**KOPELOWITZ OSTROW P.A.**
Ken Grunfeld (SBN 84121)
65 Overhill Road
Bala Cynwyd, PA 19004
Tel: (954) 525-4100
Email: grunfeld@kolawyers.com

**TYCKO & ZAVAREEI LLP**
Hassan A. Zavareei (*pro hac vice* forthcoming)
1828 L Street NW, Ste. 1000
Washington, DC 20036
Tel: (202) 973-973-0900
Email: hzavareei@tzlegal.com

**CLARKSON LAW FIRM, P.C.**
Ryan J. Clarkson (*pro hac vice* forthcoming)
Glenn Danas (*pro hac vice* forthcoming)
Yana Hart (*pro hac vice* forthcoming)
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Email: rclarkson@clarksonlawfirm.com
Email: gdanas@clarksonlawfirm.com
Email: gdanas@clarksonlawfirm.com
Email: yhart@clarksonlawfirm.com

*Counsel for Plaintiffs and the Proposed Class*

**UNITED STATES DISTRICT COURT**

**EASTERN DISTRICT OF PENNSYLVANIA**

STEVEN PRESCOTT, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

COMCAST CORPORATION, a corporation,

Defendant.

Case No.

**CLASS ACTION COMPLAINT**

1. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE SECTION 17200, *et seq.*
2. VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, CIVIL CODE SECTION 1750, *et seq.*
3. VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA"), CAL. CIV. CODE SECTION 1798.150, *et seq.*
4. DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE SECTIONS 1709, 1710
5. NEGLIGENCE
6. INTENTIONAL MISREPRESENTATION
7. BREACH OF EXPRESS WARRANTY
8. BREACH OF IMPLIED WARRANTY

**DEMAND FOR JURY TRIAL**

Plaintiff Steven Prescott individually and on behalf of all others similarly situated, ("Plaintiff") brings this Action against Defendant Comcast Corporation. ("Comcast" or "Defendant"). Plaintiff's allegations are based upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth herein, after a reasonable opportunity for discovery.

## INTRODUCTION

1. Comcast, through the wholly owned Xfinity brand, is a "leading provider of broadband, video, voice, wireless, and other services to residential customers in the United States."[1] It is a major cable communications provider, with over 250,000 customers in the United States.[2] Plaintiffs and millions of other consumers entrusted Comcast with their personal data when they registered for Xfinity accounts, providing their names, contact information, last four digits of social security numbers, dates of birth and/or security questions and answers. As stated in their own privacy policy, Comcast recognizes the heavy burden of protection and security that they bear when collecting and storing this data.[3] Indeed, Comcast represents that it "know[s] it is our responsibility to be clear about how we protect your [customers'] information."[4] Comcast touts its purported dedication to strong security by making the following advertising claims for its devices and services, including but not limited to, the following: [5,6]

[1] *BamSEC*. (2019, June 24). tegus, from https://www.bamsec.com/filing/116669123000010 (Last visited December 19, 2023).
[2] *Id.*
[3] *Xfinity Privacy Policy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/policy (Last visited December 19, 2023).
[4] *Id.*
[5] *Id.*
[6] *Xfinity Privacy Center: Safety, Security, and Privacy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/ (Last visited December 19, 2023).

> "[Xfinity's] security practices include technical, administrative, and physical safeguards."[7]
>
> "[W]e believe strong cybersecurity is essential to privacy."[8]
>
> "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."[9]

2. Comcast's representations of strong and robust security have proved false and misleading—Comcast admittedly failed to safeguard the sensitive personal identifying information of millions of its consumers or implement robust security measures to prevent this information from being stolen.

**PARTIES**

3. Plaintiff Prescott is an individual residing in California, who had his personal identifiable information ("PII") exfiltrated and compromised in the data breach *announced* by Defendant on December 19, 2023. Prescott purchased Xfinity highspeed internet in or around 2015. To gain access to the internet, Prescott was required to create an Xfinity account. Prescott created an account on or around 2015. In doing so, Prescott was required to provide Defendant with his name, postal address, email address, date of birth, last four digits of his social security number and phone number, among other information. In making his decision to create an Xfinity account to gain access to the product's features, Prescott reasonably expected that Defendant would safeguard his PII. Prescott would not have purchased the product, nor would he have created and Xfinity account, if he knew that the sensitive information collected by Defendant would be at risk. Prescott has suffered damages and remains at a significant risk now that his PII has been leaked online.

---

[7] *Xfinity Privacy Policy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/policy (Last visited December 19, 2023).

