IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

KENNETH HASSON et al., individually and on behalf of all others similarly situated, Plaintiffs, v. COMCAST CABLE COMMUNICATIONS LLC, COMCAST CORPORATION, and CITRIX SYSTEMS, INC., Defendants. This Document Relates to: All Actions	Master File No. 2:23-cv-05039-JMY **JURY TRIAL DEMANDED** **CONSOLIDATED COMPLAINT-CLASS ACTION**

CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. PARTIES 4

A. Plaintiffs 4

1. Patricia Andros (Pa.) 4

2. Michelle Birnie (Fla.) 7

3. Jessica Carey (Mass.) 10

4. Jessica Durham (Ill.) 13

5. Vince Estevez (Tex.) 16

6. Danielle Hendrickson (Del.) 21

7. Alyssia Nanez (Cal.) 23

8. Alexander Nunn (Tenn.) 26

9. Steven Prescott (Cal.) 29

10. Robert H. Smith (Ohio) 31

11. Veronica Verdier (N.J.) 34

12. Laura Wiley (Ill.) 37

13. Marcia P. Wilson (Pa.) 39

14. Jodi Wolfson (N.J.) 42

B. Defendants 44

III. JURISDICTION AND VENUE 45

IV. STATEMENT OF FACTS 47

A. Comcast Obtains, Collects, and Stores Plaintiffs' and Class Members' Private, Personally Identifiable Information. 47

B. Comcast Knows the Risk of Storing PII and Promises to Keep Customers' PII Secure. 49

C. Comcast Engaged Citrix to Improve its Systems' Data Security and Safeguard the PII in its Possession and Control. 53

D. Defendants' Legal Responsibility to Safeguard Information. 56

E. Defendants Knew the Risks of Collecting and Storing Valuable PII and the Foreseeable Harms of Exposing PII to Cybercriminals. 58

F. Despite Their Duties and the Foreseeable Risk of Harm, Comcast and Citrix Failed to Protect Plaintiffs' and Class Members' PII. 67

G. Comcast Admits It Failed to Protect Plaintiffs' PII and Compounded Its Failure by Providing Inadequate Notice to Those Impacted. 71

H. Defendants Failed to Comply with Industry Standards and Regulatory Guidance Regarding Data Security Practices. 72

I. The Data Breach Put Xfinity Customers at Imminent and Substantial Risk of Fraud, Identity Theft, and Other Cybercrimes. 77

V. PLAINTIFFS' AND CLASS MEMBERS' INJURIES AND DAMAGES 81

VI. CLASS ACTION ALLEGATIONS 85

VII. CAUSES OF ACTION 89

A. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS 90

B. CLAIMS ON BEHALF OF THE STATE SUBCLASSES 115

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS 115

CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS 125

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS 129

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS 132

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS 138

CLAIMS ON BEHALF OF THE OHIO SUBCLASS 141

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS 143

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS 145

VIII. REQUEST FOR RELIEF 149

IX. JURY TRIAL DEMAND 152

The named Plaintiffs identified in Part II below ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint against Defendants Comcast Corporation and Comcast Cable Communications, LLC (collectively, "Comcast") and Citrix Systems, Inc. ("Citrix," and collectively with Comcast, "Defendants"), seeking monetary damages, restitution, and injunctive relief arising from a data breach that resulted in the theft of Plaintiffs' highly sensitive personal information. Plaintiffs make the following allegations upon personal knowledge and on information and belief derived from, among other things, investigation of their counsel, a review of public documents, and other facts that are a matter of public record.

I. INTRODUCTION

1. Comcast is one of the largest companies in the telecommunications sector and provides internet services and products, cable television, a mobile 5G network, and landline telephone services and products to individuals and businesses across the United States under the brand name Xfinity. To obtain any of these Xfinity services, customers are required to entrust Comcast with their PII, which Comcast uses to engage in its usual business activities. Comcast understands that it has an enormous responsibility to protect the data it collected, assuring its customers that "Your Data Privacy is Our Top Priority."[1] Despite this assurance to its customers, however, Comcast failed to protect the very customer information it was entrusted, leading to a data breach of Comcast's systems that stemmed from a vulnerability in Citrix-managed software and appliances that Comcast utilized and failed to timely patch, compromising the personal information of approximately 36 million people.

[1] *2022 Xfinity Cyber Health Report*, Comcast (2022), https://update.comcast.com/wp-content/uploads/sites/33/dlm_uploads/2022/12/2022-Xfinity-Cyber-Health-Report-12.13.22-5pm-reduced.pdf at 17.

2. Citrix is one of the largest companies in the office technology sector and provides an array of business technology services, including server, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing services to hundreds of thousands of clients worldwide. Comcast contracted with Citrix to provide a variety of networking hardware and software services, including the use of Citrix NetScaler ADC and NetScaler Gateway (the "NetScaler products").

3. Together, Defendants Comcast and Citrix failed to properly secure and safeguard the highly valuable, personally identifiable information of approximately 36 million Comcast customers, including customers' usernames and hashed passwords, names, contact information, last four digits of Social Security numbers, dates of birth, and secret security questions and answers (collectively, "PII"), failed to comply with industry standards to protect information systems that contain PII, and failed to provide adequate notice to Plaintiffs and other members of the Class that their PII had been accessed and compromised.

4. Defendants are well-aware of the foreseeable risks of implementing inadequate data security measures, as some of the largest data breaches of the past year have resulted from vulnerabilities in third-party products, including the MOVEit Transfer and GoAnyWhere MFT data breaches. Despite this foreseeability, Defendants failed to implement adequate data security measures. On October 10, 2023, Citrix announced that it had discovered multiple critical vulnerabilities in its Citrix NetScaler products, which became widely known among cybersecurity commentators as the "CitrixBleed" vulnerability. As part of the announcement, Citrix released a security patch that customers could implement to eliminate the CitrixBleed vulnerability and prevent unauthorized access to customers' systems that contain PII.

5. Comcast failed to timely install the security patch in its Citrix NetScaler products, and as a result, between October 16 and October 19, 2023, cybercriminals exploited the vulnerabilities, accessed Comcast's internal systems, and accessed the PII of approximately 36 million Xfinity customers (the "Data Breach" or "Breach" herein).

6. Citrix is equally blameworthy. Despite earlier known exploits of its products' vulnerability at other companies, Citrix did not reveal the vulnerability to Comcast until two months later. And when it did finally reveal the vulnerability in October 2023, Citrix downplayed the severity of the vulnerability. It was not until two weeks later that Citrix revealed the true magnitude of the vulnerability. But by then, the damage was done.

7. As a direct and proximate result of Comcast's failure to follow industry-standard practices to secure and protect the information, timely implement the security patch and follow basic security procedures, and as a direct and proximate result of Citrix's failure to adequately test the security of its widely-used network products before selling those products to customers like Comcast who foreseeably used those products to handle sensitive PII, and as a direct and proximate result of Citrix's failure to timely disclose vulnerabilities in its products, Plaintiffs' and Class Members' PII is now in the hands of cybercriminals.

8. As a result of Defendants' conduct, Plaintiff and Class Members now face an imminent and substantial risk of fraud, identity theft, and other harms caused by the unauthorized disclosure of their PII—risks which may last for the rest of their lives. Indeed, several Plaintiffs have already experienced incidents of fraud and identity theft. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Comcast's and Citrix's unlawful and tortiously deficient data security practices have injured millions of consumers, and Plaintiffs and putative Class Members in this action therefore bring claims for negligence, negligence *per se*, breach of express and implied contract, unjust enrichment, and an array of state and federal statutory claims, seeking damages, declaratory relief, and injunctive relief.

II. PARTIES

10. Plaintiffs identified below bring this action on behalf of themselves and those similarly situated in a representative capacity for individuals across the United States.

A. Plaintiffs

1. Patricia Andros (Pa.)

11. Plaintiff Patricia Andros is an adult individual and a natural person of Pennsylvania, residing in Allegheny County, where she intends to stay, and therefore is a citizen of Pennsylvania. Plaintiff Andros received a notification from Comcast when she logged into her Comcast account on or about December 21, 2023, informing her of the Data Breach and the exposure of her PII. The notice letter informed Plaintiff Andros that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

12. Plaintiff Andros only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Andros entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its

vendors at the time of the Data Breach. Had Plaintiff Andros been informed of Comcast's and Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

13. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Andros suffered injury from a loss of privacy.

14. As a result of the Data Breach, Plaintiff Andros has been further injured by the damages to and loss in value of her PII—a form of intangible property that Plaintiff Andros entrusted to Defendants. This information has inherent value that Plaintiff Andros was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

15. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Andros to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

16. Upon information and belief, Plaintiff Andros's PII has already been stolen and misused, as she has experienced multiple incidents of fraud and identity theft. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Andros's life, specifically by making fraudulent charges on her debit card that she used to make payments to Comcast. Plaintiff Andros had to cancel her debit card and wait until ten days later to receive a new debit card, rendering her unable to pay bills during that ten-day period.

17. Furthermore, Plaintiff Andros has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach, and has had to spend a significant amount of time blocking numerous numbers and messages.

18. As a result of the actual harm Plaintiff Andros has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Andros to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, replacing her debit card and adding a monitoring service to every transaction on her debit card, spending time traveling to her bank after she froze her debit card to meet with representatives to dispute fraudulent charges, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, resetting automatic billing instructions and payment account information, and resetting her passwords. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

19. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Andros to suffer stress, fear, emotional distress, and anxiety.

20. Comcast acknowledged the risk posed to Plaintiff Andros and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Andros to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Andros to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[2]

[2] *Notice To Customers of Data Security Incident*, Xfinity, https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (last visited July 1, 2024).

21. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[3]

22. Plaintiff Andros has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

2. Michelle Birnie (Fla.)

23. Plaintiff Michelle Birnie is an adult individual and a natural person of Florida, residing in Monroe County, where she intends to stay, and therefore is a citizen of Florida. Plaintiff Birnie received a notice letter from Comcast on or about January 4, 2024, informing her of the Data Breach and the exposure of her PII. The notice letter informed Plaintiff Birnie that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

24. Plaintiff Birnie only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any

[3] *NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967*, Citrix, https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967 (last modified Nov. 27, 2023) (hereinafter "CitrixBleed Security Bulletin").

data security vulnerabilities. As a result of this expectation, Plaintiff Birnie entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Birnie been informed of Comcast's and Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

25. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Birnie suffered injury from a loss of privacy.

26. As a result of the Data Breach, Plaintiff Birnie has been further injured by the damages to and loss in value of her PII—a form of intangible property that Plaintiff Birnie entrusted to Defendants. This information has inherent value that Plaintiff Birnie was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

27. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Birnie to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

28. Upon information and belief, Plaintiff Birnie's PII has already been stolen and misused as she has experienced incidents of fraud and identity theft. On the same day that she received an alert from Comcast to change her passwords (December 29, 2023), an unauthorized person(s) attempted to purchase flights from Kuala Lumpur for $432.00 on three different booking websites using her debit card information. Plaintiff Birnie had to spend time resolving the issue,

including canceling and changing her debit card. While she was on the phone with her bank, she received numerous login attempt notifications for her Amazon account about every two minutes. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Birnie's life, specifically by subjecting Plaintiff Birnie to financial fraud and by forcing Plaintiff Birnie to change all of her passwords, including for her Comcast, Amazon, and financial accounts.

29. Furthermore, Plaintiff Birnie has experienced a substantial increase in daily spam emails, texts, and phone calls following the Data Breach.

30. As a result of the actual harm Plaintiff Birnie has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Birnie to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, self-monitoring accounts, addressing the fraudulent efforts to use her personal information, replacing credit and debit cards, resetting passwords, etc. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

31. As a result of the actual harm Plaintiff Birnie has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has also forced Plaintiff to spend money on an array of mitigation measures, such as $16 for a replacement special photo on her debit card; and $10 for gas for driving to and from the bank to resolve the fraudulent charges. Plaintiff will be required to maintain this heightened vigilance and incur the expenses of these mitigation measures well into the future.

32. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Birnie to suffer stress, fear, emotional distress, and anxiety.

33. Comcast acknowledged the risk posed to Plaintiff Birnie and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Birnie to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Birnie to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[4]

34. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed." [5]

35. Plaintiff Birnie has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

3. Jessica Carey (Mass.)

36. Plaintiff Jessica Carey is an adult individual and a natural person of Massachusetts, residing in Essex County, where she intends to stay, and therefore is a citizen of Massachusetts. Plaintiff Carey received a notification from Comcast when she logged into her Xfinity account on or about December 21, 2023, informing her of the Data Breach and the potential exposure of her PII. The notification combined with the notice letter Comcast later posted on its website informed Plaintiff Carey that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

[4] *Notice To Customers of Data Security Incident*, *supra* note 2.
[5] CitrixBleed Security Bulletin, *supra* note 3.

37. Plaintiff Carey only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Carey entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Carey been informed of Comcast's and Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

38. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Carey suffered injury from a loss of privacy.

39. As a result of the Data Breach, Plaintiff Carey has been further injured by the damages to and loss in value of her PII—a form of intangible property that Plaintiff Carey entrusted to Defendants. This information has inherent value that Plaintiff Carey was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

40. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Carey to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

41. Upon information and belief, Plaintiff Carey's PII has already been stolen and misused. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Carey's life.

42. As a result of the actual harm Plaintiff Carey has suffered due to the Data Breach and the imminent and substantial risk of future harm, Plaintiff Carey has spent significant time and energy dealing with issues related to the Data Breach, including: time spent researching the Data Breach, such as verifying the breach by logging into her Comcast account; reconfiguring her Comcast account with a two-step verification process; constantly monitoring her accounts for suspicious and fraudulent activity; and contacting a lawyer. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

43. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Carey to suffer stress, fear, emotional distress, and anxiety.

44. Comcast acknowledged the risk posed to Plaintiff Carey and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Carey to enroll in two-factor or multi-factor authentication for her Comcast account, and directing Plaintiff Carey to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[6]

45. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as

[6] *Notice To Customers of Data Security Incident*, *supra* note 2.

soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[7]

46. Plaintiff Carey has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

4. Jessica Durham (Ill.)

47. Plaintiff Jessica Durham is an adult individual and a natural person of Illinois, residing in Lake County, where she intends to stay, and therefore is a citizen of Illinois. Plaintiff Durham received a notice letter from Comcast on or about December 22, 2023, informing her of the Data Breach and the exposure of her PII. The notice letter informed Plaintiff Durham that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

48. Plaintiff Durham only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Durham entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Durham been informed of Comcast's and

[7] CitrixBleed Security Bulletin, *supra* note 3.

Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

49. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Durham suffered injury from a loss of privacy.

50. As a result of the Data Breach, Plaintiff Durham has been further injured by the damages to and loss in value of her PII-a form of intangible property that Plaintiff Durham entrusted to Defendants. This information has inherent value that Plaintiff Durham was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

51. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Durham to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

52. Upon information and belief, Plaintiff Durham's PII has already been stolen and misused as she has experienced incidents of fraud and identity theft. After the Data Breach, a nefarious actor went to Western Union and was able to generate a cashier's check that pulled money from her bank account with U.S. Bank, and the cashier's check cleared before Plaintiff Durham could discover the fraudulent activity. A nefarious actor also called U.S. Bank pretending to be Plaintiff Durham, and successfully got the bank to change the listed address for her accounts. When Plaintiff Durham called U.S. Bank's fraud line about suspicious activity, the U.S. Bank fraud employee noticed that someone was actively trying to move money around in her account

during the call. To prevent further fraud, Plaintiff Durham had to close her checking and savings accounts with U.S. Bank and was required to wait two weeks before opening new accounts and obtaining a new debit card. During this period, Plaintiff Durham had no access to any of her money, which was particularly straining as it occurred near Christmas, and Plaintiff Durham has two young children for whom she needed to purchase Christmas gifts. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Durham's life.

53. Furthermore, Plaintiff Durham has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach, and has had to spend a significant amount of time blocking numerous numbers and messages.

54. As a result of the actual harm Plaintiff Durham has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Durham to spend significant time and energy dealing with issues related to the Data Breach. Upon learning about the fraud to her checking and savings accounts, Plaintiff Durham called the Attorney General's Office of the State of Illinois to report the fraud. Plaintiff Durham also called the Lake County Sheriff's Office to make a police report regarding the fraud to her accounts. Plaintiff Durham was also required to travel to U.S. Bank and meet with the bank's fraud department in person so they could confirm her identity. Plaintiff Durham has spent time verifying the legitimacy of the Data Breach Notice Letter, self-monitoring her accounts and credit reports for fraudulent activity, resetting automatic billing instructions on all her accounts, and resetting passwords. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

55. Plaintiff will be required to maintain this heightened vigilance into the future.

56. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Durham to suffer stress, fear, emotional distress, and anxiety.

57. Comcast acknowledged the risk posed to Plaintiff Durham and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Durham to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Durham to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[8]

58. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[9]

59. Plaintiff Durham has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

5. Vince Estevez (Tex.)

60. Plaintiff Vince Estevez is an adult individual and a natural person of Texas, residing in Brazoria County, where he intends to stay, and therefore is a citizen of Texas. Plaintiff Vince Estevez received notice from Comcast on or about December 19, 2023, when he called Comcast about a suspicious phone call he had received regarding his Comcast services and an automated message played about the Data Breach. He later viewed the Notice Letter from Comcast's website informing him of the Data Breach and the exposure of his PII. The automated message and the

[8] *Notice To Customers of Data Security Incident*, *supra* note 2.
[9] CitrixBleed Security Bulletin, *supra* note 3.

notice letter informed Plaintiff Vince Estevez that his name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

61. Plaintiff Estevez only allowed Comcast and its vendors, including Citrix, to maintain, store, and use his PII because he reasonably expected that Defendants would use basic security measures to protect his PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing his PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Estevez entrusted his PII to Comcast and its vendors, and his PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Estevez been informed of Comcast's and Citrix's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Defendants.

62. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Estevez suffered injury from a loss of privacy.

