will continue to suffer damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam phone calls, letters, and emails received as a result of the Data Breach.

22. Plaintiff and Class Members have suffered, and will continue to suffer, an invasion of their property interest in their own Private Information such that they are entitled to damages from Defendants for unauthorized access to, theft of, and misuse of their Private Information. These harms are ongoing, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the information to obtain money and credit in their names for several years.

23. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed via and/or compromised by Citrix and Comcast during the Data Breach.

24. Accordingly, Plaintiff brings this action on behalf of herself and all others similarly situated against Defendants, seeking redress for their unlawful conduct asserting claims for (1) negligence; (2) negligence *per se*; (3) breach of implied contract; (4) breach of a third-party beneficiary contract; and (5) unjust enrichment.

## II. PARTIES

### A. Plaintiff

25. Plaintiff Jessica Carey ("Mrs. Carey") is a resident of Marblehead, Massachusetts and a citizen of Massachusetts. Mrs. Carey has been a customer of Xfinity since 2020.

### B. Defendants

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

27. Defendant Comcast Cable Communications, LLC d/b/a Xfinity is a Delaware corporation with its principal place of business located in Philadelphia, Pennsylvania.

## III. JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C.§ 1332(d). The amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendants.

29. This Court has personal jurisdiction over Defendants because Citrix's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

30. Venue is proper under 18 U.S.C § 1391(b)(1) because Citrix resides in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, and Defendants conduct substantial business in this District.

## IV. STATEMENT OF FACTS

### *A. Defendant Citrix's Business*

31. Originally founded in 1989, Citrix is a multinational cloud computing company that provides technology services to thousands of organizations. Their services include but are not limited to server technologies, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing technologies. Citrix claims to have over 16 million cloud users.

32. Citrix serves thousands of companies globally and has an expansive client portfolio.[2] In the United States, Citrix serves clients in the following sectors: education, energy and utility, financial services, government and public sector, healthcare, insurance, manufacturing, childcare, professional services, retail, technology, telecommunications, and transportation.[3] Through its contracts with these clients, Citrix cumulatively possesses and stores the PII of millions of people in its databases.

33. According to the company, more than 400,000 companies around the world, including 99 percent of the Fortune 500, rely on Citrix digital workspace solutions.[4]

34. Comcast is one of the companies that uses Citrix's products.

---

[2] Citrix Customer Stories, *available at* https://www.citrix.com/customers/.
[3] *Id.*
[4] Citrix Named to Cloud 500 (Mar. 1, 2022), *available at* https://www.citrix.com/news/announcements/mar-2022/citrix-named-to-cloud-500.html.

### *B. Defendant Comcast's Business*

35. Comcast is an American telecommunications business that markets a range of consumer products including cable television, internet, telephone, and wireless services.

36. Comcast divides its business into two segments: Connectivity & Platforms and Content & Experiences.[5] The Connectivity & Platforms segment contains Comcast's broadband and wireless connectivity businesses under the Xfinity and Comcast brands in the United States and under the Sky brand in certain territories in Europe.[6] The Connectivity & Platforms segment is comprised of both residential and business customers who subscribe to a range of broadband, wireless connectivity and residential and business video services.[7] Comcast generates revenue from the customers who subscribe to these services and the sale of related devices.[8]

37. According to the company's most recent earnings report, Comcast reportedly serves the following breakdown of customers: 32.3 million Broadband customers, 14.9 million video customers, and 5.9 million wireless customers.[9]

### *C. The Collection of Plaintiff's and Class Members' Private Information is Central to Defendants' Businesses*

38. In exchange for providing Plaintiff and Class Members telecommunications services, Plaintiff and Class Members were required to transfer possession of their Private Information to Defendants.

39. Through the possession and utilization of Plaintiff's and Class Members' Private Information, Defendants assumed duties owed to Plaintiff and Class Members regarding their Private Information. Therefore, Defendants knew or should have known that it was responsible

[5] Comcast Corporation (Form 10-Q) (Oct. 26, 2023).
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] Comcast Reports 2nd Quarter 2023 Results, Comcast Corporation (July 27, 2023).

for safeguarding Plaintiff's and Class Members' Private Information from unauthorized access and criminal misuse.

