UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

RAYMOND GOODROW, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CITRIX SYSTEMS, INC., and COMCAST CABLE COMMUNICATIONS, LLC d/b/a XFINITY,

Defendants.

Case No.: _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Raymond Goodrow ("Plaintiff"), by the undersigned counsel, files this Class Action Complaint, individually and on behalf of a class of all similarly situated persons, against Defendants 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 himself and his own acts, and on information and belief as to all other matters.

INTRODUCTION

1. Plaintiff and Class Members bring this class action against Defendants for their failures to adequately secure and protect the personally identifiable information ("PII") of Plaintiff and Class Members, including but not limited to names, mailing addresses, telephone numbers, dates of birth, partial Social Security numbers, usernames and encrypted passwords, as well as security question prompts and responses.

2. Citrix provides cloud computing services to over 16 million cloud users, and thousands of organizations. Its services include but are not limited to server technologies,

application and desktop virtualization, networking, software as a service (SaaS), and cloud computing technologies.

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

4. Comcast, as a substantial telecommunications and cable provider, and Citrix, as a substantial technology services company, both have the resources to take seriously the obligation to protect their customers' PII. However, Defendants failed to invest the time or resources necessary to protect the PII of Plaintiff and Class members.

5. 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 10, 2023 ("the Data Breach").

6. On October 10, 2023, Citrix announced the vulnerability in the software product used by Comcast and thousands of other companies, known as the "Citrix Bleed" vulnerability, which has been exploited by ransomware cybercriminals.[1]

7. 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' PII, data thieves were able to access and obtain the PII of Plaintiff and Class Members on or around October 10, 2023.

[1] What Is Citrix Bleed? The Next Ransomware Patch You Need, Government Technology (Dec. 6, 2023), https://www.govtech.com/security/what-is-citrix-bleed-the-next-ransomware-patch-you-need (last visited January 17, 2024).

8. On December 18, 2023, Comcast posted a copy of its Notice of Data Security Incident to its website.[2]

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

10. 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.

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

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

13. Defendants breached their duties by negligently and recklessly maintaining the PII of Plaintiff and Class Members. It is believed that the means of the data breach and the risk of improper disclosure were known and foreseeable to the Defendants. Their failure to secure the PII left it in a dangerous and vulnerable state.

14. Defendants also neglected proper monitoring of the computer network and systems containing the PII. Adequate monitoring could have detected the intrusion sooner or prevented it

[2] *Notice to Customers of Data Security Incident*, available at https://assets.xfinity.com/assets/dotcom/learn/_Data_Incident.pdf (last visited January 17, 2024).

altogether. This negligence has heightened the risk of exposure for Plaintiff and Class Members, as their identities are now in the hands of data thieves due to Defendants' actions.

15. Defendants neglected to provide sufficient notice of unauthorized access to the PII by a cyber attacker and failed to specify the information accessed and stolen.

16. Data thieves can potentially use the accessed PII to commit various crimes, including fraud, opening financial accounts, obtaining loans, filing fraudulent tax returns, and providing false information during arrests.

17. As a result of the Data Breach, Plaintiff and Class Members have suffered and continue to face a heightened and imminent risk of fraud and identity theft, requiring constant monitoring of their financial accounts.

18. As a result of the Data Breach, Plaintiff and Class Members have 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.

19. The invasion of property interest in their PII entitles Plaintiff and Class Members to damages from Defendants. These harms are ongoing, and future damages are expected as thieves continue to misuse the information for several years. To protect themselves, Plaintiff and Class Members may incur out-of-pocket costs for credit monitoring services, credit freezes, credit reports, and other protective measures.

20. Plaintiff seeks to address these issues on behalf of all similarly situated individuals affected by the Data Breach.

PARTIES

21. Plaintiff Raymond Goodrow ("Mr. Goodrow") is a resident of South Deerfield, Massachusetts, and a citizen of Massachusetts. Mr. Goodrow has been a customer of Xfinity since 2020.

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

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

JURISDICTION AND VENUE

24. 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.

25. 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.

26. 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.

FACTUAL BACKGROUND

A. Defendant Citrix's Business

27. Established in 1989, Citrix is a global cloud computing company offering technology services to numerous organizations. Its diverse range of services includes server technologies, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing technologies. Citrix boasts a substantial client base, with claims of serving over 16 million cloud users.

28. With a widespread client portfolio, Citrix caters to thousands of companies globally.[3] In the United States, it services extend across various sectors such as education, energy and utility, financial services, government and public sector, healthcare, insurance, manufacturing, childcare, professional services, retail, technology, telecommunications, and transportation.[4] Through contracts with these clients, Citrix accumulates and stores the PII of millions of individuals in its databases.