63. As a result of the Data Breach, Plaintiff Estevez has been further injured by the damages to and loss in value of his PII—a form of intangible property that Plaintiff Estevez entrusted to Defendants. This information has inherent value that Plaintiff Estevez was deprived of when his PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

64. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Estevez to suffer imminent harm arising from a substantially increased risk of additional fraud, identity

theft, financial crimes, and misuse of his PII. This highly sensitive information, which includes his name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

65. Upon information and belief, Plaintiff Estevez's PII has already been stolen and misused as he has experienced incidents of fraud and identity theft. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Estevez's life, specifically as a result of identity theft, including theft of his phone number, banking issues and attempts to open new credit card accounts in his name.

66. For example, on December 19, 2023, a person claiming to be a representative of Xfinity called Plaintiff Estevez to reportedly check on his services provided by Xfinity. Plaintiff Estevez was suspicious about the call, so he hung up and called Xfinity directly to ask whether someone from Xfinity had actually made the call to check on his services. Before reaching a representative, Xfinity provided an automated message notifying customers about the recent Data Breach. Plaintiff Estevez registered the warning and then asked the representative whether Xfinity calls to check on its customers. The representative informed Plaintiff Estevez that Xfinity does occasionally call on its customers to check on their services and told Plaintiff Estevez there was no reason for concern. About a half an hour later, Plaintiff Estevez received another call from a different person but again claiming to be a representative from Xfinity. That person asked Plaintiff Estevez to read out a six-digit code on his phone to confirm his connection, but only ten minutes after his providing that code information, Plaintiff Estevez's Xfinity-serviced cell phone was dead, his number had been stolen, and he soon learned that his account had been disconnected.

67. The next day, December 20, 2023, Plaintiff Estevez received an email from Chase Bank notifying him of three different requests to wire money out of his accounts. Plaintiff

Estevez's Chase account was accessible through Plaintiff Estevez's Xfinity-serviced cell phone that had been hacked the day before, as the Chase account was tied to an auto-pay function on Plaintiff Estevez's Xfinity account. Chase Bank reported that the first attempt, a $5,000 wire transfer, had successfully gone through, and pulled money from Estevez's linked PenFed Credit Union account. Chase Bank caught the next two wires and reported that it stopped those further transfers. Estevez soon learned, however, that a subsequent fraudulent wire transfer for $4,000 went out from his PenFed account. Estevez was ultimately refunded for the fraudulent wires.

68. On or about December 21, 2023, hackers accessed $18,000 from Plaintiff Estevez's Bank of America credit card account, which Bank of America later confirmed was fraudulent. Hackers also soon thereafter attempted to apply for new credit cards in Plaintiff Estevez's wife's name at Capital One. Fortunately, Plaintiff Estevez was able to stop that attempt after Capital One contacted him to ask for his and his wife's driver's license numbers.

69. As a result of the actual harm Plaintiff Estevez has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Estevez to spend significant time and energy dealing with issues related to the Data Breach and its aftermath, including forty to fifty hours responding to the Data Breach. Plaintiff Estevez spent much of that time dealing with fraudulent attempts to obtain access to accounts, transfer funds, and open new accounts. Plaintiff Estevez also spent hours changing passwords across his accounts, replacing credit and debit cards, closing accounts, and setting up new forms of payment for services he receives. Plaintiff Estevez also met with police, filed a police report, and investigated ways to further protect himself and his wife from additional fraud and damages. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

70. As a result of the actual harm Plaintiff Estevez has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has also forced Plaintiff to spend money on an array of mitigation measures, such as paying for identity monitoring services through Aura at a cost of $440 per year. Plaintiff Estevez will be required to maintain this heightened vigilance and incur the expense of these mitigation measures well into the future.

71. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Estevez to suffer stress, fear, emotional distress, and anxiety.

72. Comcast acknowledged the risk posed to Plaintiff Estevez and his PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Estevez to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Estevez to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[10]

73. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[11]

74. Plaintiff Estevez has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

[10] *Notice To Customers of Data Security Incident*, *supra* note 2.
[11] CitrixBleed Security Bulletin, *supra* note 3.

6. Danielle Hendrickson (Del.)

75. Plaintiff Danielle Hendrickson is an adult individual and a natural person of Delaware, residing in Kent County, where she intends to stay, and therefore is a citizen of Delaware. Plaintiff Hendrickson received a notice letter from Comcast on or about December 20, 2023, informing her of the Data Breach and the exposure of her PII. The notice letter informed Plaintiff Hendrickson that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

76. Plaintiff Hendrickson only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Hendrickson entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Hendrickson been informed of Comcast's and Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

77. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Hendrickson suffered injury from a loss of privacy.

78. As a result of the Data Breach, Plaintiff Hendrickson has been further injured by the damages to and loss in value of her PII—a form of intangible property that Plaintiff Hendrickson entrusted to Defendants. This information has inherent value that Plaintiff

Hendrickson was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

79. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Hendrickson to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

80. Upon information and belief, Plaintiff Hendrickson's PII has already been stolen and misused.

81. Plaintiff Hendrickson has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach. Plaintiff Hendrickson has had to spend a significant amount of time deleting texts and blocking numerous numbers and incoming messages.

82. As a result of the actual harm Plaintiff Hendrickson has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Hendrickson to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, and resetting her passwords. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

83. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Hendrickson to suffer stress, fear, emotional distress, and anxiety.

84. Comcast acknowledged the risk posed to Plaintiff Hendrickson and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Hendrickson to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Hendrickson to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[12]

85. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[13]

86. Plaintiff Hendrickson has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

7. Alyssia Nanez (Cal.)

87. Plaintiff Alyssia Nanez is an adult individual and a natural person of California, residing in San Joaquin County, where she intends to stay, and therefore is a citizen of California. Plaintiff Nanez received a notice letter from Comcast on or about December 20, 2023, informing her of the Data Breach and the exposure of her PII. The notice letter informed Plaintiff Nanez that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

[12] *Notice To Customers of Data Security Incident*, *supra* note 2.
[13] CitrixBleed Security Bulletin, *supra* note 3.

88. Plaintiff Nanez only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Nanez entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Nanez been informed of Comcast's and Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

89. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Nanez suffered injury from a loss of privacy.

90. As a result of the Data Breach, Plaintiff Nanez has been further injured by the damages to and loss in value of her PII—a form of intangible property that Plaintiff Nanez entrusted to Defendants. This information has inherent value that Plaintiff Nanez was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

91. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Nanez to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

92. Upon information and belief, Plaintiff Nanez's PII has already been stolen and misused. Unauthorized criminal third parties have detrimentally impacted Plaintiff Nanez's life, specifically by making attempts to hack into her Roblox account. After the Data Breach, Plaintiff Nanez received notifications that a nefarious actor was trying to hack into her Roblox account which she has loaded onto her iPhone so she can monitor her son's use of Roblox. This was particularly troubling to Plaintiff Nanez because that meant the nefarious actor was trying and could access her son's Roblox account on his iPhone with her credentials. Plaintiff Nanez contacted Roblox who informed her that an unknown person in New York was trying to hack into her account.

93. Furthermore, Plaintiff Nanez has experienced a drastic increase in daily spam emails, texts, phone calls and phishing attempts following the Data Breach and has taken extra precautions in reviewing the spam and phishing attempts and has spent a significant amount of time deleting and blocking numbers and messages.

94. As a result of the actual harm Plaintiff Nanez has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Nanez to spend significant time and energy dealing with issues related to the Data Breach, including time spent verifying the legitimacy of the Data Breach Notice Letter, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, freezing her account with her credit union, freezing her other financial accounts, adding two-step authentication to accounts, and changing user names and passwords on accounts. After the Data Breach, Plaintiff Nanez received several notifications on her iPhone of "fraud risks." Plaintiff Nanez spent time and energy resetting her iPhone and her family members' iPhones out of an abundance of concern and caution. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be

recaptured, was spent at Defendants' direction. Plaintiff will be required to maintain this heightened vigilance and incur mitigation measures well into the future.

95. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Nanez to suffer stress, fear, emotional distress, and anxiety.

96. Comcast acknowledged the risk posed to Plaintiff Nanez and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Nanez to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Nanez to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[14]

97. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[15]

98. Plaintiff Nanez has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

8. Alexander Nunn (Tenn.)

99. Plaintiff Alexander Nunn is an adult individual and a natural person of Tennessee, residing in Davidson County, where he intends to stay, and therefore is a citizen of Tennessee. Plaintiff Nunn received a notice letter from Comcast on or about January 2, 2024, informing him of the Data Breach and the exposure of his PII. The notice letter informed Plaintiff Nunn that his

[14] *Notice To Customers of Data Security Incident*, *supra* note 2.
[15] CitrixBleed Security Bulletin, *supra* note 3.

name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

100. Plaintiff Nunn only allowed Comcast and its vendors, including Citrix, to maintain, store, and use his PII because he reasonably expected that Defendants would use basic security measures to protect his PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing his PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Nunn entrusted his PII to Comcast and its vendors, and his PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Nunn been informed of Comcast's and Citrix's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Defendants.

101. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Nunn suffered injury from a loss of privacy.

102. As a result of the Data Breach, Plaintiff Nunn has been further injured by the damages to and loss in value of his PII—a form of intangible property that Plaintiff Nunn entrusted to Defendants. This information has inherent value that Plaintiff Nunn was deprived of when his PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

103. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Nunn to suffer imminent harm arising from a substantially increased risk of additional fraud, identity

theft, financial crimes, and misuse of his PII. This highly sensitive information, which includes his name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

104. As a result of the actual harm Plaintiff Nunn has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Nunn to spend time and energy dealing with issues related to the Data Breach, including researching the incident. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

105. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Nunn to suffer stress, fear, emotional distress, and anxiety.

106. Comcast acknowledged the risk posed to Plaintiff Nunn and his PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Nunn to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Nunn to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[16]

107. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[17]

[16] *Notice To Customers of Data Security Incident*, *supra* note 2.
[17] CitrixBleed Security Bulletin, *supra* note 3.

108. Plaintiff Nunn has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

9. Steven Prescott (Cal.)

109. Plaintiff Steven Prescott is an adult individual and a natural person of California, residing in Santa Cruz County, where he intends to stay, and therefore is a citizen of California. Plaintiff Prescott received a notice letter from Comcast by email on or about December 20, 2023, informing him of the Data Breach and the exposure of his PII. The notice letter informed Plaintiff Prescott that his name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

110. Plaintiff Prescott only allowed Comcast and its vendors, including Citrix, to maintain, store, and use his PII because he reasonably expected that Defendants would use basic security measures to protect his PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing his PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Prescott entrusted his PII to Comcast and its vendors, and his PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Prescott been informed of Comcast's and Citrix's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Defendants.

111. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Prescott suffered injury from a loss of privacy.

112. As a result of the Data Breach, Plaintiff Prescott has been further injured by the damages to and loss in value of his PII—a form of intangible property that Plaintiff Prescott entrusted to Defendants. This information has inherent value that Plaintiff Prescott was deprived of when his PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

113. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Prescott to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of his PII. This highly sensitive information, which includes his name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

114. Upon information and belief, Plaintiff Prescott's PII has already been stolen and misused, and these actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Prescott's life.

115. Furthermore, Plaintiff Prescott has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach, including calls for sales, to take loans, and 30-40 spam emails in his box every morning.

116. As a result of the actual harm Plaintiff Prescott has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Prescott to spend significant time and energy dealing with issues related to the Data Breach, including time spent researching the Data Breach and monitoring his accounts for suspicious activity. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

117. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Prescott to suffer stress, fear, emotional distress, and anxiety.

118. Comcast acknowledged the risk posed to Plaintiff Prescott and his PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Prescott to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Prescott to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[18]

119. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[19]

120. Plaintiff Prescott has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

10. Robert H. Smith (Ohio)

121. Plaintiff Robert H. Smith is an adult individual and a natural person of Ohio, residing in Delaware County, where he intends to stay, and therefore is a citizen of Ohio. Plaintiff Smith received a notice letter from Comcast on or about December 20, 2023, informing him of the Data Breach and the exposure of his PII. The notice letter informed Plaintiff Smith that his name, date of birth, last four digits of Social Security number, phone number, address, email address,

[18] *Notice To Customers of Data Security Incident*, *supra* note 2.
[19] CitrixBleed Security Bulletin, *supra* note 3.

Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

122. Plaintiff Smith only allowed Comcast and its vendors, including Citrix, to maintain, store, and use his PII because he reasonably expected that Defendants would use basic security measures to protect his PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing his PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Smith entrusted his PII to Comcast and its vendors, and his PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Smith been informed of Comcast's and Citrix's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Defendants.

123. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Smith suffered injury from a loss of privacy.

124. As a result of the Data Breach, Plaintiff Smith has been further injured by the damages to and loss in value of his PII—a form of intangible property that Plaintiff Smith entrusted to Defendants. This information has inherent value that Plaintiff Smith was deprived of when his PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

125. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Smith to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of his PII. This highly sensitive information, which includes his

name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

126. Upon information and belief, Plaintiff Smith's PII has already been stolen and misused as he has experienced incidents of fraud and identity theft. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Smith's life, specifically by subjecting Plaintiff Smith to banking fraud. About one month after the Data Breach, a stranger attempted to open a new financial account with JP Morgan Chase using Plaintiff Smith's PII.

127. Furthermore, Plaintiff Smith has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach, requiring him to take extra precautions in reviewing the spam calls and spend a significant amount of time deleting and blocking numbers and messages.

128. As a result of the actual harm Plaintiff Smith has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Smith to spend significant time and energy dealing with issues related to the Data Breach, including spending time verifying the legitimacy of the Data Breach Notice Letter, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred, and spending hours on communicating with Chase Bank and Allstate Identity Protection to resolve banking fraud. Much of the time and energy that Plaintiff Smith expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

129. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Smith to suffer stress, fear, emotional distress, and anxiety.

130. Comcast acknowledged the risk posed to Plaintiff Smith and his PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your

information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Smith to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Smith to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[20]

131. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[21]

132. Plaintiff Smith has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

11. Veronica Verdier (N.J.)

133. Plaintiff Veronica Verdier is an adult individual and a natural person of New Jersey, residing in Burlington County, where she intends to stay, and therefore is a citizen of New Jersey. Plaintiff Verdier received a notice letter from Comcast on or about December 20, 2023, informing her of the Data Breach and the exposure of her PII. The notice letter informed Plaintiff Verdier that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

134. Plaintiff Verdier only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as

[20] *Notice To Customers of Data Security Incident*, *supra* note 2.
[21] CitrixBleed Security Bulletin, *supra* note 3.

requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Verdier entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Verdier been informed of Comcast's and Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

135. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Verdier suffered injury from a loss of privacy.

136. As a result of the Data Breach, Plaintiff Verdier has been further injured by the damages to and loss in value of her PII—a form of intangible property that Plaintiff Verdier entrusted to Defendants. This information has inherent value that Plaintiff Verdier was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

137. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Verdier to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

138. Upon information and belief, Plaintiff Verdier's PII has already been stolen and misused. Plaintiff Verdier has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach, including a day in which she received dozens of spam emails in

one morning. These actions by unauthorized criminal third parties have thus detrimentally impacted Plaintiff Verdier's life.

139. As a result of the actual harm Plaintiff Verdier has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Verdier to spend significant time and energy dealing with issues related to the Data Breach, including researching the Data Breach, tracking the notices from her already existing Credit Karma monitoring account, and monitoring her accounts. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

140. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Verdier to suffer stress, fear, emotional distress, and anxiety.

141. Comcast acknowledged the risk posed to Plaintiff Verdier and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Verdier to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Verdier to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[22]

142. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[23]

[22] *Notice To Customers of Data Security Incident*, *supra* note 2.
[23] CitrixBleed Security Bulletin, *supra* note 3.

143. Plaintiff Verdier has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

12. Laura Wiley (Ill.)

144. Plaintiff Laura Wiley is an adult individual and a natural person of Illinois, residing in Cook County, where she intends to stay, and therefore is a citizen of Illinois. Plaintiff Wiley received a notice letter from Comcast on or about January 2, 2024, informing her of the Data Breach and the exposure of her PII. The notice letter informed Plaintiff Wiley that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

145. Plaintiff Wiley only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Wiley entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Wiley been informed of Comcast's and Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

146. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Wiley suffered injury from a loss of privacy.

147. As a result of the Data Breach, Plaintiff Wiley has been further injured by the damages to and loss in value of her PII-a form of intangible property that Plaintiff Wiley entrusted to Defendants. This information has inherent value that Plaintiff Wiley was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

148. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Wiley to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

149. Upon information and belief, Plaintiff Wiley's PII has already been stolen and misused, and these actions by unauthorized criminal third parties have thus detrimentally impacted Plaintiff Wiley's life.

150. As a result of the actual harm Plaintiff Wiley has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Wiley to spend significant time and energy dealing with issues related to the Data Breach, including time spent researching the Data Breach and self-monitoring her accounts for suspicious activity. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

151. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Wiley to suffer stress, fear, emotional distress, and anxiety.

152. Comcast acknowledged the risk posed to Plaintiff Wiley and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Wiley to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Wiley to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[24]

153. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[25]

154. Plaintiff Wiley has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

13. Marcia P. Wilson (Pa.)

155. Plaintiff Wilson is an adult individual and a natural person of Pennsylvania, residing in Chester County, where she intends to stay, and therefore is a citizen of Pennsylvania. In late December, after announcing the Data Breach, Comcast instructed Plaintiff Wilson to change her account passwords. This is because Plaintiff Wilson's account was likely compromised as a result of the Data Breach.

156. Plaintiff Wilson only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as

[24] *Notice To Customers of Data Security Incident*, *supra* note 2.
[25] CitrixBleed Security Bulletin, *supra* note 3.

requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Wilson entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Wilson been informed of Comcast's and Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

157. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Wilson suffered injury from a loss of privacy.

158. As a result of the Data Breach, Plaintiff Wilson has been further injured by the damages to and loss in value of her PII—a form of intangible property that Plaintiff Wilson entrusted to Defendants. This information has inherent value that Plaintiff Wilson was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

159. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Wilson to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

160. Upon information and belief, Plaintiff Wilson's PII has already been stolen and misused as she has experienced incidents of fraud and identity theft. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Wilson's life, specifically due to

multiple fraudulent attempts to access her email connected to her Comcast account, which has required her to reset her password.