40. Indeed, these duties are expressly assumed and stated by Comcast in the Privacy Policy posted on the company website, stating, "We follow industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain."[10]

41. Plaintiff and Class Members relied on Defendants to keep their Private Information secure and safeguarded for authorized purposes. Defendants owed a duty to Plaintiff to secure their Private Information as such, and ultimately breached that duty.

***D. The Data Breach***

42. On or around October 10, 2023, Citrix announced a vulnerability in a product used by Comcast and thousands of other companies worldwide. This vulnerability has come to be referred to as the "Citrix Bleed."[11] Security researchers dubbed the vulnerability as critical in nature.[12]

43. In announcing the vulnerability, Citrix revealed that it was impacting on-premises versions of its NetScaler ADC and NetScaler Gateway platforms. These products are used for application delivery and VPN connectivity. Citrix released patches to address the vulnerability, but then updated its advisory to customers on October 17, 2023, noting it had been exploited by data thieves. According to Comcast, Citrix issued additional mitigation on October 23, 2023.

---

[10] *Our Privacy Policy*, Xfinity, *available at* https://www.xfinity.com/privacy/policy.
[11] *See* Carly Page, *Hackers are exploiting 'CitrixBleed' bug in the latest wave of mass cyberattacks*, TECHCRUNCH (Nov. 14, 2023), https://techcrunch.com/2023/11/14/citrix-bleed-critical-bug-ransomware-mass-cyberattacks/.
[12] *Id.*

44. More than two weeks after Citrix first discovered the vulnerability, Comcast discovered on October 25, 2023, that between October 16, 2023 and October 19, 2023, data thieves received unauthorized access to and possession of the Private Information of Plaintiff and Class Members. Comcast purports to have launched an investigation into the Data Breach.

45. On December 6, 2023, Comcast concluded that the stolen information includes usernames, hashed passwords, names, contact information, portions of Social Security numbers, dates of birth, and security question prompts and answers. Critically, Comcast notes in its Notice of Data Security Incident that their "data analysis is continuing," and that they will "provide additional notices as appropriate." This indicates that the data Comcast alleges was stolen in the Data Breach should not, in fact, be taken as a whole and definitive list at this time.

46. While Citrix did not release patches for the vulnerability until October, Google's Mandiant cybersecurity group says that hackers had been exploiting the Citrix Bleed since *at least* August to break into systems.[13]

47. Following Defendants' realization of the Data Breach, the company failed to provide meaningful notice to Plaintiff and the Class Members. Any notice provided by Defendants failed to include substantive details on the extent of the Data Breach, the software and/or programs exploited in the Data Breach, what subset of customers had what information stolen in the Data Breach, and what steps were taken to mitigate the risk of subsequent cyberattacks and further harm to Plaintiff and the Class Members.

[13] Sebastian Demmer, Nicole Jenaye, Doug Bienstock, Tufail Ahmed, John Wolfram, Ashley Frazer, Investigation of Session Hijacking via Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966), MANDIANT (Nov. 2, 2023), https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966.

### *E. Plaintiff's Experiences Following the Data Breach*

48. Plaintiff Carey ("Mrs. Carey") has been a customer of Comcast since 2020. Specifically, she is a wireless internet customer.

49. Mrs. Carey was required to provide Comcast with her Private Information as a condition of receiving telecommunications services.

50. Mrs. Carey received notice of the Data Breach from Comcast by logging into her account in December 2023. Upon logging in, Mrs. Carey saw the alert that Comcast had experienced a data breach and prompt urging her to change her password and set up two-factor authentication.

51. Thereafter, Mrs. Carey spent time taking action to mitigate the impact of the Data Breach. This effort included checking her bank accounts and other online accounts, changing her passwords, examining her credit score, and researching the potential impact of the Data Breach, all as a result of her Private Information being exposed in the Data Breach. Mrs. Carey intends to spend additional time and effort taking steps to protect her Private Information in the future. Because of the Data Breach, Mrs. Carey spent valuable time attempting to mitigate the harm she otherwise would have spent on other obligations.