29. According to the company, Citrix's digital workspace solutions are relied upon by more than 400,000 companies worldwide, including 99 percent of the Fortune 500.[5]

B. Defendant Comcast's Business

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

31. Comcast is an American telecommunications business, which provides a spectrum of consumer products and services, including cable television, internet services, telephone, and wireless services.

---

[3] Citrix Customer stories, available at https://www.citrix.com/customers/ (last visited January 17, 2024).
[4] *Id.*
[5] Citrix Named to Cloud 500 (Mar. 1, 2022), available at https://www.citrix.com/news/announcements/mar-2022/citrix-named-to-cloud-500.html (last visited January 17, 2024).

32. Comcast divides its business into two segments: Connectivity & Platforms and Content & Experiences.[6] 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.[7] 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.[8] Comcast generates revenue from the customers who subscribe to these services and the sale of related devices.[9]

33. According to a 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.[10]

C. Defendants' Businesses Hinge Significantly on the Aggregation of PII Belonging to Plaintiff and Class Members

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

35. Through the possession and utilization of Plaintiff's and Class Members' PII, Defendants assumed duties owed to Plaintiff and Class Members regarding their PII. Therefore, Defendants knew or should have known that they were responsible for safeguarding Plaintiff's and Class Members' PII from unauthorized access and criminal misuse.

36. 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

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

the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain."[11]

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

D. The Data Breach

38. 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."[12] Security researchers dubbed the vulnerability as critical in nature.[13]

39. 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.

40. 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 PII of Plaintiff and Class Members. Comcast purports to have launched an investigation into the Data Breach.

---

[11] Our Privacy Policy, Xfinity, available at https://www.xfinity.com/privacy/policy (last visited January 17, 2024).
[12] *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/ (last visited January 17, 2024).
[13] *Id.*

41. 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.

42. 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.[14]

43. 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.

E. Plaintiff's Experiences Following the Data Breach

44. Plaintiff Raymond Goodrow ("Mr. Goodrow") was a customer of Comcast at the time of the Data Breach.

45. Mr. Goodrow was required to provide Comcast with his PII as a condition of receiving telecommunications services.

[14] 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 (last visited January 17, 2024).

46. As a result of the Data Breach, Mr. Goodrow has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Mr. Goodrow otherwise would have spent performing other activities, such as his job, and/or leisurely activities for the enjoyment of life.

47. As a result of the Data Breach, Mr. Goodrow has suffered emotional distress as a result of the release of his PII which he expected Defendants to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing, and potentially using his PII.

48. As a result of the Data Breach, Mr. Goodrow 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 were Aware or Should Have Been Aware of Both the Value of PII and the Associated Risk of Cyberattacks for those in Possession of such PII.

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

50. PII 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.[15] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground websites, commonly referred to as the dark web.

51. 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.[16] In 2022, 1,802

[15] What to Know About Identify Theft, Fed. Trade Comm'n, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited January 17, 2024).
[16] Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource

data compromises were reported that impacted over 422 million victims—marking a 42% increase in the number of victims impacted since 2021.[17] That upward trend continues.

52. The ramifications of Defendants' failures to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII 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.

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

54. 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.

55. 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' PII 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.

Center and CyberScout, CISION PR NEWSWIRE (Jan. 19, 2017) 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 (last visited January 17, 2024).

[17] 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 January 17, 2024)

G. Defendants Failed to Comply with FTC Guidelines

56. 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.[18]

57. 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.[19]

58. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[20] 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.

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

[18] *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).
[19] 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 January 17, 2024).
[20] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N, *available at* https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last visited January 17, 2024).

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

60. 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.

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

62. Defendants were fully aware of their obligations to protect the PII 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 PII 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.

63. Despite their obligations, Defendants failed to properly implement basic data security practices, and Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to the PII of Plaintiff and Class Members constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

H. Cybercriminals have Accessed and are Likely to Persist in Using the PII of Plaintiff and Class Members for Illicit Activities

64. Plaintiff's and Class Members' PII is of immense 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:

65. PII 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.

66. 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.[21]

67. 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 [Dark] 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."[22]

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

I. Plaintiff and Class Members Suffered Damages

69. For the aforementioned reasons, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways.

70. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2)

[21] Ari Lazarus, How fast will identity thieves use stolen info?, FED. TRADE COMM'N (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last visited January 17, 2024).
[22] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, DATA BREACHES & IDENTITY THEFT (2007).

change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

71. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct. Further, the value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach.

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

73. 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.

74. 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'

PII as detailed above, and Plaintiff and Class Members are now at a heightened risk of identity theft and fraud.

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

76. 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.

77. 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.

78. As a result of the Data Breach, Plaintiff's and Class Members' PII has diminished in value.

79. The PII 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 PII to any other person as required by applicable law and industry standards.