161. Furthermore, Plaintiff Wilson has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach. She receives multiple calls from spam numbers each day and has spent significant time answering and blocking these spam callers.

162. As a result of the actual harm Plaintiff Wilson has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Wilson to spend significant time and energy dealing with issues related to the Data Breach, including researching the breach incident by reading news articles about the incident and monitoring her personal accounts to determine if she was affected by it. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

163. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Wilson to suffer fear, emotional distress, and anxiety.

164. Comcast has acknowledged the risk posed to their users as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging users to enroll in two-factor or multi-factor authentication for their Comcast accounts, and directing them to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[26]

165. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as

[26] *Notice To Customers of Data Security Incident*, *supra* note 2.

soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[27]

166. Plaintiff Wilson has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

14. Jodi Wolfson (N.J.)

167. Plaintiff Jodi Wolfson is an adult individual and a natural person of New Jersey, residing in Mercer County, where she intends to stay, and therefore is a citizen of New Jersey. Plaintiff Wolfson received a notice letter from Comcast on or about December 20, 2023, informing her of the Data Breach and the exposure of her PII. The notice letter informed Plaintiff Wolfson that her name, date of birth, last four digits of Social Security number, phone number, address, email address, Comcast username(s) and password(s), and Comcast security questions and answers were potentially compromised in the Data Breach.

168. Plaintiff Wolfson only allowed Comcast and its vendors, including Citrix, to maintain, store, and use her PII because she reasonably expected that Defendants would use basic security measures to protect her PII and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access databases storing her PII, exercising appropriate managerial control over vendors' data security, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Wolfson entrusted her PII to Comcast and its vendors, and her PII was within the possession and control of Comcast and its vendors at the time of the Data Breach. Had Plaintiff Wolfson been informed of Comcast's and

[27] CitrixBleed Security Bulletin, *supra* note 3.

Citrix's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Defendants.

169. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Wolfson suffered injury from a loss of privacy.

170. As a result of the Data Breach, Plaintiff Wolfson has been further injured by the damages to and loss in value of her PII—a form of intangible property that Plaintiff Wolfson entrusted to Defendants. This information has inherent value that Plaintiff Wolfson was deprived of when her PII was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

171. Given the nature of the information involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff Wolfson to suffer imminent harm arising from a substantially increased risk of additional fraud, identity theft, financial crimes, and misuse of her PII. This highly sensitive information, which includes her name, birth date, and last four digits of Social Security number, is now in the hands of criminals as a direct and proximate result of Defendants' misconduct.

172. Furthermore, Plaintiff Wolfson has experienced a drastic increase in daily spam emails, texts, and phone calls following the Data Breach, requiring her to take extra precautions in reviewing the spam calls and spend a significant amount of time deleting and blocking numbers and messages.

173. As a result of the actual harm Plaintiff Wolfson has suffered due to the Data Breach and the imminent and substantial risk of future harm, the Data Breach has forced Plaintiff Wolfson to spend significant time and energy dealing with issues related to the Data Breach, including self-monitoring her accounts to ensure no fraudulent activity has occurred, investigating fraudulent

activity, alerting her banking services about the breach, and changing identifying information and passwords for her accounts. Much of the time and energy that Plaintiff expended, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

174. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff Wolfson to suffer stress, fear, emotional distress, and anxiety.

175. Comcast acknowledged the risk posed to Plaintiff Wolfson and her PII as a result of the Data Breach, explicitly stating that "We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter," encouraging Plaintiff Wolfson to enroll in two-factor or multi-factor authentication for their Comcast account, and directing Plaintiff Wolfson to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[28]

176. Similarly, Citrix "strongly urge[d] customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions of NetScaler ADC and NetScaler Gateway as soon as possible," as "exploits of [the CitrixBleed vulnerability] on unmitigated appliances have been observed."[29]

177. Plaintiff Wolfson has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Comcast's possession, is protected, and safeguarded from future breaches.

B. Defendants

178. Defendant Comcast Corporation is a Pennsylvania corporation with its principal place of business located at Comcast Center, 1701 JFK Boulevard, Philadelphia, Pennsylvania 19103.

[28] *Notice To Customers of Data Security Incident*, *supra* note 2.
[29] CitrixBleed Security Bulletin, *supra* note 3.

179. Defendant Comcast Cable Communications, LLC is a Delaware limited liability company that maintains its headquarters at Comcast Center, 1701 JFK Boulevard, Philadelphia, Pennsylvania 19103. Upon information and belief, Comcast Corporation is the only member of Comcast Cable Communications, LLC. Defendant Comcast Cable Communications, LLC is a citizen of each state in which its members are citizens. As such, Defendant Comcast Cable Communications, LLC is a citizen of Pennsylvania.

180. Defendant Citrix Systems, Inc. ("Citrix") is a Delaware corporation with its principal place of business in Fort Lauderdale, Florida, and is therefore a citizen of Florida. Citrix's direct parent corporation is Picard Parent, Inc. Picard Parent, Inc. is a direct, wholly owned subsidiary of Cloud Software Group, Inc., which is a direct wholly owned subsidiary of Cloud Software Holdings, Inc., which is a direct, wholly owned subsidiary of Picard Holdco, Inc.

III. JURISDICTION AND VENUE

181. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

182. This Court has general personal jurisdiction over Defendant Comcast Corporation because Comcast Corporation maintains its principal place of business in this District, has sufficient minimum contacts with this District, and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

183. This Court has general personal jurisdiction over Defendant Comcast Cable Communications, LLC because Comcast Cable Communications, LLC maintains its principal

place of business in this District, has sufficient minimum contacts with this District, and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

184. This Court has general personal jurisdiction over Citrix Systems, Inc., pursuant to 42 Pa. C.S.A. § 5301(a)(2). Specifically, this Court has general jurisdiction over Citrix because Citrix is an out-of-state corporation registered to do business under the laws of the Commonwealth of Pennsylvania since September 29, 1999. As part of registering to do business in the Commonwealth of Pennsylvania, Citrix "shall enjoy the same rights and privileges as a domestic entity and shall be subject to the same liabilities, restrictions, duties and penalties . . . imposed on domestic entities." 15 Pa. C.S.A. § 402(d). Among other things, Pennsylvania law is explicit that "qualification as a foreign corporation under the laws of [the] Commonwealth" shall permit state courts to "exercise general personal jurisdiction" over a registered foreign corporation, just as they can over domestic entities. Pa. C.S.A. § 5301. Thus, by registering to do business in the Commonwealth of Pennsylvania and benefiting from the opportunity to do business in the Commonwealth of Pennsylvania, Citrix has consented to being subject to general jurisdiction in the Commonwealth of Pennsylvania.

185. Alternatively, this Court has specific personal jurisdiction over Citrix because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Additionally, the exercise of personal jurisdiction is proper because Citrix has purposefully availed itself of the privileges of conducting business within this District, and has established sufficient minimum contacts within the District.

186. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Comcast's principal place of business is located in this District and a substantial part of the events

or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

IV. STATEMENT OF FACTS

A. Comcast Obtains, Collects, and Stores Plaintiffs' and Class Members' Private, Personally Identifiable Information.

187. Comcast is one of the largest companies in the American telecommunications sector, and provides internet services and products, cable television, mobile 5G network cellular services, and landline telephone services and products to individuals and businesses across the United States under the brand name Xfinity.[30]

188. The bulk of Comcast's consumer-facing business comes from its cable communications services, which include broadband, video, voice, wireless, and other services that are offered individually and as bundled services to residential customers nationwide. According to its 2022 Annual Report, Comcast provides its cable communications services to almost 32 million residential customers.[31] While Comcast, under the Xfinity brand, primarily serves residential customers, Comcast also boasts a sprawling business division that serves over 2 million business services customers, with Xfinity's business operations recently "approaching $10 billion in annual revenue."[32]

189. Xfinity's reach is substantial, even compared to its competitors across the United States, with Comcast claiming that Xfinity is now the "largest internet provider in the U.S."[33]

---

[30] *Comcast 2022 Annual Report on Form 10-K*, https://www.cmcsa.com/static-files/156da323-653e-4cc6-9bb4-d239937e9d2f (last visited July 1, 2024).

[31] Annual Report, *supra* note 30.

[32] *Connectivity & Platforms*, Comcast, https://corporate.comcast.com/company/connectivity-platforms (last visited July 1, 2024).

[33] *Connectivity & Platforms*, *supra* note 32.

190. Beyond traditional cable communications services, Xfinity also operates a nationwide network of 20 million internet hot spots, which non-residential services customers can sign up to utilize under an array of hotspot-only internet plans.[34]

191. Comcast also offers 5G network wireless cellular service plans under the Xfinity Mobile and NOW Mobile brands that leverage the extensive Xfinity internet hot spot network. These services are also fast-growing, with more than six million customers.[35]

192. To run its business, Comcast collects, maintains, and profits from the PII of millions of U.S. consumers. Depending on the Xfinity product(s) that customers sign up for, Comcast requires customers to provide their name, phone number, residential address, date of birth, last four digits of Social Security number, demographic information, their mobile phone's unique technical identifier (also known as an International Mobile Equipment Identity or "IMEI" number), information and forms required for proof of residency, credit card or debit card information, and/or bank account information. Comcast collects this PII from all prospective and current customers and maintains and profits from the PII regardless of whether a potential customer eventually purchases Xfinity services. Comcast also maintains the PII of former Xfinity customers for an indefinite period after they terminate their Xfinity services.

193. To use any of Comcast's Xfinity services, customers must also create an online account with Xfinity and create a username, password, and secret questions and answers to assist with account recovery.

[34] *Xfinity Wifi*, Xfinity, https://www.xfinity.com/learn/internet-service/wifi (last visited July 1, 2024).

[35] *Wireless*, Comcast, https://corporate.comcast.com/company/xfinity/wireless (last visited July 1, 2024).

B. Comcast Knows the Risk of Storing PII and Promises to Keep Customers' PII Secure.

194. As a company storing and using sensitive customer data, Comcast is at great risk of cyberattacks. Comcast is well-aware of this risk and expressly represents to customers that it will protect their PII.

195. Comcast recognizes the foreseeable risk of cyberattacks it faces. In Comcast's 2022 Cyber Health Report, Comcast states "[w]e know that our customers' data is what bad actors are after" and states "[d]ata breaches have become a part of daily life. We hear about a breach on the news and we hope we don't get the dreaded email saying our data was compromised. But while data breaches may seem sadly normal, we don't think they have to be, and we're committed to helping prevent them."[36]

196. Comcast's 2022 Cyber Health Report similarly recognizes that it is Comcast's responsibility to safeguard its customers' PII, not the other way around: "[w]e don't expect our customers to be cybersecurity experts. That's why we make a point of prioritizing security for them, from the gateway in their home through to the core of our network."[37]

197. Further, Comcast has an entire sub-page of the Xfinity website dedicated to customer data protection and privacy. At the top of this Privacy sub-page, Comcast represents to consumers that "[y]our privacy matters to us," and emphasizes that "[w]e know you rely on us to stay connected to the people and things you care about most. And your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure and put you in control of it."[38]

---

[36] 2022 Cyber Health Report, *supra* note 1, at 1, 12.

[37] *Id.* at 1.

[38] *Privacy*, Xfinity, http://xfinity.com/privacy (last visited July 1, 2024).

198. Indeed, Comcast explicitly states "[w]e believe strong cybersecurity is essential to privacy," and highlights to customers that it works tirelessly to protect their sensitive information from cyberattacks:

> We help protect you with multiple layers of security that automatically detect and block hundreds of thousands of cyber events every second and a team of security experts who work to protect you 24 hours a day, 365 days a year.[39]

199. Comcast goes on to describe all the "tools and support" it provides to help customers "stay safe online," including "free security software and tools, like multi-factor authentication," and "access to free online tips and advice and an Xfinity security and privacy team to help protect you and your family from cyber threats."[40]

200. The Xfinity Privacy Policy similarly goes to great lengths to promise customers that Comcast will protect the PII that it collects:

> 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. These security practices include technical, administrative, and physical safeguards, which may vary, depending on the type and sensitivity of the information. Although we take the responsibility of safeguarding your personal information seriously, no security measures are 100% effective and we cannot guarantee that these practices will prevent every unauthorized attempt to access, use, or disclose your information. Comcast also takes additional steps to increase the security and reliability of customer communications. We do not read your outgoing or incoming email, file attachments, video mail, private chat, or instant messages. However, we (along with our service providers) use software and hardware tools to help prevent and block "spam" emails, viruses, spyware, and other harmful or unwanted communications and programs from being sent and received over Comcast.net email and the Comcast Services. To help protect you and the Services against these harmful or unwanted communications and programs, these tools may automatically scan your emails, video mails, instant messages, file

[39] *Id.*

[40] *Id.*

> attachments, and other files and communications. We do not use these tools for marketing or advertising.[41]

201. Comcast also acknowledged the risk of inadequate data security—including through use of third-party products and services—in its SEC filings:

> … In the ordinary course of our business, there are constant attempts by third parties to cause systems-related events and security incidents and to identify and exploit vulnerabilities in security architecture and system design. These incidents include computer hackings, cyber attacks, computer viruses, worms or other destructive or disruptive software, denial of service attacks, phishing attacks, malicious social engineering, and other malicious activities. Incidents also may be caused inadvertently by us or our third-party vendors, such as process breakdowns and vulnerabilities in security architecture or system design. . . . Moreover, as we also obtain certain confidential, proprietary and personal information about our customers, personnel and vendors, and in some cases provide this information to third party vendors who agree to protect it, we face the risk that this information may become compromised through a cyber attack or data breach, misappropriation, misuse, leakage, falsification or accidental release or loss of information. Due to the nature of our businesses, we may be at a disproportionately heightened risk of these types of incidents occurring because we maintain certain information necessary to conduct our business in digital form. We also incorporate third-party software (including extensive open-source software), applications, and data hosting and cloud-based services into many aspects of our products, services and operations, as well as rely on service providers to help us perform our business operations, all of which expose us to cyber attacks on such third-party suppliers and service providers.
>
> While we develop and maintain systems, and operate extensive programs that seek to prevent security incidents from occurring, these efforts are costly and must be constantly monitored and updated in the face of sophisticated and rapidly evolving attempts to overcome our security measures and protections. . . . Despite our efforts, we expect that we will continue to experience such incidents in the future, and there can be no assurance that any such incident will not have an adverse effect on our business, reputation or results of operations.[42]

---

[41] *Our Privacy Policy*, Xfinity, https://www.xfinity.com/privacy/policy (last visited July 1, 2024).

[42] *Comcast 2022 Annual Report on Form 10-K*, Comcast (Feb. 3, 2023), https://www.cmcsa.com/static-files/b5959ccc-6216-4bbb-a0ca-de6f689925f7.

202. The risk that cybercriminals will breach Comcast's systems and gain unauthorized access to customers' PII, and use that information for malicious purposes, is not theoretical. As Comcast itself states, Comcast is bombarded with "hundreds of thousands of cyber events every second."[43]

203. In fact, Comcast's systems have previously been breached at least three times, which should have put Comcast on notice as to both weaknesses in its security practices as well as cybercriminals' desire to target its systems.

204. In 2015, for example, a hacker breached Comcast's systems and stole nearly 590,000 then-current and former Comcast email addresses and passwords, which the hacker subsequently posted for sale on the "dark web."[44] The dark web is a heavily encrypted part of the Internet that conceals users' identities and online activity, and makes it difficult for authorities to detect the location or owners of a website when illegally-acquired information is disclosed or put up for sale.

205. In 2021, hackers were able to breach Comcast's systems and display a cryptic message to any Xfinity customer that logged into their account. Starting on December 19th, many Xfinity email users began receiving notifications that their account information had been changed. However, when attempting to access the accounts, they could not log in as the passwords had been

[43] Xfinity Privacy Center, *supra* note 38.

[44] Pierluigi Paganini, *200,000 Comcast Login Credentials Available on the Dark Web*, Security Affairs (Nov. 10, 2015), https://securityaffairs.com/41875/cyber-crime/200000-comcast-login-darkweb.html.

changed. "After regaining access to the accounts, they discovered they had been hacked and a secondary email at the disposable @yopmail.com domain was added to their profile."[45]

206. And in 2022, Comcast was the victim of yet *another* breach, when cybercriminals were able to bypass Xfinity's two-factor authentication safeguard and compromise an unidentified number of Xfinity accounts.[46]

207. At all relevant times, Comcast therefore knew of the attendant risks that it and its customers faced as a result of collecting and storing the PII of millions of individuals and was well-aware that it must develop a robust cybersecurity program, including developing policies to prevent additional data breaches moving forward.

208. Indeed, because of the highly sensitive and personal nature of Plaintiffs' PII that Comcast collects and stores, Comcast has publicly affirmed its obligation and duty to secure PII, as noted *supra*.

209. Despite Comcast's duty, and its representations made to its consumers, Comcast's data security practices fell flat, leading to the Data Breach and the compromise of its customers' PII.

C. Comcast Engaged Citrix to Improve its Systems' Data Security and Safeguard the PII in its Possession and Control.

210. As part of its strategy to protect and safeguard the PII that customers had entrusted to it, Comcast contracted with Defendant Citrix to implement the NetScaler products to support its network systems and provide protection against cyberattacks.

---

[45] Sarah J. Callahan, *Comcast Customers Face a Huge Holiday Data Breach*, The Street (Dec. 24, 2022), https://www.thestreet.com/technology/comcast-xfinity-data-breach-two-factor-auth-help-bypass.