52. Moreover, Mrs. Carey spent this time at Defendant Comcast's direction. In the Notice posted by Comcast, Comcast encouraged Plaintiff and Class Members to spend time mitigating their losses by "enrolling in two-factor or multi-factor authentication" and changing passwords where re-used across multiple accounts. Comcast also stated that Plaintiff and Class Members should "remain vigilant against incidents of fraud and identity theft."

53. As a result of the Data Breach, Mrs. Carey has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Mrs. Carey otherwise

would have spent performing other activities, such as her job, and/or leisurely activities for the enjoyment of life.

54. As a result of the Data Breach, Mrs. Carey has suffered emotional distress as a result of the release of her Private Information which she expected Defendants to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing, and potentially using her Private Information.

55. As a result of the Data Breach, Mrs. Carey will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

### *F. Defendants Knew or Should Have Known Both the Value of Private Information and the Risk of Cyberattacks to Those Who Possess Such Private Information*

56. At all relevant times, Defendants were well aware that the Private Information they collect from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

57. Private Information is a valuable commodity to cyber attackers. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[14] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground websites, commonly referred to as the dark web.

58. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[15] In 2022, 1,802

[14] *What to Know About Identify Theft*, Fed. Trade Comm'n, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited December 29, 2023).

[15] Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout, CISION PR NEWSWIRE (Jan. 19, 2017),

data compromises were reported that impacted over 422 million victims—marking a 42% increase in the number of victims impacted since 2021.[16] That upward trend continues.

59. The ramifications of Defendants' failures to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

60. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

61. Approximately 21 percent of victims do not realize their identities have been compromised until more than two years after it has happened. This gives data thieves ample time to seek multiple treatments under the victim's name.

62. As entities serving consumers in the information technology, software, and telecommunications space, Defendants knew, or reasonably should have known, the importance of safeguarding Plaintiff's and Class Members' Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html.

[16] 2022 Annual Data Breach Report, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited December 29, 2023).

### *G. Defendants Failed to Comply with FTC Guidelines*

63. Defendants were also prohibited by the Federal Trade Commission Act ("FTCA") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.[17]

64. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[18]

65. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[19] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.

66. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

---

[17] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[18] *Start With Security: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited December 29, 2023).

[19] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited December 29, 2023).

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

68. Defendants failed to properly implement basic data security practices. Defendant's' failures to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

69. Defendants were fully aware of their obligations to protect the Private Information of Plaintiff and Class Members because of their positions as entities whose businesses center on contractual relationships with their clients and necessary collection, storage, and safeguarding of Private Information as a result of those contractual relationships. Defendants were also aware of the significant repercussions that would result from their failures to make good on those obligations.

### *H. Cyber Criminals Have and Will Continue to Use Plaintiff's and Class Members' Private Information for Nefarious Purposes*

70. Plaintiff's and Class Members' Private Information is of great value to cybercriminals, and the data stolen in the Data Breach can be used in a variety of ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature:

their one goal was to access Defendants' systems in order to obtain valuable Private Information to sell on the dark web.

71. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

72. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to personally identifiable information, they will use it.[20]

73. Cyber thieves may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.

74. If cyber criminals manage to access financial information, health insurance information, and other personally sensitive data using the Private Information compromised in the Data Breach, there is no limit to the amount of fraud to which Defendants may have exposed the Plaintiff and Class Members.

### *I. Plaintiff and Class Members Suffered Damages*

75. The ramifications of Defendants' failures to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen,

[20] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[21]

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

77. Defendants further owed and breached their duties to Plaintiff and Class Members to implement processes and specifications that would detect a breach of their security systems in a timely manner and to timely act upon warnings and alerts, including those generated by their own security systems.

78. As a direct result of Defendants' intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, cyber thieves were able to access, acquire, view, publicize, and/or otherwise cause the misuse and/or identity theft of Plaintiff's and Class Members' Private Information as detailed above, and Plaintiff and Class Members are now at a heightened risk of identity theft and fraud.

79. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because

[21] 2014 LexisNexis True Cost of Fraud Study, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

80. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

81. Plaintiff and Class Members did not receive the full benefit of the bargain for the received telecommunications services. As a result, Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value of the telecommunications services with data security protection they paid for and the services they received without the data security protection.