80. The Data Breach was a direct and proximate result of Defendants' failures to: (a) properly safeguard and protect Plaintiff's and Class Members' PII 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' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

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

82. 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' PII.

83. 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.

84. 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."[23]

85. Defendants' failures to adequately protect Plaintiff's and Class Members' PII 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.

[23] 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://bjs.ojp.gov/content/pub/pdf/vit12.pdf (last visited January 17, 2024).

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.

86. 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 PII;

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 PII, 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 PII 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 PII.

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

CLASS ACTION ALLEGATIONS

88. Plaintiff brings claims on behalf of himself, and for certain claims, on behalf of the proposed class of:

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

89. The following people are excluded from the class: (1) any Judge or Magistrate Judge presiding over this action and the members of their family; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or its parents have a controlling interest and their current employees, officers, and directors; (3) persons who properly execute and file a timely request for exclusion from the class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel, and their experts and consultants; and (6) the legal representatives, successors, and assigns of any such excluded persons.

90. ***Numerosity*:** The proposed class contains members so numerous that separate joinder of each member of the class is impractical. Defendants have identified at least 35.8 million individuals whose PII may have been improperly accessed and compromised in the Data Breach.

91. ***Commonality*:** There are questions of law and fact common to the proposed class. Common questions of law and fact include, without limitation:

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' PII;

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' PII;

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

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

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 PII 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.

92. ***Typicality*:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of Plaintiff and Class Members are based on the same legal theories and arise from the same unlawful and willful conduct because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

93. ***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.

94. ***Adequacy of Representation*:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained

counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

95. ***Superiority*:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

96. ***Predominance***: Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

97. ***Injunctive Relief***: Defendants has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

98. ***Ascertainability***: Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class against both Defendants)

99. Plaintiff incorporates by reference paragraphs 1 through 98 as though fully set forth herein.

100. Plaintiff and Class Members were required to submit their PII to Defendants in order to receive telecommunications services.

101. Defendants knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiff and Class Members.

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

103. 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' PII.

104. Defendants acted with wanton disregard for the security of Plaintiff's and Class Members' PII. 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.

105. 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 PII of Plaintiff and the Class Members—information that

Plaintiff and the Class Members were required to provide in order to receive the telecommunications services.

106. 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.

107. 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 PII.

108. 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.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class against both Defendants)

109. Plaintiff incorporates by reference paragraphs 1 through 98 as though fully set forth herein.

110. 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' PII.

111. 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' PII.

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

113. 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.

114. 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 PII.

115. 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.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class against both Defendants)

116. Plaintiff incorporates by reference paragraphs 1 through 98 as though fully set forth herein.

117. 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 PII. The PII provided by Plaintiff and Class Members to Defendants was governed by and subject to Defendants' privacy duties and policies.

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

119. 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.

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

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

122. Defendants breached their implied contracts with Plaintiff and Class Members to protect Plaintiff's and Class Members' PII 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 PII was compromised as a result of the Data Breach.

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

FOURTH CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and the Class against Defendant Citrix)

124. Plaintiff incorporates by reference paragraphs 1 through 98 as though fully set forth herein.

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

126. 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 PII of Plaintiff and Class Members.

127. These contracts were made for the benefit of Plaintiff and Class Members given the transfer of their PII 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.

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

129. 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' PII.

130. 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' PII.

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

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class against both Defendants)

132. Plaintiff incorporates by reference paragraphs 1 through 98 as though fully set forth herein.

133. 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).

134. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their PII—PII that has inherent value. In exchange,

Plaintiff and Class Members should have been entitled to Defendants' adequate storage and safeguarding of their PII.

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

136. Defendants profited from Plaintiff's and Class Members' retained PII and used their PII for business purposes.

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

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

139. 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.

140. 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.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is hereby demanded for all claims so triable.

Dated: January 17, 2024

Respectfully submitted,

By: /s/ *Jeff Ostrow*

Jeff Ostrow (Fla. Bar No. 121452)
Steven Sukert (Fla. Bar No. 1022912)
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Ft. Lauderdale, Florida 33301
Telephone No.: (954) 525-4100
ostrow@kolawyers.com
sukert@kolawyers.com

Alan M. Feldman*
Zachary Arbitman*
Samuel Mukiibi*
FELDMAN SHEPHERD WOHLGELERNTER

TANNER WEINSTOCK & DODIG, LLP
1845 Walnut Street, 21st Floor
Philadelphia, PA 19103
T: (215) 567-8300
F: (215) 567-8333
afeldman@feldmanshepherd.com
zarbitman@feldmanshepherd.com
smukiibi@feldmanshepherd.com

*Application for *Pro Hac Vice* Admission
To Be Submitted

Attorneys for Plaintiff and the Class