[46] *Id.*

211. Founded in 1989, Citrix has grown into one of the largest companies in the office technology sector. It provides an array of cloud computing and virtualization products to hundreds of thousands of clients worldwide, including server, application and desktop virtualization, networking, software as a service (SaaS), and other cloud-related services. As of 2024, Citrix cloud-related services alone are used by over 16 million customers.[47]

212. In 2016, Citrix consolidated all of its networking products under the NetScaler product line. The NetScaler line includes NetScaler ADC, an application delivery controller (ADC), NetScaler AppFirewall, an application firewall, NetScaler Unified Gateway, which offered remote access to virtual desktops, NetScaler Application Delivery Management (ADM), and NetScaler SD-WAN, which provides software-defined wide-area networking management.

213. The NetScaler products at issue here combine to purportedly improve the efficiency and speeds of applications (NetScaler ADC) and consolidate remote access infrastructure by providing a single-sign-on across all applications (NetScaler Gateway).[48]

214. NetScaler was spun off into a different business unit of Cloud Software Group, Inc, Citrix's parent company, when Citrix was taken private in 2022. However, on information and belief, Citrix has remained responsible for maintenance and support of the NetScaler line of products as recently as the Data Breach, as Citrix itself released the patch for the NetScaler vulnerability that was exploited in the Data Breach.[49]

---

[47] *About*, CITRIX, https://www.citrix.com/about/ (last visited July 1, 2024).
[48] *See What is an application delivery controller?*, Citrix, https://www.netscaler.com/articles/what-is-an-application-delivery-controller (last visited July 1, 2024); *NetScaler Gateway*, NetScaler (Jan. 8, 2024), https://docs.netscaler.com/en-us/netscaler-gateway.html.
[49] CitrixBleed Security Bulletin, *supra* note 3.

215. Citrix knows that its products are used to manage highly sensitive information and the risks that come from storing and managing sensitive customer information.

216. In the "Citrix Trust Center" on Citrix's website, Citrix emphasizes that customers' "security is our priority," noting that "[r]esponsibly adopting advanced technologies requires a critical eye on cybersecurity and data privacy. Because we design our products around centralized delivery, visibility and control of apps and data, security is built into the core of our solutions and practices."[50]

217. Elsewhere on the Trust Center webpage, Citrix markets its ability to keep customers' data secure, stating: "For almost 30 years, our customers have trusted our ability to handle their data with care and respect. That's why organizations from the most highly regulated sectors rely on us to protect their most sensitive information wherever work happens."[51]

218. Similarly, the privacy policy for Citrix/Cloud Software Group, Inc., states that Citrix protects personal information by "maintain[ing] administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Personal Information."[52]

219. At all relevant times, Citrix therefore knew of the risk that vulnerabilities in its products could lead to unauthorized access to its customers' sensitive data, and that, on information and belief, Citrix determined that it must place data security at the heart of its business model.

---

[50] *Citrix Trust Center*, Citrix, https://www.citrix.com/about/trust-center/ (last visited July 1, 2024).
[51] *Privacy & Certifications*¸ Citrix, https://www.citrix.com/about/trust-center/privacy-compliance.html (last visited July 1, 2024).
[52] https://www.cloud.com/privacy-policy (last visited July 1, 2024).

D. Defendants' Legal Responsibility to Safeguard Information.

220. Beyond the obligations created in their security and privacy policies and other promises made to consumers about the security of their data, Comcast and Citrix owed Plaintiffs and Class Members a legal duty to safeguard their PII.

221. First, as described further below, Comcast and Citrix owed a duty to safeguard PII pursuant to several federal and state statutes, including the Federal Trade Commission Act ("FTC Act") and the Cable Communications Policy Act, to ensure that all information collected and stored was secure. These statutes were intended to protect Plaintiffs and Class Members from the type of conduct by Comcast and Citrix alleged herein.

222. Comcast also owed a nondelegable duty to safeguard PII given that Comcast knew that it was maintaining highly valuable data, for which Comcast knew would be targeted by cybercriminals. Comcast likewise knew of the extensive harm that would occur if Plaintiffs' and Class Members' PII were exposed through a Data Breach, and thus owed a nondelegable duty to safeguard that information.

223. Citrix similarly was well-aware that its products were used by customers that handled sensitive PII, and as such knew that any vulnerabilities in its products could lead to the access, compromise, and theft of PII.

224. Given the sensitive nature of the PII obtained by the cybercriminals in the Data Breach, Comcast knew that these hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, social engineering attacks, and other identity-related fraud if they were able to exfiltrate the PII from Comcast's system. Comcast also knew that individuals whose PII was stored on Comcast's servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated. Indeed, in its notice letter, Comcast expressly acknowledged, recognized, and appreciated the imminent threat and

substantial risk of identity theft and fraud as a direct and proximate result of the Data Breach when it stated that consumers could take certain actions like monitoring their financial accounts and credit reports.

225. Citrix similarly recognized that, given its customers used its products to store and manage PII, any breach of those products' security vulnerabilities would result in identity theft, financial fraud, phishing, social engineering attacks, and other identity-related fraud. Citrix also knew that individuals whose PII was stored on its customers' systems would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

226. Comcast also owed a duty to safeguard Plaintiffs' and Class Members' data based upon the promises that it made to its customers to safeguard data, as well as the disclosures that it made in its data security policies and privacy policies. Comcast undertook efforts to keep that data secure as part of its business model and thus owes a continuing obligation to Plaintiffs and Class Members to keep their PII secure.

227. Citrix similarly owed a duty to safeguard Plaintiffs' and Class Members' data based upon the promises that it made to its customers regarding its products' ability to safeguard data, as well as the disclosures that it made in its data security policies and privacy policies. Citrix undertook efforts to keep customers' data secure as part of its business model and thus owes a continuing obligation to Plaintiffs and Class Members to keep their PII secure.

228. Comcast and Citrix each also owed a duty to comply with industry standards in safeguarding PII, which—as discussed herein—neither company complied with.

E. Defendants Knew the Risks of Collecting and Storing Valuable PII and the Foreseeable Harms of Exposing PII to Cybercriminals.

229. At all relevant times, Comcast knew it was storing and collecting customers' sensitive PII, and, that as a result, those systems would be attractive targets for cyber criminals.

230. Similarly, at all relevant times, Citrix knew that its NetScaler products would be used by companies such as Comcast, to prevent cybercriminals from gaining access to their computer systems and networks.

231. The data that Comcast stores and utilizes Citrix NetScaler to protect is a treasure trove for cyber criminals as this data contains all of the necessary building blocks to commit fraud. Indeed, the PII that customers entrusted to Comcast includes usernames and hashed passwords, names, contact information, last four digits of Social Security numbers, dates of birth, and secret security questions and answers.

232. The ramifications of Defendants' failure to protect Plaintiffs' and the Class's PII is long lasting and severe, particularly given the risk of identity theft that Plaintiffs and the Class now face. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

233. The Federal Trade Commission recognizes identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[53] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

[53] 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[54]

234. PII, including the information collected by Comcast, is highly valued by criminals, as evidenced by the prices that such information commands on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, a single victim's personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[55] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[56]

235. Moreover, there may be a time lag between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[57]

236. Moreover, the telecommunications industry is "among the most-targeted sectors globally for cybercriminals, and it's not hard to see why. Sensitive user information is carried at a massive scale on telecom networks, and that naturally makes them an attractive target for malicious

---

[54] *Id.*

[55] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.

[56] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

[57] Report to Congressional Requesters, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

actors."[58] Indeed, there have been numerous high-profile data breaches in the telecommunications industry in recent years, including Comcast, T-Mobile, and AT&T.

237. The breadth of the data compromised in the Data Breach also makes the information particularly valuable to cybercriminals and leaves Comcast's customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

238. **Social Security Numbers**—An individual's Social Security number is made up of three parts: (1) an area number (the first three digits); (2) a group number (the middle two digits); and (3) a serial number (the last four digits). The area number corresponds to the state in which an individual applied for their Social Security number, while the group number refers to the specific order in which Social Security numbers are distributed within a geographical region. Finally, the serial number corresponds with the area and group number and is designed to distinguish one Social Security number from the next.[59]

239. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

---

[58] Katy, Allan, *The growing concerns in telecommunication cybersecurity*, Cyber Magazine (Oct. 30, 2023), https://cybermagazine.com/articles/the-growing-concerns-in-telecommunication-cybersecurity.

[59] *Structure of Social Security Numbers*, Barcodes, https://www.barcodesinc.com/articles/structure-of-social-security-numbers.htm (last visited July 1, 2024).

240. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[60]

241. Moreover, even the theft of the last four digits of an individual's Social Security number can subject them to identity theft and fraud as companies and creditors often verify someone's identity by asking only for the last four digits, or the "serial number," of an individual's Social Security number. As such, cyber criminals armed with the last four digits of an individual's Social Security number, in combination with other personal information—as is the case here—can open accounts, access an individual's name, or apply for benefits in that person's name.[61] Cybercriminals can also use computer programs to easily predict the first five digits of an

[60] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[61] Hari Ravichandran, *What Can Someone Do With Your Social Security Number*, Aura (Apr. 8, 2024), https://www.aura.com/learn/what-can-someone-do-with-your-social-security-number#:~:text=Many%20banks%2C%20government%20agencies%2C%20and,for%20benefits%20in%20your%20name.

individual's Social Security number, thus allowing them to determine an individual's full nine-digit number and commit even more types of fraud.[62]

242. **Usernames and Passwords**—When cybercriminals gain access to an individual's username and password for one account, cybercriminals gain access to the username and password for an individual's other accounts, as well. Research has indicated that individuals typically reuse passwords on 10 of their personal accounts and that more than 6 in 10 people have admitted to reusing passwords. When these studies are combined with studies that suggest that more than 80% of confirmed breaches are related to stolen, weak, or reused passwords, the compromise of an individual's username and password in one data breach provides cybercriminals with the ammunition needed to wreak havoc on an individual's other accounts.[63]

243. **Security Questions and Answers**—Security questions and answers are also dangerous in the hands of cybercriminals. Security questions and answers which often involve supposedly "secret" information like a consumer's favorite place to travel or the street on which the consumer grew up, are frequently utilized by cybercriminals to reset an individual's password and thereby gain access to their account. Because security questions are commonly repeated across various websites, often involving things like an individual's mother's maiden name, the city in which they were born, or an individual's first pet, they are reused across many accounts, and their compromise in one data breach will lead to the compromise across many other accounts, subjecting an individual to a single point of compromise across all accounts.[64]

---

[62] Xeni Jardin, *Reverse-engineering SSNs from publicly available data*, BoingBoing (July 6, 2009), https://boingboing.net/2009/07/06/reverse-engineering.html.

[63] Clare Stouffer, *139 password statistics to help you stay safe in 2024*, Norton (June 27, 2023), https://us.norton.com/blog/privacy/password-statistics.

[64] Lily Hay Newman, *Time to Kill Security Questions—or Answer Them With Lies*, Wired (Sept. 28, 2016), https://www.wired.com/2016/09/time-kill-security-questions-answer-lies/.

244. Even if cybercriminals do not gain access to a complete set of an individual's PII during a data breach, cybercriminals can cross-reference two or more sources of PII to marry data available elsewhere with criminally stolen data, resulting in complete and accurate dossiers on individuals. These dossiers are known as "Fullz" packages.

245. The development of "Fullz" packages means stolen PII from a data breach can easily be linked to victims' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers is not included in the PII stolen in a specific incident, criminals can easily create a "Fullz" package that links that information together and sell the package at a higher price.

246. Importantly, once a cybercriminal has a "Fullz" package, cybercriminals can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs, medical identity fraud, tax refund fraud, and buy now pay later frauds.[65] Most problematic, however, is that cybercriminals in possession of a "Fullz" package "are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures."[66]

247. Finally, the PII compromised in the Data Breach is valuable to cybercriminals because it can be used to commit "porting-out" scams, whereby cybercriminals use different methods to highjack an individual's phone number, assume their identity, intercept security

[65] *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DataDome, https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/#:~:text=Identity%20fraud%3A%20A%20set%20of,personal%20or%20business%2Drelated%20information (last visited July 1, 2024).

[66] *Protection Against Fullz and Fraud, Integrity*, Aristotle (Apr. 18, 2022), https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/.

protocols sent to an individual's phone, and gain access to their financial and social media accounts.[67]

248. In a port-out scam, as explained by the FTC, cybercriminals will target an individual's PII, including their name, address, birth date, PINs, passwords, and the last four digits of their Social Security number to initiate a port request with the individual's phone company. Specifically, cybercriminals can use the PII compromised in the Data Breach to scam an individual's phone company into porting the individual's phone number to a different mobile device or a service account set up by the cybercriminal. Once the cybercriminal's porting request is successful, the cybercriminal begins receiving the individual's private texts and calls, can reset the access credentials for many financial and social medial accounts as text messages are frequently used by businesses to verify an individual's identity when requesting account updates, and subsequently drain the victim's accounts or ransom back access to the victim's accounts.[68]

249. To protect against porting out scams, the FTC advises individuals to guard against personal details that can be used to verify their identity, including the last four digits of their Social Security numbers, their phone numbers, their dates of birth, the make and model of their cars, their pet's name, and their mother's maiden name—the very PII that was compromised in the Data Breach and now in the hands of cyber criminals.[69]

250. Aside from these risks of identity theft and fraud, PII is also property that has monetary value to data breach victims.

---

[67] *Port-Out Fraud Targets Your Private Accounts*, Federal Trade Comm'n (Nov. 17, 2023), https://www.fcc.gov/port-out-fraud-targets-your-private-accounts.

[68] *Id.*

[69] *Id.*

251. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[70]

252. In 2013, the Organization for Economic Cooperation and Development ("OECD") published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[71] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[72]

253. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [$2] for a date of birth, USD 8 [$8] for a Social Security number (government ID number), USD 3 [$3] for a driver's license number and USD 35 [$35] for a military record. A combination of address, date of birth, Social Security number, credit record and military [record] is estimated to cost USD 55 [$55]."[73]

254. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee-for-services-provided to monetizing their users'

---

[70] Brad Brown et al., *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/capabilities/quantumblack/our-insights/capturing-value-from-your-customer-data.

[71] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[72] *Id.* at 25.

[73] *Id.*

data—including user data that is not necessary for product or service, which she refers to as "behavioral surplus."[74]

255. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to users. Market exchanges have sprung up where individual users like Plaintiffs can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay users for their data.[75] Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.[76]

256. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished when users discover how their data is being covertly intercepted, collected, used, and disclosed.

257. As a group of information technology professors relayed in a 2016 article entitled "The Economics of Privacy," published in the Journal of Economic Literature:

> Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, and consumption habits) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.[77]

258. In other words, a successful cyberattack leaves criminals with a lucrative and readily monetized supply of PII—and deprives its victims of the exclusive use of their own information.

---

[74] Shoshanna Zuboff, *The Age of Surveillance Capitalism* 166 (2019).

[75] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash, Best Wallet Hacks* (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.

[76] Jacob Kastrenakes, *A new TikTok Clone hit the top of the App Store by paying users to watch videos*, The Verge (May 29, 2020), https://www.theverge.com/2020/5/29/21274994/zynn-tiktokclone-pay-watch-videos-kuaishou-bytedance-rival.

[77] Alessandro Acquisti et al., *The Economics of Privacy*, 54 J. of Econ. Lit. 442, 444 (June 2016).

259. The documented increase in cyberattacks, combined with increasing monetary incentives that heighten the risk of future attacks, was widely known to the public and to anyone in Defendants' industries, including Defendants, at the time of the Data Breach.

260. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the telecommunications industry preceding the date of the Data Breach.

261. Plaintiffs and Class Members, as current and former customers of Comcast, relied on both Comcast and Citrix to keep their PII confidential and secure, to use their information for business purposes only, and to make only authorized disclosure of their information.

262. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII, Comcast assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiffs' and Class Members' PII from foreseeable risks of disclosure to unauthorized parties. Comcast agreed to and undertook legal duties to securely store and maintain the PII of Plaintiffs and Class Members.

263. Similarly, by providing Comcast with NetScaler products to protect Plaintiffs' and Class Members' PII, Citrix assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiffs' and Class Members' PII from foreseeable risks of disclosure to unauthorized parties.

F. Despite Their Duties and the Foreseeable Risk of Harm, Comcast and Citrix Failed to Protect Plaintiffs' and Class Members' PII.

264. At the same time Comcast collected, stored, and profited from Plaintiffs' PII using Citrix technology—and while Comcast was actively promising consumers that "we're always working to keep your personal information secure" and Citrix told was telling customers like Comcast that they could rely on the company's products to "protect their most sensitive

information"—cybercriminals exploited a vulnerability in Citrix's products and stole nearly 36 million current and former Comcast customers' PII.

265. On October 10, 2023, Citrix published a security bulletin entitled "NetScalerADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967" that announced: "Multiple vulnerabilities have been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway)."[78] The CVE-2023-4966 vulnerability has become known in the cybersecurity community as "CitrixBleed," and allows cyberattackers to gain unauthorized access to sensitive data contained on internal systems.[79] Specifically, an attacker exploiting CitrixBleed sends an HTTP GET request to a vulnerable NetScaler appliance, which returns a session cookie that allows the hacker to establish an authenticated session with the NetScaler appliance without any need for a username, password, or multi-factor authentication token or device.[80]

266. The CitrixBleed vulnerability was likely exploited well before Citrix's announcement. Mandiant, a leading cybersecurity and threat intelligence firm that is a subsidiary of Google, identified exploitation of the CitrixBleed vulnerability "in the wild" beginning in August of 2023, based on its discovery of "multiple instances of successful exploitation of CVE-2023-4966 that resulted in the takeover of legitimate user sessions on NetScaler ADC and Gateway appliances." Mandiant discovered these exploitations prior to October 10, 2023, while it was

[78] CitrixBleed Security Bulletin, *supra* note 3.

[79] *CitrixBleed, a vulnerability in massive exploitation phase*, Telefónica Tech (Dec. 4, 2023), https://telefonicatech.com/en/blog/citrixbleed-a-vulnerability-in-massive-exploitation-phase.

[80] *Investigation of Session Hijacking via Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966),* Mandiant, https://cloud.google.com/blog/topics/threat-intelligence/session-hijacking-citrix-cve-2023-4966/ (last visited July 1, 2024).