82. As a result of the Data Breach, Plaintiff's and Class Members' Private Information has diminished in value.

83. The Private Information belonging to Plaintiff and Class Members is private, private in nature, and was left inadequately protected by Defendants who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

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

85. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite their obligations to protect patient data.

86. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

87. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

88. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[22]

89. Defendants' failures to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Rather than assist those affected by the Data Breach, Defendants are putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

[22] Erika Harrell, & Lynn Langton, Victims of Identity Theft, 2012, U.S. DEP'T OF JUST., OFF. OF JUST. PROGRAMS BUREAU OF JUST. STATS. (Dec. 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

90. As a result of Defendants' failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

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

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

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from 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 identity theft and fraud;

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

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

f. Anxiety and distress resulting from fear of misuse of their Private Information.

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

## V. CLASS ACTION ALLEGATIONS

92. Plaintiff brings this class action on behalf of herself and all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

93. The Class that Plaintiff seeks to represent is defined as follows, subject to amendment as appropriate:

> **All individuals in the United States whose Private Information was compromised as a result of the data breach reported by Xfinity in December 2023.**

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

95. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

96. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendants have identified at least 35.8 million individuals whose Private Information may have been improperly accessed and compromised in the Data Breach.

97. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and when Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining Class Members' Private Information;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' Private Information;

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' Private Information;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Members' Private Information secure and prevent loss or misuse of that Private Information;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiff's and Class Members' damages;

i. Whether Defendants violated the law by failing to promptly notify Class Members that their Private Information had been compromised;

j. Whether Plaintiff and the other Class Members are entitled to actual damages, extended credit monitoring, and other monetary relief;

k. Whether Defendants violated common law and statutory claims alleged herein.

98. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members, because all had their Private Information compromised as a result of the Data Breach, due to Defendants' misfeasance.

99. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and making final injunctive relief appropriate with respect to the Class

as a whole. Defendants' policies challenged herein apply to and affect the Class uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

100. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

101. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

102. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendants would necessarily gain

an unconscionable advantage since Defendants would be able to exploit and overwhelm the limited resources of the Class with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

103. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

104. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

105. Unless a Class-wide injunction is issued, Plaintiff and Class Members remain at risk that Defendants will continue to fail to properly secure the Private Information of Plaintiff and Class Members resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Class Action Complaint.

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

107. 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 the following:

a. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

## VI. CLAIMS

### COUNT I
### Negligence
### (On Behalf of Plaintiff and the Class against both Defendants)

108. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

109. Plaintiff and Class Members were required to submit their Private Information to Defendants in order to receive telecommunications services.

110. Defendants knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiff and Class Members.

111. As described above, Defendants owed duties of care to Plaintiff and Class Members whose Private Information had been entrusted with Defendants.

112. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

113. Defendants acted with wanton disregard for the security of Plaintiff's and Class Members' Private Information. Defendants knew or reasonably should have known that they had inadequate data security practices to safeguard such information, and Defendants knew or reasonably should have known that data thieves were attempting to access databases containing PII, such as those of Defendants.

114. A "special relationship" exists between Defendants and Plaintiff and Class Members. Defendants entered into a "special relationship" with Plaintiff and Class Members because Defendants collected the Private Information of Plaintiff and the Class Members—information that Plaintiff and the Class Members were required to provide in order to receive the telecommunications services.

115. But for Defendants' wrongful and negligent breaches of the duties owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

116. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or reasonably should have known they were failing to meet their duties, and that Defendants' breaches of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

117. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT II**
**Negligence *Per Se***
**(On Behalf of Plaintiff and the Class against both Defendants)**

118. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

119. Pursuant to the FTCA (15 U.S.C. §45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

120. Defendants breached their duties to Plaintiff and Class Members under the FTCA (15 U.S.C. §45) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

121. Defendants' failures to comply with applicable laws and regulations constitutes negligence *per se*.

122. But for Defendants' wrongful and negligent breaches of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

123. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or reasonably should have known that they were failing to meet their duties, and that Defendants' breaches would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

124. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT III**
**Breach of Implied Contract**
**(On Behalf of Plaintiff and the Class against both Defendants)**

125. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

126. Plaintiff and Class Members entered into an implied contract with Defendants when they obtained telecommunications services in exchange for which they were required to provide their Private Information. The Private Information provided by Plaintiff and Class Members to Defendants was governed by and subject to Defendants' privacy duties and policies.