[8] *Xfinity Privacy Center: Safety, Security, and Privacy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/ (Last visited December 19, 2023).

[9] *Id.*

4. Defendant Comcast Corporation is a global media and technology company. Defendant is incorporated in Pennsylvania and headquartered in the city of Philadelphia.

## JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one Plaintiff (CA) and Defendant (PA) are citizens of different states. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

6. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant is registered in Pennsylvania and headquartered in this District, Defendant gains revenue and profits from doing business in this District, consumers sign up for Xfinity accounts and provide Comcast with their PII in this District, Class members affected by the breach reside in this District, Defendant has a corporate office in this District, and Defendant employs numerous people in this District.

7. Defendant is subject to personal jurisdiction in Pennsylvania as a resident of this state. Defendant is authorized to do and is doing business, advertises, and solicits business within the state. By residing in Pennsylvania, Defendant is physically present and subject to its laws.

## FACTUAL ALLEGATIONS

8. Defendant is a media and technology company that operates three primary businesses: Comcast Cable, NBCUniversal, and Sky. Defendant touts 34.3 million "customer relationships" across the United States, with over 500,000 cable communications customers in most major U.S. cities. As of 2022, Defendant provided broadband internet to 29.8 million customers and video streaming/cable to 15.6 million customers, all under the brand name Xfinity.[10]

[10] *BamSEC*. (2019, June 24). tegus, from https://www.bamsec.com/filing/116669123000010 (Last visited December 19, 2023).

9. Defendant collects and processes the personal data of millions of consumers, including personal information. For its internet and streaming/cable services, Defendant requires that consumers create an Xfinity account, forcing consumers to entrust Defendant with their PII, in order to use Defendant's products and services. Since Defendant's products all feature subscription payment schedules, consumers are required to create an account through which they pay their bills. Consumers are therefore forced to register accounts to use the service at all.

10. The information collected and stored by Defendant includes, but is not limited to, ***names, dates of birth, addresses, precise geolocation data, email addresses, phone numbers, answers to personal security questions and last four digits of social security numbers***. Defendant collected this PII by requiring consumers to complete account registration.

11. Defendant holds itself as a trustworthy company, which recognized and values the customers' privacy and personal information and has repeatedly assured its customers that it "believe[s] strong cybersecurity is essential to privacy."[11] Further, Defendant makes representations that its security practices are *robust*, including "technical, administrative, and physical safeguards,"[12] and employing "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."[13]

12. Defendant's privacy policy and online advertisements clearly and unequivocally state that any personal information provided to Defendant will remain secure and protected.

13. Defendant is clear in their communication to customers that it "know[s] you care about your privacy and the protection of your personal information" and state that their privacy

---

[11] *Xfinity Privacy Center: Safety, Security, and Privacy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/ (Last visited December 19, 2023).

[12] *Xfinity Privacy Policy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/policy (Last visited December 19, 2023).

[13] *Xfinity Privacy Center: Safety, Security, and Privacy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/ (Last visited December 19, 2023).

policy is designed to be "clear," driving the point home that *Defendant wants customers to believe their personal information will be safeguarded*:

> **We know you care about your privacy and the protection of your personal information. We also know it is our responsibility to be clear about how we protect your information. We designed this Privacy Policy to do just that. It explains the types of personal information we collect, and how we collect, use, maintain, protect, and share this information. This Privacy Policy also tells you about the rights and choices you may have when it comes to your personal information.**
>
> **Some of what we say in our Privacy Policy is required by law, and may at times seem long and complicated, but we've worked hard to try to make our Privacy Policy easy to understand and provide examples where possible.**

14. Plaintiff and other similarly situated consumers relied to their detriment on Defendant's uniform representations and omissions regarding data security, including Defendant's failure to alert customers that its security protections were inadequate, and that Defendant would forever store Plaintiff's and customers' PII, failing to archive it, protect it, or at the very minimum warn consumers of the anticipated and foreseeable data breach.[14]

15. Had Defendant disclosed to Plaintiffs and its other customers that its data systems were not secure at all and were vulnerable to attack, Plaintiffs would not have purchased Defendant's products or utilized its services. In fact, Defendant would have been forced to adopt reasonable data security measures and comply with the law.

16. Plaintiffs and other similarly situated consumers trusted Defendant with their sensitive and valuable PII. Defendant did not need to collect this PII at all. It did so, to increase its

[14] *Notice To Customers of Data Security Incident*. (2023, December 18). Xfinity, from https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (Last visited December 19, 2023).

profits, gather the information regarding its customers, and be able to track their customers and their behaviors.