"conducting investigations where a threat actor was taking over user's NetScaler sessions through unknown means."[81]

267. Mandiant's investigation into the Citrix Bleed vulnerability demonstrated the risks that come from widespread use of Citrix's NetScaler products. According to Mandiant, exploitation of the Citrix Bleed vulnerability occurred across many sectors, as Mandiant itself was investigating breaches related to CitrixBleed exploitation in "legal and professional services, technology, and government organizations." Additionally, Mandiant suspected that "the number of impacted organizations is far greater" and occurred in even more sectors, "[g]iven the widespread adoption of Citrix in enterprises globally."[82]

268. Indeed, upon information and belief, prior to the Data Breach, Comcast and Citrix were well-aware that Citrix NetScaler applications had an array of vulnerabilities and a lack of security protocols that made it dangerous and extremely risky to use NetScaler to store any sensitive information.

269. Despite Citrix releasing the initial patch for the CitrixBleed vulnerability on October 10, 2023, Comcast, by its own admission, did not institute the patch and secure its systems until October 23, 2023, even though it later claimed to customers that it "promptly patched and mitigated [its] systems."[83]

---

[81] *Id.*

[82] *Id.*

[83] *Notice To Customers of Data Security Incident*, Xfinity, https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (last visited July 1, 2024).

270. Later, between November 16 and December 6, 2023, Comcast discovered that cybercriminals had hacked into its systems by exploiting the CitrixBleed vulnerability during the time between the release of the CitrixBleed patch and Comcast's implementation of the patch.

271. Specifically, between October 16 and October 19, 2023, cyberattackers gained unauthorized access to Comcast's internal systems and stole Xfinity customers' PII.

272. Several weeks later, Comcast finally determined that the data that was exfiltrated included Xfinity customers' usernames and passwords, and likely included an array of additional sensitive information, including names, contact information, last four digits of Social Security numbers, dates of birth and/or secret questions and answers.

273. Citrix is equally blameworthy for this Data Breach. Along with a belated disclosure of the vulnerability, Citrix also initially failed to reveal the severity of the vulnerability. While Citrix originally recommended "customers of NetScaler ADC and NetScaler Gateway to install the relevant updated versions" of the NetScaler products "as soon as possible,"[84] it was not until a week later that Citrix revealed—in bold and underlined font—that "**[e]xploits of CVE-2023-4966 on unmitigated appliances have been observed.**"[85] And six days after that, Citrix finally recommended that those using the NetScaler products "kill[] all active and persistent sessions[.]"[86]

---

[84] *NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967*, Citrix (Oct. 10, 2023), https://web.archive.org/web/20231012010221/https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967/.

[85] *NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967*, Citrix (Oct. 17, 2023), https://web.archive.org/web/20231018100605/https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967.

[86] Anil Shetty, *CVE-2023-4966: Critical security updated now available for NetScaler ADC and NetScaler Gateway* (Oct. 23, 2023), https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/.

274. Indeed, many companies failed to timely deploy the Citrix patches, which, on information and belief, was due to the lack of urgency and severity communicated in the initial Citrix bulleting. For example, one analysis in December 2023 found that roughly 4,600 vulnerable Citrix products were still online as of October 31, 2023, and 1,300 vulnerable products remained online by December 31, 2023.[87] And while many companies timely patched their Citrix products and prevented a breach of their systems, several large companies beyond Comcast were also hacked through an exploit of CitrixBleed, including Boeing, Toyota, and the law firm Allen & Overy.[88] Had Citrix revealed the severity of the breach sooner, the Comcast Data Breach, and many others, may have been mitigated.

G. Comcast Admits It Failed to Protect Plaintiffs' PII and Compounded Its Failure by Providing Inadequate Notice to Those Impacted.

275. Comcast announced the breach in a press release on December 18, 2023, and subsequently distributed a "Notice to Customers of Data Security Incident" (the "Notice") to impacted customers. Comcast's first public acknowledgement of the breach thus occurred over two months after Comcast learned of the CitrixBleed vulnerability and over a month after Comcast concluded that customers' PII had been stolen by cybercriminals exploiting the vulnerability.

276. In the Notice, Comcast admits that cybercriminals were able to exploit the CitrixBleed vulnerability to access customers' PII prior to Comcast's implementation of the vulnerability patch.

---

[87] Sam Sabin, *The security flaw haunting cyber defenders in 2024,* Axios (Jan. 2, 2024), https://www.axios.com/2024/01/02/citrix-bleed-security-hacks-impact.

[88] Dan Goodin, *Xfinity waited to patch critical Citrix Bleed 0-day. Now it's paying the price*, Ars Technica (Dec. 19, 2023 6:14 PM), https://arstechnica.com/security/2023/12/hack-of-unpatched-comcast-servers-results-in-stolen-personal-data-including-passwords/.

277. Comcast's Notice, however, failed to disclose how many consumers' PII was breached, leaving consumers to speculate whether it was likely that their own PII has been compromised. Based on a document that Comcast filed with the Maine Attorney General regarding the data breach, however, nearly 36 million former and current Xfinity customers had their PII compromised in the breach.[89]

278. The Notice also demonstrated that Comcast's internal investigation failed to identify which information was stolen for which users:

> On December 6, 2023, we concluded that the information included usernames and hashed passwords. For some customers, other information was also included, such as names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. However, our data analysis is continuing, and we will provide additional notices as appropriate.[90]

279. The Notice also failed to provide any offer of enhanced identity protection and credit monitoring service, and instead contained nothing more than boilerplate language about preventing identity theft and fraud, and simple (and woefully insufficient) suggestions about resetting passwords and setting up two-factor or multi-factor authentication.

H. Defendants Failed to Comply with Industry Standards and Regulatory Guidance Regarding Data Security Practices.

280. Because of the value of PII to hackers and identity thieves, companies that store, maintain, and secure customer PII, such as Comcast, or companies that provide the software and

---

[89] Office of the Maine AG, *Consumer Protection: Privacy, Identity Theft and Data Security Breaches*, https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml (last visited July 1, 2024).

[90] *Notice To Customers of Data Security Incident*, Xfinity, https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (last visited July 1, 2024).

hardware used to store, maintain, and secure customer PII, such as Citrix, are particularly vulnerable to cyber-attacks.

281. Comcast and Citrix knew their systems were handling and storing large amounts of PII belonging to Plaintiffs and other consumers. Just as banks should anticipate that they are attractive targets for thieves due to the large volumes of cash and other valuables that banks routinely store, Comcast and Citrix should have anticipated that their systems would be attractive targets for data thieves.

282. As a result, Comcast and Citrix knew or should have known that failure to safeguard their networks could cause foreseeable harm to the customers whose PII was contained in Defendants' systems.

283. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by companies that handle or facilitate the handling of customer PII, including, but not limited to: establishing secure password and authentication procedures for employees; building secure networks by setting up network protection tools like firewalls and constantly monitoring for and patching vulnerabilities; encrypting sensitive data using robust encryption algorithms; limiting access to customer data to only relevant staff; and training staff regarding critical points.[91] Indeed, Comcast and Citrix both recognize these best practices, and discuss many of them in their security and privacy protocols and policies.

284. Federal and State governments have likewise established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and

[91] *Customer Data Security: Best Practices for Data Privacy*, CDP, https://cdp.com/articles/customer-data-security-best-practices/; *Securing Networks: Best Practices for Cybersecurity in Telecommunications*, Prismecs, https://prismecs.com/blog/securing-networks-best-practices-for-cybersecurity-in-telecommunications (last visited July 1, 2024).

financial institutions. For example, Comcast is prohibited by the FTC Act 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 FTC Act.

285. The FTC has issued numerous guides for business outlining reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.[92]

286. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.[93] The guidelines note businesses should, among other best practices:

a. Protect the personal customer and consumer information that they keep;

b. Properly dispose of personal information that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.[94]

287. The guidelines further recommend that businesses implement an array of specific methods to protect its systems, such as:

a. Using an intrusion detection system to expose a breach as soon as it occurs;

---

[92] *Start with Security: A Guide for Business* at 2, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[93] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[94] *See id.*

b. Monitoring all incoming traffic for activity indicating someone is attempting to hack the system;

c. Watching for large amounts of data being transmitted from the system; and

d. Having a response plan ready in the event of a breach.[95]

288. The FTC also recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

289. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer 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 FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations. Indeed, just last year, the FTC brought an enforcement action against telecommunications provider Global Tel*Link Corporation for failing to secure the sensitive data of hundreds of thousands of individuals.[96]

290. Further, the National Institute of Standards in Technology ("NIST") publishes substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data

[95] *Id.*

[96] *FTC Finalizes Order with Global Tel*Link Over Security Failures that Led to Breach of Sensitive Data*, Federal Trade Comm'n (Feb. 23, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-finalizes-order-global-tellink-over-security-failures-led-breach-sensitive-data.

security controls, network monitoring, breach detection, and incident response.[97] Upon information and belief, Defendants failed to adhere to the NIST guidance.

291. Comcast and Citrix also have obligations created by additional laws, regulations, contracts, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to protect Plaintiffs' and Class Members' PII from unauthorized access and disclosure.

292. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain PII to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access. Similarly, California requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure." Cal. Civ. Code § 1798.81.5(b).

293. To provide another example, under the Cable Communications Policy Act, 47 U.S.C. § 551 (the "Cable Act"), cable operators like Comcast must not disclose PII without prior written or electronic consent of the subscriber, and must destroy PII of former subscribers. Cable operators must also provide annual notice of the nature of PII collected; the nature, frequency, and purpose of any disclosure; the period during which information will be maintained; and the times and place at which the subscriber may access such information. Comcast itself acknowledges the obligations imposed on it through the Cable Act and states that a consumer may "enforce the limitations imposed on us by the Cable Act as applicable with respect to your personally

[97] *Protecting Personal Information: A Guide for Business*, *supra,* note 93 at Table 2, 26-43.

identifiable information through a civil lawsuit seeking damages, attorneys' fees, and litigation costs."[98]

294. Comcast and Citrix were, at all times, fully aware of their obligations to comply with these laws, regulations and best practices to protect individuals' PII. Despite their duties, however, Comcast and Citrix failed to fully comply with industry-standard cybersecurity practices, including, but not limited to: proper firewall configuration, network segmentation, secure credential storage, user-activity monitoring, data-loss prevention, vigilant monitoring for and patching vulnerabilities, and intrusion detection and prevention.

295. As a result, Comcast and Citrix failed to adequately secure and protect Xfinity customers' PII, allowing Plaintiffs' and Class Members' PII to be stolen, disclosed, and misused.

I. The Data Breach Put Xfinity Customers at Imminent and Substantial Risk of Fraud, Identity Theft, and Other Cybercrimes.

296. Comcast's and Citrix's failure to keep Plaintiffs' and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, addresses, zip codes, phone numbers, email addresses, dates of birth, the last four digits of Social Security numbers, and usernames and passwords—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

297. On information and belief, Plaintiffs' and Class Members' PII from the Data Breach is already circulating on the "dark web." The dark web conceals users' identities and online

[98] *Our Privacy Policy*, Xfinity, https://www.xfinity.com/privacy/policy (last visited July 1, 2024).

activity, which makes it difficult for authorities to detect the location or owners of a website when illegally acquired information is disclosed or put up for sale.

298. Plaintiffs' stolen PII is circulating on the dark web because it is highly valuable and useful to cybercriminals. Malicious actors can use stolen PII such as a victim's name, date of birth, and last four digits of a Social Security number to, among other things, gain access to consumers' bank accounts, social media, credit card accounts, and other consumer accounts. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain unemployment or other government benefits, obtain government IDs, or create "synthetic identities," whereby a cybercriminal combines real and fake information to create a new "synthetic" identity which makes it even easier to commit fraud.

299. Importantly, even though full Social Security numbers were not involved in the Data Breach, as noted previously, cybercriminals can easily use the information involved in the Data Breach to reverse engineer an individual victim's full Social Security number. Using nothing but an individual's date of birth and state of residence, computer programs can easily predict the first five digits of an individual's Social Security number.[99] Cybercriminals can combine these reverse-engineered digits with the last four digits stolen in the Data Breach, and then use the victim's full, nine-digit Social Security number to gain access to the victim's accounts and commit more complicated types of fraud.

300. Plaintiffs and Class Members who were Xfinity Mobile or NOW Mobile customers specifically also face an imminent risk of falling victim to "SIM-swap" fraud. A SIM swap is a

[99] Xeni Jardin, *Reverse-engineering SSNs from publicly available data*, BoingBoing (July 6, 2009), https://boingboing.net/2009/07/06/reverse-engineering.html.

scheme whereby a hacker gains control of a victim's mobile phone number and service in order to intercept communications intended for the victim, including text messages that a victim's customer, financial, and medical accounts may use to verify the victim's identity for login purposes. Following a fraudulent SIM swap, the legitimate subscriber (now victim)'s phone loses connection to the wireless network, meaning they cannot use the wireless network to call, text, or use the internet, and they are inhibited in their attempts to warn their wireless carrier of the fraud. All phone calls and text messages that would normally have gone to the victim's phone now go to the imposter's phone. Hackers can thus easily use the victim's phone number as a key to access and take over the victim's other digital accounts, such as email, file storage, and financial accounts.

301. In addition to the risk of a SIM swap faced by Xfinity Mobile and NOW Mobile customers, all Xfinity customers impacted by the Data Breach also face a substantial and imminent risk of "port-out" fraud discussed previously, whereby cybercriminals hijack a victim's phone number using the victim's name, address, birth date, passwords, and the last four digits of their Social Security number.

302. Once cybercriminals start committing fraud and other identity theft-related crimes using a victim's PII, the disruption to the victim's life can be catastrophic. A study by the Identity Theft Resource Center ("ITRC") found that, among individuals who experienced fraudulent use of their PII, nearly all of them had experienced some form of costs or other harm in their lives, including having to borrow money, being forced out of their home or residence, and being unable to care for their family.[100] Indeed, as the U.S. Government Accountability Office ("GAO") found

[100] Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].

in a 2007 report, victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[101]

303. Further, although the theft of PII creates an imminent risk of becoming a victim of identity theft and fraud, malicious actors often wait months or years to use the PII obtained in data breaches. GAO determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[102] During this delay, victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. Some of the Plaintiffs and many of the Class Members are in their twenties and thirties, and these Plaintiffs must vigilantly monitor their financial accounts for many, many years to come.

304. Cybercriminals will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiffs' and Class Members' data may have been compromised in other data breaches, the fact that the Data Breach centralizes the PII and identifies the victims as Xfinity's current and former customers materially increases the risk to Plaintiffs and the Class.

305. Plaintiffs and Class Members are particularly at risk of additional data breaches because part of the PII stolen in the Data Breach involved their usernames and passwords, which makes it far more likely that Plaintiffs and Class Members will be victims of a future "credential stuffing" attack.

---

[101] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, U.S. Gov't Accountability Office (June 2007), https://www.gao.gov/assets/270/262899.pdf.

[102] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm.

306. Credential stuffing is a type of cyberattack in which the attacker collects stolen account credentials, typically consisting of lists of usernames or email addresses and the corresponding passwords (often from a data breach), and then uses the credentials to gain unauthorized access to user accounts on other systems through large-scale automated login requests that test whether the user's stolen credentials are *also* used for other systems and accounts. Credential stuffing was behind several notable recent data breaches, including 23andMe[103] and Roku.[104]

307. Even if cybercriminals use Plaintiffs' and Class Members' data to commit fraud and identity theft imminently, there is often a lag between when a person suffers harm due to theft of their PII and when they *discover* that harm. The substantial and imminent risk that Plaintiffs currently face therefore will not decrease over the next several months and years, and Plaintiffs will need to spend time and money to continuously monitor their accounts for years to ensure their PII is not used in malicious ways to harm them.

V. PLAINTIFFS' AND CLASS MEMBERS' INJURIES AND DAMAGES

308. Plaintiffs are current and former customers of Comcast, including current and former subscribers to Comcast's Xfinity Internet, TV/Cable, Phone/Voice, Home Security, and/or Xfinity Mobile services. Plaintiffs were required to provide PII to Comcast in exchange for access to these services, which Comcast had a duty to secure and safeguard.

---

[103] Mack DeGeurin, *Hackers got nearly 7 million people's data from 23andMe. The firm blamed users in 'very dumb' move*, The Guardian (Feb. 15, 2024), https://www.theguardian.com/technology/2024/feb/15/23andme-hack-data-genetic-data-selling-response.

[104] Jeffrey Burt, *Roku: Credential Stuffing Attacks Affect 591,000 Accounts*, Security Boulevard (Apr. 15, 2024), https://securityboulevard.com/2024/04/roku-credential-stuffing-attacks-affect-591000-accounts/.

309. As a direct and proximate result of Citrix's and Comcast's failure to institute adequate data security measures, Plaintiffs and Class Members were injured and incurred damages when third-party cybercriminals breached Citrix's products and Comcast's systems and stole Plaintiffs' and Class Members' PII.

310. Indeed, Plaintiffs' PII was compromised as a direct and proximate result of the Data Breach. While Comcast knew of the CitrixBleed vulnerability as early as October 10, 2023, Comcast waited at least *thirteen days* to patch the vulnerability, leaving Plaintiffs' PII vulnerable to cybercriminals. Moreover, Plaintiffs did not start receiving the Notice until around December 20, 2023, at the earliest—over two months after the vulnerability was announced and the Data Breach occurred. Like Plaintiffs, Class Members' PII was also compromised as a direct and proximate result of the Data Breach.

311. The harm faced by Plaintiff and Class Members is substantial and imminent, as unauthorized cybercriminals now have possession of their information, available for their use however and whenever they see fit, including posting or selling that information on the dark web. Defendants acknowledge that the risk borne by Plaintiffs and Class Members is a real one, as evidenced by the Notice sent by Comcast to Plaintiffs, which advises Plaintiffs to remain vigilant, monitor their credit, and engage in preventative measures to avoid identity theft.

312. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been injured in a myriad of other ways.