127. Defendants agreed to safeguard and protect the Private Information of Plaintiff and Class Members and to timely and accurately notify Plaintiff and Class Members in the event that their Private Information was breached or otherwise compromised.

128. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Defendants would use part of the monies paid to Defendants under the implied contracts to fund adequate and reasonable data security practices.

129. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract or implied terms between Plaintiff and Class Members and Defendants. The safeguarding of the Private Information of Plaintiff and Class Members and prompt and sufficient notification of a breach involving Private Information was critical to realize the intent of the parties.

130. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

131. Defendants breached their implied contracts with Plaintiff and Class Members to protect Plaintiff's and Class Members' Private Information when they: (1) failed to have security protocols and measures in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide sufficient notice that their Private Information was compromised as a result of the Data Breach.

132. As a direct and proximate result of Defendants' breaches of implied contract, Plaintiff and Class Members have suffered damages.

## COUNT IV
**Breach of Third-Party Beneficiary Contract**
**(On behalf of Plaintiff and the Class against Defendant Citrix)**

133. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

134. This Count is pleaded in the alternative to the breach of implied contract claim above (Count III).

135. Upon information and belief, Defendant Citrix entered into contracts with its clients, including Plaintiff's telecommunications service provider, Comcast, to provide software services—including data security practices, procedures, and protocols sufficient to safeguard the Private Information of Plaintiff and Class Members.

136. These contracts were made for the benefit of Plaintiff and Class Members given the transfer of their Private Information to Citrix for storage, protection, and safeguarding was the objective of the contracting parties. Therefore, Plaintiff and Class Members were direct and express beneficiaries of these contracts.

137. Defendant Citrix knew that a breach of these contracts with its clients would harm Plaintiff and Class Members.

138. Defendant Citrix breached the contracts with its clients when it failed to utilize adequate computer systems or data security practices to safeguard Plaintiff's and Class Members' Private Information.

139. Plaintiff and Class Members were harmed by Defendant Citrix's breaches in failing to use reasonable security measures to safely store and protect Plaintiff's and Class Members' Private Information.

140. Plaintiff and Class Members are therefore entitled to damages in an amount to be determined at trial.

## COUNT V
### Unjust Enrichment
### (On behalf of Plaintiff and the Class against both Defendants)

141. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

142. This Count is pleaded in the alternative to the breach of implied contract claim above (Count III) and the breach of third-party beneficiary claim above (Count IV).

143. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their Private Information—Private Information that has inherent value. In exchange, Plaintiff and Class Members should have been entitled to Defendants' adequate storage and safeguarding of their Private Information.

144. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

145. Defendants profited from Plaintiff's and Class Members' retained Private Information and used their Private Information for business purposes.

146. Defendants failed to store and safeguard Plaintiff's and Class Members' Private Information. Thus, Defendants did not fully compensate Plaintiff and Class Members for the value of their Private Information.

147. As a result of Defendants' failures, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the healthcare services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate healthcare services without reasonable data privacy and security practices and procedures that they received.

148. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement—or adequately implement—the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state and local laws, and industry standards.

149. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by Defendants.

150. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiff and Class Members.

## VII. PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the Class as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is the proper class representative; and appoint Plaintiff's Counsel as Class counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendants from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and members of the Class compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiff be granted the declaratory relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

Dated: January 3, 2024

Respectfully submitted,

*/s/ Jay Eng*

Jay Eng (FL. Bar No. 146676)
**BERMAN TABACCO**
Patrick T. Egan (*pro hac vice* forthcoming)
Christina L. Gregg (*pro hac vice* forthcoming)
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
jeng@bermantabacco.com
pegan@bermantabacco.com
cgregg@bermantabacco.com