313. First, Plaintiffs and Class Members face immediate and substantial risk of identity theft or fraud, such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members also face substantial risk of being targeted for future phishing, data

intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs in the near future. This harm can be quantified by putting Plaintiffs and the Class in the position they would have been in but for the Data Breach, including by quantifying the cost of high-quality monitoring for Plaintiffs and the Class.

314. Second, as noted previously, there is often a lag between cybercriminals' acquisition of PII and use of that information to commit fraud, identity theft, phishing, and other schemes. As a direct and proximate result of Comcast's and Citrix's conduct, Plaintiffs and Class Members must incur and continue to incur out-of-pocket costs for protective measures such as on-going high quality credit monitoring and additional costs for credit report fees, and similar costs directly related to the Data Breach, for years to come.

315. Third, and relatedly, Plaintiffs and Class Members have and will suffer ascertainable losses in the form of out-of-pocket expenses and the loss of the value of their time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Placing "freezes" and "alerts" with credit reporting agencies;

f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

g. Contacting financial institutions and closing or modifying financial accounts;

h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

j. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come; and

k. Interacting with government agencies and law enforcement to address the impact and harm caused by this breach.

316. Fourth, Plaintiffs have lost the value of their PII because the information is a valuable commodity. PII is a valuable commodity on the black market, and one study of PII vendors on the dark web estimated that a limited group of vendors received more than $140 million from the sale of stolen PII in just eight months.[105] Indeed, PII is a valuable asset even among legal companies and entities,[106] with "Big Data" corporations like Alphabet, Inc. earning hundreds of *billions* of dollars annually in recent years by leveraging PII that they collect.[107] Some companies are now explicitly offering consumers money in exchange for a non-exclusive license to use their personal information, up to nearly $50 per month.[108] Thus, PII has considerable market value that is diminished when it is compromised.

---

[105] Christian J. Howell & David Maimon, *Darknet markets generate millions in revenue selling stolen personal data, supply chain study finds*, The Conversation (Dec. 2, 2022, 8:42 AM), https://theconversation.com/darknet-markets-generate-millions-in-revenue-selling-stolen-personal-data-supply-chain-study-finds-193506.

[106] *See, e.g.*, John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

[107] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

[108] Tatum Hunter, *These companies will pay you for your data. Is it a good deal?*, Washington Post (Feb. 6, 2023, 6:00 AM), https://www.washingtonpost.com/technology/2023/02/06/consumers-paid-money-data/.

317. Fifth, Plaintiffs are, at the very least, entitled to nominal damages for Comcast's and Citrix's violations as discussed herein. As a result of Comcast's and Citrix's failure to safeguard Plaintiffs' and Class Members' PII, Plaintiffs and Class Members are forced to live with the knowledge that their PII—which contains private and personal details of their life—has likely been disclosed or made available for sale to the entire world online, thereby making them vulnerable to cybercriminals, permanently subjecting them to loss of security, and depriving Plaintiffs and Class Members of their fundamental right to privacy.

318. Sixth, Plaintiffs are entitled to statutory damages, as provided, based upon the relevant causes of action alleged herein, and described below.

319. Seventh, Comcast and Citrix were unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Among other things, Comcast continues to benefit and profit from their PII while its value to Plaintiffs and Class Members has been diminished.

320. Finally, Plaintiffs and Class Members have an interest in ensuring that their PII, which remains in the possession of Comcast is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Plaintiffs' and Class Members' data is not accessible online and that access to such data is limited and secured.

VI. CLASS ACTION ALLEGATIONS

321. Plaintiffs bring this action on their own behalf and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as "Class Members."

322. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), and (c)(4) as applicable, Plaintiffs propose the following Nationwide Class and Subclass definitions, subject to amendment as appropriate:

> **Nationwide Class**: All natural persons residing in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach.

323. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs propose the following Cable Communications Policy Act Subclass (the "Cable Act Subclass"), on behalf of all individuals who are/were Xfinity Cable Television, Xfinity TV, Xfinity Internet, or Xfinity Voice customers, subject to amendment as appropriate:

> **Cable Act Subclass**: All natural persons residing in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach, and who received Xfinity Residential Services (including Xfinity Cable Television, Xfinity TV, Xfinity Internet, and/or Xfinity Voice).

324. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs propose the following state-by-state claims in the alternative to the nationwide claims, as well as statutory claims brought under state data breach and consumer protection statutes, on behalf of statewide subclasses for each State (the "Statewide Subclasses"), subject to amendment as appropriate:

> **[State] Subclass**: All natural persons residing in [name of state or territory] whose Personally Identifiable Information was compromised as a result of the Data Breach.

325. Excluded from the Class and Subclasses are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, 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 their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

326. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

327. **Numerosity under Federal Rule of Civil Procedure 23(a)(1).** The members of the Class (and Subclasses) are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the class consists of millions of persons whose data was compromised in the Data Breach who can be identified by reviewing the PII exfiltrated from Comcast's databases. Based upon public filings, the current number of people impacted is approximately 36 million.

328. **Commonality under Federal Rule of Civil Procedure 23(a)(2).** There are questions of law and fact common to Plaintiffs and Class Members, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Comcast unlawfully used, maintained, or disclosed Plaintiffs' and the Class Members' PII;

b. Whether Comcast and Citrix failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

c. Whether Comcast and Citrix truthfully represented the nature of their security systems, including their vulnerability to hackers;

d. Whether Comcast's and Citrix's data security protocols prior to and during the Data Breach complied with applicable data security laws and regulations;

e. Whether Comcast's and Citrix's data security protocols prior to and during the Data Breach were consistent with industry standards;

f. Whether Comcast and Citrix each owed a duty to Class Members to safeguard their PII;

g. Whether Comcast and Citrix breached their duties to Class Members to safeguard their PII;

h. Whether cyberhackers obtained, sold, copied, stored or released Class Members' PII;

i. Whether Comcast and Citrix knew or should have known that their data security programs and monitoring processes were deficient;

j. Whether and when Comcast and Citrix actually learned of the Data Breach;

k. Whether Comcast adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII was compromised;

l. Whether Comcast violated the law by failing to adequately, promptly, and accurately inform Plaintiffs and Class Members that their PII was compromised;

m. Whether the Class Members suffered legally cognizable damages as a result of Comcast's and Citrix's misconduct; and

n. Whether Plaintiffs and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

329. **Typicality under Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of those of the Class Members because Plaintiffs' PII, like that of every class member, was compromised in the Data Breach.

330. **Adequacy of Representation under Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs will fairly and adequately represent and protect the interests of Class Members, including those from states and jurisdictions where they may not reside. Plaintiffs' Counsel are competent and experienced in litigating class actions and were appointed to lead this litigation by the Court pursuant to Federal Rule of Civil Procedure 23(g).

331. **Predominance under Federal Rule of Civil Procedure 23(b)(3).** Comcast and Citrix have each engaged in a common course of conduct toward Plaintiffs and Class Members, in that all Plaintiffs' and the Class Members' data at issue here was stored by Comcast using Citrix appliances and was accessed during the Data Breach. The common issues arising from Comcast's and Citrix's respective conduct affecting Class Members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

332. **Superiority under Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Comcast and Citrix. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

333. **Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2).** Comcast and Citrix both failed to take actions to safeguard Plaintiffs' and Class Members' PII such that injunctive relief is appropriate and necessary. Comcast and Citrix have each acted on grounds that apply generally to the Class (and Subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

334. **Issue Certification is Appropriate under Federal Rule of Civil Procedure 23(c)(4).** In the alternative, this litigation can be brought and maintained as a class action with respect to particular issues, such as Comcast's and Citrix's respective liability in regard to the foregoing causes of action.

VII. CAUSES OF ACTION

335. Plaintiffs bring these causes of action on behalf of the Nationwide Class and State Subclasses, as defined herein. The application of one specific state's laws to any cause of action

is premature at this juncture, without the benefit of discovery, as Comcast maintained servers and Citrix NetScaler appliances in several states, and Xfinity customers exist across the United States.

A. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1: CABLE COMMUNICATIONS POLICY ACT 47 U.S.C. §§ 521 *et seq.*

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Cable Act Subclass, against Comcast only)

336. Plaintiffs restate and reallege all foregoing factual allegations as if fully set forth herein.

337. The Cable Communications Policy Act provides in relevant part that "a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator." 47 U.S.C § 551(c).

338. The Cable Communications Policy Act further provides that a "[a]ny person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court." 47 U.S.C § 551(f)(1).

339. Comcast is a cable operator as it "provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system," or "otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system." 47 U.S.C. § 522(5).

340. Comcast's provision of Xfinity TV and cable services to Plaintiffs and Class Members qualifies as "cable services" as defined by the Cable Communications Policy Act because such services include "the one-way transmission to subscribers of video programming or

other programming service and subscriber interaction which is required for the selection or use of the video programming or other programing service." 47. U.S.C. § 522 (6).

341. Comcast's provision of Internet service to Plaintiffs and Class Members separately qualifies as an "other service" as defined by the Cable Communications Policy Act because such Internet service is a "wire or radio communication[] service provided using any of the facilities of a cable operator that are used in the provision of cable service." 47 U.S.C § 551(a)(2).

342. Comcast's provision of Xfinity Voice service to Plaintiffs and Class Members also separately qualifies as an "other service" as defined by the Cable Communications Policy Act because such Voice service is a "wire or radio communication[] service provided using any of the facilities of a cable operator that are used in the provision of cable service." 47 U.S.C § 551(a)(2).

343. Plaintiffs' and Class Members' PII is "personally identifiable information" within the meaning of 47 U.S.C § 551.

344. Plaintiffs and Class Members are "subscribers" of Comcast's "cable services" and "other services" within the meaning of 47 U.S.C. § 551 because they have paid for and/or purchased cable/television service, internet service, and/or mobile service from Comcast.

345. At all relevant times hereto, pursuant to 47 U.S.C. § 551, Comcast was required to take such actions as necessary to prevent unauthorized access to Plaintiffs' and Class Members' PII by a person other than the subscriber or cable operator.

346. Comcast violated 47 U.S.C § 551(c) by failing to prevent unauthorized access to Plaintiffs' and Class Members' PII by unauthorized third parties. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiffs at this time, on information and belief, Comcast violated 47 U.S.C §§ 551(c) and (e) through some combination of the following errors and omissions that allowed the Data Breach to occur: (a) mismanaging its

system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII; (i) failing to timely patch known vulnerabilities to its computer systems or networks; and (j) failing to destroy PII no longer necessary for the purpose for which it was collected.

347. As a direct and proximate result of Comcast's violation of 47 U.S.C § 551(c), (e), Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII;

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

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Comcast with the mutual understanding that Comcast would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Comcast's possession and is subject to further breaches so long as Comcast fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

348. As a direct and proximate result of Comcast's violation of the Cable Communications Policy Act, Plaintiffs and Class Members seek statutory damages of at least $1,300 per subscriber per violation or actual damages (the statute awards damages of $100 per day or $1,000, whichever is greater, and Comcast's violation lasted from approximately October 10–23, 2023), as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COUNT 2: NEGLIGENCE

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses, against Comcast only)

349. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

350. Comcast required Plaintiffs and Class Members to submit their sensitive PII in order to obtain or apply for its products and/or services.

351. Comcast owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting

their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Comcast's security systems to ensure that Plaintiffs' and Class Members' PII in Comcast's possession was adequately protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generating by its own security systems, regarding instructions to its networks or systems; (d) maintaining security measures consistent with industry standards; (e) exercising appropriate discretion in selecting third-party vendors with whom it makes Plaintiffs' and Class Members' PII available; (f) exercising appropriate control over Citrix's data security practices, and (g) timely rectifying known vulnerabilities its networks or systems.

352. Comcast's duty to use reasonable care arose from several sources, including but not limited to those described below.

353. Comcast has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Comcast. By receiving, maintaining, and handling valuable PII that is routinely targeted by criminals for unauthorized access and use for nefarious purposes, Comcast was obligated to act with reasonable care to protect against these foreseeable threats.

354. Comcast also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Comcast's conduct included its failure to adequately restrict access to its computer networks and systems that held Plaintiffs' and Class Members' PII, as Comcast knew it was more than likely than not Plaintiffs and Class Members would be harmed if it allowed such a breach of its computer networks and systems.

355. Comcast's duty also arose as a result of the special relationship that existed between Comcast, on the one hand, and Plaintiffs and Class Members on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted Comcast with their PII as part of the applications for and/or purchase and signing up for the products Comcast offers as a major telecommunications company. Comcast alone could have ensured that its security systems were sufficient to prevent or minimize the Data Breach.

356. Comcast's duty also arose from Comcast's unique position as one of the largest telecommunications companies in the United States. As a telecommunications company, Comcast holds itself out as a protector of consumer data and thereby assumes a duty to reasonably protect the PII that it was entrusted by Plaintiffs and Class Members. Comcast has stated that "[w]e know you rely on us to stay connected to the people and things you care about most and your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure and put you in control of it."[109] Because of its role as one of the largest telecommunications companies in the U.S., Comcast was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

357. Comcast admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect Plaintiffs' and Class Members' PII.

358. Further, Comcast's duty arose from various statutes requiring Comcast to implement reasonable data security measures, including but not limited to: Section 5 of the FTC Act. For example, Section 5 of the FTC Act required Comcast to take reasonable measures to protect Plaintiffs' and the Class's sensitive data and is a further source of Comcast's duty to

[109] *Privacy*, Xfinity, https://www.xfinity.com/privacy (last visited July 1, 2024).

Plaintiffs and the Class. Section 5 of the FTC Act prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Comcast for failing to use reasonable measures to protect highly sensitive data. Therefore, Comcast was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Comcast's duties to adequately protect sensitive information.

359. Comcast is subject to an "independent duty," untethered to any contract between Comcast and Plaintiffs and Comcast and Class Members. The sources of Comcast's duty are identified above.

360. Comcast breached the duties owed to Plaintiffs and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiffs at this time, on information and belief, Comcast breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its customers; (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and

databases containing sensitive PII; and (i) failing to timely patch known vulnerabilities to its computer systems or networks.

361. But for Comcast's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

362. Comcast's failure to implement adequate security measures to protect the sensitive PII of Plaintiffs and Class Members created conditions conductive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' PII.

363. Plaintiffs and Class Members were the foreseeable victims of Comcast's inadequate data security measures, and it was also foreseeable that Comcast's failure to protect Plaintiffs' and Class Members' PII would result in injury to Plaintiffs and Class Members as described in this Consolidated Class Action Complaint.

364. As a direct and proximate result of Comcast's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII;

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

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Comcast with the mutual understanding that Comcast would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Comcast's possession and is subject to further breaches so long as Comcast fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

365. As a direct and proximate result of Comcast's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT 3: NEGLIGENCE PER SE

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses, against Comcast only)

366. Plaintiffs restate and reallege all foregoing factual allegations as if fully set forth herein.

367. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Comcast for failing to use reasonable measures to protect consumer PII. Various FTC publications and orders also form the basis of Comcast's duty.

368. Comcast violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumer PII and not complying with the industry standards. Comcast's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving a company as large as Comcast, including the damages that would result to Plaintiffs and Class Members.

369. Comcast's violation of Section 5 of the FTC Act constitutes negligence *per se*.

370. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

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

372. Comcast also violated the Cable Communications Policy Act as described in Count I of the Consolidated Complaint.

373. Comcast's violation of the Cable Communications Policy Act also constitutes negligence *per se*.

374. Plaintiffs and Class Members are subscribers of "cable services" and "other services" within the class of persons the Cable Communications Policy Act was intended to protect. And the harm that has occurred is the type of harm that the Cable Communications Policy Act was intended to guard against. Indeed, the Cable Communications Policy Act was intended to protect subscribers from the harm caused by the unauthorized disclosure and unlawful retention of subscribers' PII—the same harms alleged herein.

375. Comcast breached its duties to Plaintiffs and Class Members under Section 5 of the FTC Act and the Cable Communications Policy Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

376. Plaintiffs and Class Members were foreseeable victims of Comcast's violations of Section 5 of the FTC Act and the Cable Communications Policy Act. Comcast also knew or should

have known that its failure to implement reasonable data security measures to protect and secure Plaintiffs' and Class Members' PII would cause damage to Plaintiffs and Class Members.

377. But for Comcast's violation of the applicable laws and regulations, Plaintiffs' and Class Members' PII would not have been compromised by unauthorized third parties.

378. As a direct and proximate result of Comcast's negligence *per se*, Plaintiffs and Class Members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT 4: BREACH OF EXPRESS CONTRACT

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses, against Comcast only)

379. Plaintiffs restate and reallege all foregoing paragraphs as if fully set forth herein.

380. Comcast's Privacy Policy[110] is an agreement between Comcast and individuals who provided their PII to Comcast, including Plaintiffs and Class Members.

381. Comcast's Privacy Policy states that "it applies to the information we collect when you use or interact with the business entities, products, services, networks, and platforms, including our websites, mobile apps, and other services and devices where this policy is referenced. These may include Xfinity-branded services, Comcast-branded Services, Xumo-branded Services, and other products and services we deliver."[111]

382. Comcast's Privacy Policy stated at the time of the Data Breach that Comcast uses "technical, administrative, and physical safeguards" so "secure the information we collect to

[110] Citations throughout Count 3 are to *Privacy Policy*, Xfinity (effective Sept. 20, 2023), https://web.archive.org/web/20231004141125/https://www.xfinity.com/privacy/policy/.

[111] Examples of when the Privacy Policy applies include: "Xfinity® TV and Streaming, Xfinity Internet, xFi and Xfinity Advanced Security, Xfinity Voice, Xfinity Stream app, Xfinity WiFi service, Xfinity Home, Xfinity Mobile, Xfinity Flex, Comcast Business Services, Effectv, Xumo, Xumo TV, Xumo Play."

prevent the unauthorized access, use, or disclosure of any personal information that we collect and maintain."

383. Comcast further promised at the time of the Data Brech that it would only share Plaintiffs' and Class Members' data under certain enumerated circumstances, which include: "The Comcast family of business;" "Account owners and other authorized users;" "Service providers," such as billing and collection providers, accounting, auditing and tax providers, and marketing, advertising, and sales programs; and "Third parties," such as online advertising partners, consumer reporting agencies, and directory services. None of the enumerated circumstances involve sharing Plaintiffs' or Class Members' PII with unauthorized third parties.

384. Comcast emphasized in its Privacy Policy at the time of the Data Breach that "we take our responsibility of safeguarding your personal information seriously" and further referenced the "Xfinity Privacy Center," which stated that "[w]e know you rely on us to stay connected to the people and things you care about most and your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure and put you in control of it."[112]

385. Plaintiffs and Class Members on the one side, and Comcast on the other, formed a contract when Plaintiffs and Class Members obtained products or services from Comcast, or otherwise provided PII to Comcast subject to its Privacy Policy.

386. Plaintiffs and Class Members fully performed their obligations under the contracts with Comcast.

[112] https://web.archive.org/web/20231028014023/https://www.xfinity.com/privacy (captured Oct. 28, 2023).

387. Comcast breached its agreements with Plaintiffs and Class Members by failing to protect their PII. Specifically, Comcast: (1) failed to take reasonable steps to secure its computer networks and systems to protect PII; and (2) disclosed Plaintiffs' and Class Members' PII to unauthorized third parties, in violation of the agreement.

388. As a direct and proximate result of Comcast's breach of contract. Plaintiffs and Class Members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Such injuries include: lost benefit of their bargains, overcharges for services or products, and those described herein.

COUNT 5: BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses, against Comcast only)

389. Plaintiffs restate and reallege all foregoing factual allegations as if fully set forth herein.

390. Plaintiffs and Class Members entered into implied contracts with Comcast when they obtained products or services from Comcast, or otherwise provided PII to Comcast. Indeed, Plaintiffs and Class Members were required to provide their PII to Comcast as a condition of using Comcast's products and/or services.

391. In doing so, Plaintiffs and Class Members entered into implied contracts with Comcast by which Defendant agreed to safeguard and protect such PII and keep such PII secure and confidential.

392. When entering into these implied contracts, Plaintiffs and Class Members reasonably believed and expected that Comcast's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and to timely notify them of a data breach. Plaintiffs and Class Members further reasonably believed and

expected that Comcast would use part of the monies paid to Comcast under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund adequate and reasonable data security measures.

393. Indeed, implicit in these exchanges was a promise by Comcast to ensure the PII of Plaintiffs and Class Members in its possession would be used to provide the agreed-upon services and that Comcast would take adequate measures to protect Plaintiffs' and Class Members' PII.

394. It is clear by these exchanges that the Parties intended to enter into implied agreements supported by mutual assent. Plaintiffs and Class Members would not have disclosed their PII to Comcast but for the prospect of Comcast's promise of services and/or products. Conversely, Comcast presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class Members with products and services.

395. Plaintiffs and Class Members would not have provided their PII to Comcast or would have paid less for Comcast services or products in the absence of the implied contract between them and Comcast as the safeguarding of Plaintiffs' and Class Members' PII was critical to realize the intent of the parties.

396. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Comcast.

397. Comcast breached its implied contracts with Plaintiffs and Class Members by failing to protect their PII. Specifically, Comcast: (1) failed to take reasonable steps to secure its computer networks and systems to protect PII; and (2) disclosed Plaintiffs' and Class Members' PII to unauthorized third parties, in violation of the agreement.

398. As a direct and proximate result of Comcast's breach of implied contract. Plaintiffs and Class Members have been injured and are entitled to damages, including compensatory,

punitive, and nominal damages, in an amount to be proven at trial. Such injuries include: lost benefit of their bargains, overcharges for services or products, and those described above herein.

COUNT 6: UNJUST ENRICHMENT

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses, against Comcast only)

399. Plaintiffs restate and reallege all foregoing factual allegations, except those under Counts 4 and 5, as if fully set forth herein.

400. Plaintiffs bring this claim in the alternative to their breach of express and breach of implied contract claims.

401. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Comcast and that was ultimately compromised in the Data Breach.

402. By engaging in the conduct described in this Complaint, Comcast has knowingly obtained and derived benefits from Plaintiffs and Class Members at Plaintiffs' and Class Members' expense, namely the profits gained from payment in exchange for the use of Comcast's services, such that it would be inequitable and unjust for Defendant to retain.

403. Comcast also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended on Comcast maintaining the privacy and confidentiality of that PII.

404. But for Comcast's willingness and commitment to maintaining Plaintiffs' and Class Members' PII, that PII would not have been transferred to and entrusted with Comcast.

405. Comcast admits that it uses the PII it collects for, among other things, advertising and marketing for its own and others' products and services, to improve its services, "develop new products and services, give recommendations, deliver personalized consumer experiences."[113]

406. Because of its use of Plaintiffs' and Class Members' PII, Comcast has sold more services and products than it otherwise would have. Comcast was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiffs and Class Members.

407. Further, by engaging in the acts and failures to act described in this Consolidated Amended Complaint, Comcast has been knowingly enriched by the savings in costs that should have been reasonably expensed to protect the PII of Plaintiffs and the Class. Comcast knew or should that known that theft of consumer PII could happen, yet it failed to take reasonable steps to pay for the level of security required to have prevented the theft of its consumers' PII.

408. Comcast's failure to direct profits derived from Plaintiffs' and Class Members' payments for services toward safeguarding Plaintiffs' and Class Members' PII constitutes the inequitable retention of a benefit without payment for its value.

409. Comcast will be unjustly enriched if it is permitted to retain the benefits derived after the theft of Plaintiffs' and Class Members' PII.

410. It is inequitable, unfair, and unjust for Comcast to retain these wrongfully obtained benefits. Comcast's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience

[113] https://web.archive.org/web/20231004141125/https://www.xfinity.com/privacy/policy/ (captured Oct. 4, 2023).

411. The benefit conferred upon, received, and enjoyed by Comcast was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Comcast to retain the benefit.

412. Comcast's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiffs and Class Members other damages as described herein.

413. Plaintiffs and Class Members have no adequate remedy at law.

414. Comcast is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Comcast as a result of its wrongful conduct, including specifically: the value to Comcast of the PII that was stolen in the Data Breach; the profits Comcast received and is receiving from the use of that information; the amounts that Comcast overcharged Plaintiffs and Class Members for use of Comcast's products and services; and the amounts that Comcast should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

COUNT 7: NEGLIGENCE

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses, against Citrix only)

415. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

416. Plaintiffs and Class Members were required to submit their sensitive PII to Comcast in order to obtain or apply for its products and/or services. To collect, manage, and store the data that Plaintiffs and Class Members entrusted to Comcast, Comcast utilized allegedly secure appliances/software produced and maintained by Citrix.

417. Citrix, as an entity that helps to store and maintain Plaintiffs' and Class Members' PII, owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in securing, safeguarding, and protecting their PII from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Citrix's appliances and security systems to ensure that Plaintiffs' and Class Members' PII in Citrix's clients' possession, including Comcast's possession, was adequately protected; (b) implementing processes that would detect vulnerabilities or breaches of its systems in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own systems and those publicized by third-parties, regarding its networks or systems; (d) maintaining security measures consistent with industry standards; and (e) timely rectifying known vulnerabilities its networks or systems.

418. Citrix's duty to use reasonable care arose from several sources, including but not limited to those described below.

419. Citrix has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Citrix. By helping its customers maintain and handle valuable PII that is routinely targeted by criminals for unauthorized access and use for nefarious purposes, Citrix was obligated to act with reasonable care to protect against these foreseeable threats.

420. Citrix also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Citrix's conduct included its failure to adequately test its products, networks, and systems that stored and managed Plaintiffs' and Class Members' PII, as

Citrix knew it was more than likely than not Plaintiffs and Class Members would be harmed if it failed to timely disclose and patch a vulnerability in its products used by Comcast.

421. Citrix's duty also arose, indirectly, as a result of the special relationship that existed between Comcast and its customers, including Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Comcast with their PII as part of the applications for and/or purchase and signing up for the products Comcast offers as a major telecommunications company, which Comcast in turn then entrusted to software and products produced and managed by Citrix. Citrix alone could have ensured that its own security systems were sufficient to prevent or minimize the Data Breach.

422. Citrix's duty also arose from Citrix's unique position as one of the largest cloud computing and virtualization companies in the United States. As a large, multinational technology company, Citrix holds itself out as a protector of data collected by its customers, including Comcast, and thereby assumes a duty to reasonably protect the PII that Plaintiffs and Class Members entrusted to Comcast and, by extension, Citrix. Citrix has stated that: "For almost 30 years, our customers have trusted our ability to handle their data with care and respect. That's why organizations from the most highly regulated sectors rely on us to protect their most sensitive information wherever work happens."[114] Indeed, because of its role as one of the largest office technology companies in the U.S., Citrix was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

423. Further, Citrix's duty arose from various statutes requiring Citrix to implement and utilize reasonable data security measures, including but not limited to Section 5 of the FTC Act. Section 5 of the FTC Act prohibits unfair practices in or affecting commerce, including, as

[114] https://www.citrix.com/about/trust-center/privacy-compliance.html (last visited July 1, 2024).

interpreted and enforced by the FTC, the unfair act or practice by businesses like Citrix of failing to use reasonable measures to protect highly sensitive data. Therefore, Citrix was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein, as well as other federal and state laws and regulations, thus form the basis of Citrix's duties to adequately protect sensitive information.

424. Citrix is subject to an "independent duty," untethered to any contract that may exist between Citrix and Plaintiffs and Citrix and Class Members. The sources of Citrix's duty are identified above.

425. Citrix breached the duties owed to Plaintiffs and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties to exploit the CitrixBleed vulnerability are unclear at this time, on information and belief, Citrix breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of its NetScaler products and other products, which resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to adequately engage in penetration and vulnerability testing to assess and mitigate these risks; (d) failing to design and implement safeguards to control these risks; (e) failing to adequately test and monitor the effectiveness of the safeguards' controls, systems, and procedures; (f) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (g) failing to detect the CitrixBleed vulnerability and exploitation thereof at the time the exploitation began or within a reasonable time thereafter; (h) failing to

follow its own privacy policies and practices published to its customers; (i) failing to adequately train and supervise employees regarding the risk inherent to its customers' use of its products to collect, manage, and store sensitive PII; and (j) failing to timely identify and patch known vulnerabilities in its products, systems, or networks.

426. But for Citrix's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

427. Citrix's failure to implement adequate security measures to protect the sensitive PII of Plaintiffs and Class Members created conditions conductive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' PII.

428. Plaintiffs and Class Members were the foreseeable victims of Citrix's inadequate data security measures, and it was also foreseeable that Citrix's failure to protect Plaintiffs' and Class Members' PII would result in injury to Plaintiffs and Class Members as described in this Consolidated Class Action Complaint.

429. As a direct and proximate result of Citrix's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII;

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

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Citrix with the mutual understanding that Citrix would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in the possession of Citrix's customers, namely Comcast, and is subject to further breaches so long as Citrix fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

430. As a direct and proximate result of Citrix's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT 8: NEGLIGENCE PER SE

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses, against Citrix only)

431. Plaintiffs restate and reallege all foregoing factual allegations as if fully set forth herein.

432. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Citrix for failing to use reasonable measures to protect consumer PII. Various FTC publications and orders also form the basis of Citrix's duty.

433. Citrix violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumer PII and not complying with the industry standards. Citrix's conduct was particularly unreasonable given the nature and amount of PII that Citrix's customers, such as

Comcast, obtained and stored, and the foreseeable consequences of a data breach involving Citrix's widely used NetScaler products, including the damages that would result to Plaintiffs and Class Members.

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

435. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

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

437. Citrix breached its duties to Plaintiffs and Class Members under Section 5 of the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

438. Plaintiffs and Class Members were foreseeable victims of Citrix's violations of Section 5 of the FTC Act. Citrix also knew or should have known that its failure to implement reasonable data security measures to protect and secure Plaintiffs' and Class Members' PII would cause damage to Plaintiffs and Class Members.

439. But for Citrix's violation of the applicable laws and regulations, Plaintiffs' and Class Members' PII would not have been compromised by unauthorized third parties.

440. As a direct and proximate result of Citrix's negligence *per se*, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT 9: DECLARATORY JUDGMENT

(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses, against both Defendants)

441. Plaintiffs restate and reallege all foregoing factual allegations as if fully set forth herein.

442. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described herein.

443. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Comcast and Citrix are each currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Comcast's and Citrix's respective data security measures remain inadequate. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur for as long as Comcast and Citrix each maintain inadequate data security measures.

444. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Comcast owes a legal duty to secure consumers' PII under the common law, Section 5 of the FTC Act, and the Cable Communications Policy Act;

b. Citrix owes a legal duty to secure consumers' PII under the common law and Section 5 of the FTC Act;

c. Comcast continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiffs' and Class Members' PII; and

d. Citrix continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiffs' and Class Members' PII.

445. This Court also should issue corresponding prospective injunctive relief requiring Comcast and Citrix to each employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

446. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Comcast or another entity using Citrix's appliances. The risk of another such breach is real, immediate, and substantial. If another breach at Comcast or a similar entity occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

447. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Comcast or Citrix if an injunction is issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Comcast and Citrix of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Comcast and Citrix each have a pre-existing legal obligation to employ such measures.

448. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Comcast or a similar entity, thus eliminating the additional injuries that would result to Plaintiffs and consumers whose confidential information would be further compromised.

B. CLAIMS ON BEHALF OF THE STATE SUBCLASSES

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 10: CALIFORNIA CUSTOMER RECORDS ACT,
Cal. Civ. Code §§ 1798.80, *et seq*.
(On behalf of California Plaintiffs and the California Subclass, against Comcast only)

449. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the foregoing factual allegations as if fully alleged herein.

450. This claim is brought individually under the laws of California and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

451. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

452. Comcast is a business that owns, maintains, and licenses "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Plaintiff and California Sub Class Members.

453. Businesses that own or license computerized data that includes personal information, including Social Security numbers, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach

notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." *Id.*

454. Comcast is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

455. Plaintiff's and California Subclass Members' PII includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

456. Because Comcast reasonably believed that Plaintiff's and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Comcast had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

457. By failing to disclose the Data Breach in a timely and accurate manner, Comcast violated Cal. Civ. Code § 1798.82.

458. As a direct and proximate result of Comcast's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members suffered damages, as described above.

459. Plaintiff and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 11: CALIFORNIA UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code §§ 17200, *et seq*.

(On behalf of California Plaintiffs and the California Subclass, against Comcast only)

460. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeat and allege the preceding factual allegations as if fully alleged herein.

461. This claim is brought individually under the laws of California and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair competition.

462. Comcast is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

463. Comcast violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and fraudulent or deceptive business acts and practices.

464. Comcast's "unfair," "fraudulent," and "deceptive" acts and practices include:

a. Failing to implement and maintain reasonable security measures to protect Plaintiffs' and California Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Comcast failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security after previous cybersecurity incidents. For example, Comcast failed to timely patch the CitrixBleed vulnerability, which allowed cybercriminals to penetrate Comcast's systems. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the California Subclass, whose PII has been compromised;

b. Failing to implement and maintain reasonable security measures in a way that was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including California's Consumer Legal Remedies Act ("CLRA"), Cal Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq*., and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5;

c. Failing to implement and maintain reasonable security measures which led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Comcast's inadequate security, consumers could not have reasonably avoided the harms that the Data Breach caused;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass

Members' PII, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, and the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California Subclass Members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' PII, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, and the FTC Act, 15 U.S.C. § 45;

h. Failing to timely and adequately notify the Plaintiffs and California Subclass Members of the Data Breach; and

i. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

465. Comcast has engaged in "unlawful" business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §§ 1798.80, *et seq.*, the CLRA, Cal. Civ. Code §§ 1780, *et seq.*, 15 U.S.C. § 680, *et seq.,* and the FTC Act, 15 U.S.C. § 45.

466. Comcast's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' PII, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, and the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass

Members' PII, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, and the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California Subclass Members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' PII, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, and the FTC Act, 15 U.S.C. § 45; and

h. Failing to timely and adequately notify the Plaintiffs and California Subclass Members of the Data Breach;

467. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII, and thus deceived consumers into believing that their PII was not exposed and that they did not need to take actions to secure their identities.

468. As a direct and proximate result of Comcast's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass Members were injured and lost money or property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII, including but not limited to the diminishment of their present and future property interest in their PII and the deprivation of the exclusive use of their PII.

469. Comcast acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and California Subclass Members' rights.

470. Plaintiffs and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Comcast's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable

attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 12: CALIFORNIA CONSUMER LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, *et seq*.

(On behalf of California Plaintiffs and the California Subclass, against Comcast only)

471. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein.

472. This claim is brought individually under the laws of California and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer legal remedies.

473. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

474. Comcast is a "person" as defined by Civil Code §§ 1761(c) and 1770 and has provided "services" as defined by Civil Code §§ 1761(b) and 1770. Specifically, Comcast provides telecommunications services to consumers including cable, internet, phone, and other services, which involve the collection and storage of PII.

475. As part of the services Comcast offers, Comcast touts its ongoing efforts to keep consumers' PII secure, as discussed *supra*.

476. Plaintiffs and the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

477. Comcast's acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the California Subclass Members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

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

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not;

e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, among other statutes;

j. Failing to timely and adequately notify the Plaintiffs and California Subclass Members of the Data Breach;

k. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and California Subclass Members' PII; and

l. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*

478. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII.

479. Had Comcast disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Comcast would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Comcast was trusted with the sensitive and valuable PII of millions of consumers, including Plaintiffs, the Class, and the California Subclass. Comcast accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Comcast held itself out as maintaining a secure database of sensitive customer data, Plaintiffs, the Class, and the California Subclass Members acted reasonably in relying on Comcast's misrepresentations and omissions, the truth of which they could not have discovered.

480. As a direct and proximate result of Comcast's violations of California Civil Code § 1770, Plaintiffs and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII, including but not limited to the diminishment of their present and future property interest in their PII and the deprivation of the exclusive use of their PII.

481. Plaintiffs and the California Subclass seek injunctive relief enjoining the acts and practices described above. Plaintiffs and the California Subclass further intend to seek compensatory and punitive damages. Pursuant to Cal. Civ. Code. § 1782(a), Plaintiffs and the California Subclass will serve Comcast with notice of its alleged violations of the CLRA by certified mail return receipt requested. If, within thirty days after the date of such notification, Comcast fails to provide appropriate relief for its violations of the CLRA, Plaintiffs will amend this Consolidated Complaint to also seek monetary damages.

COUNT 13: CALIFORNIA CONSUMER PRIVACY ACT, Cal. Civ. Code §§ 1798.100, *et seq*.

(On behalf of California Plaintiffs and the California Subclass, against Comcast only)

482. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein.

483. This claim is brought individually under the laws of California and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer privacy.

484. Plaintiffs and California Subclass Members are residents of California.

485. Comcast is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual gross revenues over $25 million.

486. Comcast is a business that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e). Specifically, Comcast obtains, receives, or accesses consumers' personal information when customers sign up for and utilize Xfinity services provided by Comcast.

487. Comcast violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs' and the California Subclass Members' nonencrypted and nonredacted

personal information from unauthorized access and exfiltration, theft, or disclosure as a result of Comcast's and Citrix's violations of their respective duties to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

488. Comcast knew or should have known that its data security practices were inadequate to secure California Subclass Members' PII and that its inadequate data security practices created the risk of a data breach.

489. Comcast failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII that Comcast collected and stored.

490. The cybercriminals accessed "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d) in the Data Breach.

491. Upon information and belief, Plaintiffs' and California Subclass Members' PII accessed by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

492. Plaintiffs seek injunctive relief in the form of an order requiring Comcast to employ adequate security practices consistent with law and industry standards to protect the California Subclass Members' PII, requiring Comcast to complete its investigation into the breach, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the California Subclass Members' authorization, along with more detailed explanation of how the data breach occurred.

493. Plaintiffs and the California Subclass seek injunctive relief enjoining the acts and practices described above. Plaintiffs and the California Subclass further intend to seek compensatory and punitive damages. Pursuant to Cal. Civ. Code. § 1798.150(a), Plaintiffs and the California Subclass will serve Comcast with notice of its alleged violations of the CLRA by

certified mail return receipt requested. If, within thirty days after the date of such notification, Comcast fails to provide appropriate relief for its violations of the CLRA, Plaintiffs will amend this Consolidated Complaint to also seek monetary damages..

494. As a direct and proximate result of Comcast's violations of the Cal. Civ. Code § 1798.150, Plaintiffs and California Subclass Members suffered damages, as described above.

CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS

COUNT 14: DELAWARE COMPUTER SECURITY BREACH ACT, 6 Del. Code Ann. §§ 12b-102, *et seq*.

(On behalf of Delaware Plaintiffs and the Delaware Subclass, against Comcast only)

495. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges the foregoing factual allegations as if fully alleged herein.

496. This claim is brought individually under the laws of Delaware and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding computer security.

497. Comcast is a business that owns or licenses computerized data that includes "personal information" as defined by 6 Del. Code Ann. § 12B-102(a).

498. Plaintiff's and Delaware Subclass Members' PII includes "personal information" covered under 6 Del. Code Ann. § 12B-101(4).

499. Comcast is required to accurately notify Plaintiff and Delaware Subclass Members if Comcast becomes aware of a breach of its data security program which is reasonably likely to result in the misuse of a Delaware resident's PII, in the most expedient time possible and without unreasonable delay under 6 Del. Code Ann. § 12B-102(a).

500. Because Comcast was aware of a breach of its security system which is reasonably likely to result in misuse of Delaware residents' PII, Comcast had an obligation to disclose the data breach in a timely and accurate fashion as mandated by 6 Del. Code Ann. § 12B-102(a).

501. By failing to disclose the Data Breach in a timely and accurate manner, Comcast violated 6 Del. Code Ann. § 12B-102(a).

502. As a direct and proximate result of Comcast's violations of 6 Del. Code Ann. §12B-102(a), Plaintiff and Delaware Subclass Members suffered damages, as described above.

503. Plaintiff and Delaware Subclass Members seek relief under 6 Del. Code Ann. § 12B-104, including actual damages and equitable relief.

COUNT 15: DELAWARE CONSUMER FRAUD ACT,
6 Del. Code §§ 2513, *et seq*.

(On behalf of Delaware Plaintiffs and the Delaware Subclass, against Comcast only)

504. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and realleges all foregoing factual allegations as if fully alleged herein.

505. This claim is brought individually under the laws of Delaware and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

506. Comcast is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

507. Comcast advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

508. Comcast used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent

that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Delaware Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Delaware Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Delaware Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Delaware Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100;

f. Failing to timely and adequately notify Plaintiff and Delaware Subclass Members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Delaware Subclass Members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Delaware Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100.

509. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII.

510. Comcast acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act and recklessly disregarded Plaintiff's and Delaware Subclass Members' rights.

511. Had Comcast disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Comcast would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Comcast was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs, the Class, and the Delaware Subclass. Comcast accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Comcast held itself out as maintaining a secure platform for PII data, Plaintiffs, the Class, and the Delaware Subclass Members acted reasonably in relying on Comcast's misrepresentations and omissions, the truth of which they could not have discovered.

512. Comcast's unlawful trade practices were gross, oppressive, and aggravated, and Comcast breached the trust of Plaintiff and the Delaware Subclass.

513. As a direct and proximate result of Comcast's unlawful acts and practices, Plaintiff and Delaware Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

514. Plaintiff and Delaware Subclass Members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Comcast's unlawful conduct; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 16: FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq*.

(On behalf of Florida Plaintiffs and the Florida Subclass, against Comcast only)

515. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and alleges the foregoing factual allegations as if fully alleged herein.

516. This claim is brought individually under the laws of Florida and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive and unfair trade practices.

517. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201 *et seq.* The stated purpose of this Act is to "protect the consuming public . . . from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." *Id*. § 501.202(2).

518. Plaintiff and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

519. Comcast advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

520. Comcast engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Florida Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Florida Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Failing to timely and adequately notify Plaintiff and Florida Subclass Members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Florida Subclass Members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

521. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII.

522. Comcast had exclusive knowledge of material facts concerning the inadequate security and vulnerabilities of its systems and networks that contained Plaintiff's and Florida Subclass Members' PII, including that such information was vulnerable to cyberattack, unauthorized access, exfiltration, and misuse.

523. On information and belief, prior to the Data Breach, Comcast had been repeatedly notified by employees that its systems and networks were vulnerable to cyberattack and that such cyberattack would likely be successful.

524. Despite Comcast's exclusive knowledge of material facts that its systems and networks that contained Plaintiff's and Florida Subclass Members' PII were not adequately secure and were vulnerable to cyberattack, Comcast actively concealed such information from Plaintiff and Florida Subclass Members.

525. Comcast had exclusive knowledge of material facts concerning when and what PII was accessed and exfiltrated during the Data Breach; however, Comcast actively concealed such information from Plaintiff and Florida Subclass Members, and otherwise misrepresented that certain PII was not accessed and exfiltrated.

526. Had Comcast disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Comcast would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

527. Instead, Comcast was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs, the Class, and the Florida Subclass. Comcast accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public.

528. Accordingly, because Comcast held itself out as maintaining a secure platform for PII data, Plaintiffs, the Class, and the Florida Subclass Members acted reasonably in relying on Comcast's misrepresentations and omissions, the truth of which they could not have discovered.

529. As a direct and proximate result of Comcast's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

530. Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT 17: ILLINOIS CONSUMER FRAUD ACT, 815 ILCS §§ 505, *et seq*.

(On behalf of Illinois Plaintiffs and the Illinois Subclass, against Comcast only)

531. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein.

532. This claim is brought individually under the laws of Illinois and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

533. Comcast is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

534. Plaintiff and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

535. Comcast's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

536. Comcast's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of

Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Plaintiff and Illinois Subclass Members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' PII;

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a); and

j. Failing to disclose the Data Breach in a timely fashion, in violation of 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.

537. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII.

538. Comcast intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

539. The above unfair and deceptive practices and acts by Comcast offend public policy, and were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

540. Comcast acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff's and Illinois Subclass Members' rights.

541. As a direct and proximate result of Comcast's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

542. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 18: ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILCS §§ 510/2, *et seq*.

(On behalf of Illinois Plaintiffs and the Illinois Subclass, against Comcast only)

543. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein.

544. This claim is brought individually under the laws of Illinois and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

545. Comcast is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

546. Comcast engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

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

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

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

547. Comcast's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Plaintiff and Illinois Subclass Members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a)).

548. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII.

549. The above unfair and deceptive practices and acts by Comcast were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

550. As a direct and proximate result of Comcast's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

551. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 19: NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J. Stat. Ann. §§ 56:8-163, *et seq*.

(On behalf of New Jersey Plaintiffs and the New Jersey Subclass, against Comcast only)

552. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of New Jersey and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer security.

553. Comcast is a business that compiles or maintains computerized records that include "personal information" on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

554. Plaintiff's and New Jersey Sub Class Members' PII includes "personal information" covered under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

555. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person."

556. Because Comcast discovered a breach of its security system in which PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, Comcast had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

557. By failing to disclose the Data Breach in a timely and accurate manner, Comcast violated N.J. Stat. Ann. § 56:8-163(b).

558. As a direct and proximate result of Comcast's violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass Members suffered the damages described above.

559. Plaintiff and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT 20: NEW JERSEY CONSUMER FRAUD ACT, N.J. Stat. Ann. §§ 56:8-1, *et seq*.

(On behalf of New Jersey Plaintiffs and the New Jersey Subclass, against Comcast only)

560. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of New Jersey and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

561. Comcast is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

562. Comcast sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

563. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, *et seq.*, prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

564. Comcast's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New Jersey Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Sub class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New Jersey Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Failing to timely and adequately notify the Plaintiff and New Jersey Subclass Members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass Members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

565. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII.

566. Comcast intended to mislead Plaintiff and New Jersey Subclass Members and induce them to rely on its misrepresentations and omissions.

567. Comcast acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff's and New Jersey Subclass Members' rights.

568. As a direct and proximate result of Comcast's unconscionable and deceptive practices, Plaintiff and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

569. Plaintiff and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 21: OHIO DECEPTIVE TRADE PRACTICES ACT, Ohio Rev. Code §§ 4165.01, *et seq*.

(On behalf of Ohio Plaintiffs and the Ohio Subclass, against Comcast only)

570. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Ohio and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

571. Comcast, Plaintiff, and Ohio Subclass Members are a "person," as defined by Ohio Rev. Code § 4165.01(D).

572. Comcast advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

573. Comcast engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);

b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9);

c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11);

d. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Ohio Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

g. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Ohio Subclass Members' PII, including by implementing and maintaining reasonable security measures;

h. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

i. Failing to timely and adequately notify Plaintiffs and Ohio Subclass Members of the Data Breach;

j. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

k. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Ohio Subclass Members' PII; and

l. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

574. Comcast did not engage in reasonable data security measures and/or did not follow its own data security measures in place at the time of the Data Breach.

575. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII.

576. Comcast intended to mislead Plaintiff and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

577. Comcast acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Ohio Subclass Members' rights.

578. As a direct and proximate result of Comcast's deceptive trade practices, Plaintiff and Ohio Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

579. Plaintiff and Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 22: TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT, Tenn. Code Ann. §§ 47-18-2107, *et seq*.

(On behalf of Tennessee Plaintiffs and the Tennessee Subclass, against Comcast only)

580. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, restate and reallege all foregoing factual

allegations as if fully set forth herein. This claim is brought individually under the laws of Tennessee and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding personal consumer information.

581. This claim is brought individually under the laws of Tennessee and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding personal consumer information.

582. Comcast is a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

583. Plaintiff's and Tennessee Subclass Members' PII include "Personal Information" as covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

584. Comcast is required to accurately notify Plaintiff and Tennessee Subclass Members following discovery or notification of a breach of its data security program in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, within 45 days from discovery of the breach under Tenn. Code Ann. § 47-18-2107(b).

585. Because Comcast discovered a breach of its security system in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, Comcast had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

586. By failing to disclose the Data Breach in a timely and accurate manner, Comcast violated Tenn. Code Ann. § 47-18-2107(b).

587. As a direct and proximate result of Comcast's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass Members suffered damages, as described above.

588. Plaintiff and Tennessee Subclass Members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 23: DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq*.

(On behalf of Texas Plaintiffs and the Texas Subclass, against Comcast only)

589. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Texas and on behalf of all other natural persons whose PII was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

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

591. Plaintiff and the Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

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

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

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

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

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

d. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Texas Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Texas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

g. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Texas Subclass Members' PII, including by implementing and maintaining reasonable security measures;

h. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Texas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

i. Failing to timely and adequately notify Plaintiff and Texas Subclass Members of the Data Breach;

j. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

k. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Texas Subclass Members' PII; and

l. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Texas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

594. Comcast intended to mislead Plaintiff and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

595. Comcast's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Comcast's data security and ability to protect the confidentiality of consumers' PII.

596. Had Comcast disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Comcast would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Comcast was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs, the Class, and the Texas Subclass. Comcast accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Comcast held itself out as maintaining a secure platform for PII data, Plaintiffs, the Class, and the Texas Subclass Members acted reasonably in relying on Comcast's misrepresentations and omissions, the truth of which they could not have discovered.

597. Comcast had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the PII in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiffs and the Texas Subclass, repose a trust and confidence in Comcast. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and Comcast because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Comcast. Comcast's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully

withholding material facts from Plaintiff and the Texas Subclass that contradicted these representations.

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

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

600. Comcast intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Comcast's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Comcast's unconscionable business acts and practices, exposed Plaintiff and Texas Subclass Members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiff and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the data breach.

601. Comcast acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Sub Class Members' rights.

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

603. Comcast's violations present a continuing risk to Plaintiff and Texas Subclass Members as well as to the general public.

604. Plaintiff and the Texas Subclass intend to provide notice of their claims for damages to Comcast, in compliance with Tex. Bus. & Com. Code Ann. § 17.505.

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

VIII. REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Defendants Comcast and Citrix, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead Interim Class Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Comcast and Citrix from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

a. Prohibiting Comcast and Citrix from engaging in the wrongful and unlawful acts described herein;

b. Requiring Comcast and Citrix to protect all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. Requiring Comcast to delete, destroy and purge the PII of Plaintiffs and Class Members unless Comcast can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

d. Requiring Comcast and Citrix to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII;

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

f. Requiring Comcast and Citrix to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring Comcast and Citrix to audit, test, and train their security personnel regarding any new or modified procedures;

h. Requiring Comcast to segment data by, among other things, creating firewalls and access controls so that if one area of Comcast's network is

compromised, hackers cannot gain access to other portions of Comcast's systems;

i. Requiring Comcast to conduct regular database scanning and security checks;

j. Requiring Comcast to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

k. Requiring Comcast to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

l. Requiring Comcast to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Comcast's policies, programs and systems for protecting PII;

m. Requiring Comcast to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor Comcast's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

n. Requiring Comcast to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

o. Requiring Comcast to implement logging and monitoring programs sufficient to track traffic to and from Comcast servers; and

p. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis Comcast's and Citrix's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

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

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

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

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

G. For an aware pre- and post-judgment interest on any amounts awarded; and

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

IX. JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated: July 1, 2024

Respectfully submitted,

/s/ Norman E. Siegel
Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Rd., Ste. 200
Kansas City, MO 64112
T: (816) 714-7100
siegel@stuevesiegel.com

Co-Lead Interim Class Counsel

/s/ Gary F. Lynch
Gary F. Lynch (PA No. 56887)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com

Co-Lead Interim Class Counsel

Charles E. Schaffer (PA No. 76259)
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
T: (215) 592-1500
cschaffer@lfsblaw.com

Co-Liaison Counsel

James A. Francis (PA No. 77474)
FRANCIS MAILMAN SOUMILAS, P.C.
1600 Market Street, Suite 2510
Philadelphia, PA 19103
T: (215) 735-8600
jfrancis@consumerlawfirm.com

Co-Liaison Counsel

Ryan J. Clarkson
CLARKSON LAW FIRM, P.C.
22525 Pacific Coast Highway
Malibu, CA 90265
T: (213) 788-4050
rclarkson@clarksonlawfirm.com

Amanda G. Fiorilla
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
T: (914) 997-0500
afiorilla@lowey.com

Kevin Laukaitis (PA No. 321670)
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Joe P. Leniski, Jr.
HERZFELD, SUETHOLZ, GASTEL, LENISKI & WALL, PLLC
223 Rosa L. Parks Avenue, Suite 300
Nashville, Tennessee 37203
T: (615) 800-6225
joey@hsglawgroup.com

Amber L. Schubert
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
T: (415) 788-4220
aschubert@sjk.law

E. Michelle Drake
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
T: (612) 594-5933
emdrake@bm.net

Todd S. Garber
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
T: (914) 298-3281
tgarber@fbfglaw.com

Matthew L. Lines
ISICOFF RAGATZ
601 Brickell Key Dr Ste 750
Miami, FL 33131
T: (305) 373-3232
lines@irlaw.com

Rosemary M. Rivas
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
T: (510) 350-9720
rmr@classlawgroup.com

Diana J. Zinser (PA No. 203449)
SPECTOR ROSEMAN AND KODROFF, P.C.
2001 Market Street, Suite 3420
Philadelphia, PA 19103
T: (215) 496-0300
dzinser@srkattorneys.com

Plaintiffs' Executive Committee

Public court record.

This copy was downloaded from https://storage.courtlistener.com/recap/gov.uscourts.paed.617030/go
on 2026-10-19 and is hosted, unaltered, for reference at
https://chimo.ai/class-action/comcast

Court: U.S. District Court for the Eastern District of Pennsylvania
Case number: 2:23-cv-05039-JMY
Filed: 2024-07-01

Chimo hosts public court records for readers' reference; documents are
unaltered copies from the court docket or the court-approved settlement website.