17. Defendant knew or should have known that Plaintiffs and Class Members would reasonably rely upon and trust Defendant's promises regarding security and safety of their data and systems.

18. By collecting, using, selling, monitoring, and trafficking Plaintiff's and other customers' PII, and utterly failing to protect it by maintaining inadequate security systems, failing to properly archive the PII, allowing access of third parties, and failing to implement security measures, Defendant caused harm to Plaintiffs and consumers.

## DATA BREACH

19. At all material times, Defendant failed to maintain proper security measures despite its promises of safety and security to consumers.

20. On October 10, 2023, Defendant became aware that a vulnerability was found in a software product used by Defendant. Before Defendant notified consumers, and before mitigation took place, approximately between October 16 and October 19, 2023, there was unauthorized access to Defendant's internal systems. On November 16, 2023, Defendant concluded that customers' information was likely acquired.[15]

21. Defendant notified customers on December 19, 2023, when over two months had passed since learning of the software vulnerability and over a month had passed since Defendant concluded that customer information had likely been acquired.

22. In its statement, Defendant does not disclose how many consumers' PII was breached, leaving consumers to speculate whether it is likely that their PII has been compromised and without any clear instruction on what they can do to protect themselves now that their PII has

[15] *Notice To Customers of Data Security Incident*. (2023, December 18). Xfinity, from https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf (Last visited December 19, 2023).

been exposed. It is believed *all of Xfinity's 35.9 million* US consumers had their PII compromised in the breach.[16]

## IMPACT OF DATA BREACH ON CONSUMERS

23. Plaintiffs and the Class have suffered actual harm as a result of Defendant's conduct. Defendant failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. This breach allowed hackers to access the PII, including first and last names, postal addresses, precise geolocation data, email addresses, and telephone numbers, for Plaintiff and the Class. This PII has since been publicly leaked online, which has allowed for digital and potential physical attacks against Plaintiff and the Class. Now that the PII has been leaked, it is available for other parties to sell or trade and will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[17]

### Digital Phishing Scams

24. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $57 million to such scams in 2019 alone.[18]

25. Defendant's customers are now more likely to become victims of SIM Swap attacks because of the released personal information.

### SIM-Swap

---

[16] *Office of the Maine AG: Consumer Protection: Privacy, Identity Theft and Data Security Breaches*. (n.d.). Office of the Maine AG: Consumer Protection: Privacy, Identity Theft and Data Security Breaches, from https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml (Last visited December 19, 2023).

[17] *See* U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 29 2007. https://www.gao.gov/new.items/d07737.pdf. (Last visited December 19, 2023).

[18] *See How to Recognize and Avoid Phishing Scams*, FTC Consumer Advice, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (Last visited December 19, 2023).

26. The data leak can also lead to SIM-swap attacks against the Class.[9] A SIM-swap attack occurs when the scammers trick a telephone carrier to porting the victim's phone number to the scammer's SIM card. By doing so, the attacker is able to bypass two-factor authentication accounts, as are used to access cryptocurrency wallets and other important accounts. The type of personal information that has been leaked poses a profound tangible risk of SIM-swap attacks for the Class.

27. Defendant's customers are now more likely to become victims of SIM Swap attacks because of the released personal information.

**Loss of Time**

28. As a result of this breach, Plaintiff and impacted consumers will suffer unauthorized email solicitations, and experience a significant increase in suspicious phishing scam activity via email, phone calls, text messages, all following the breach. In addition, Plaintiff, as a result of the breach spent significant time and effort researching the breach, monitoring his account for fraudulent activity, reviewing the unsolicited emails, texts, and answering telephone calls.

29. Plaintiff also spent significant time monitoring personal accounts (banking, credit monitoring, financial applications, and even other applications/accounts that may be attacked) for fraudulent activity. Plaintiff, in great distress, is attempting to change their passwords and associated accounts which may be connected to various pieces of stolen PII. Plaintiff has been monitoring their credit activity, living in constant fear and apprehension of further attacks.

**Overpayment for the Products**

30. Plaintiff and the Class would not have purchased the products that led to their account creation if they knew that doing so would result in their PII being compromised and exfiltrated. Thus, they significantly overpaid based on what the products were represented compared to what they received.

**Threat of Identity Theft**

31. As a direct and proximate result of Defendant's breach of confidence, and failure to protect the PII, Plaintiff and the Class have also been injured by facing ongoing, imminent,

impending threats of identity theft crimes, fraud, scams, and other misuse of this PII, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen PII, illegal sales of the compromised PII on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries. Defendant, through its misconduct, has enabled numerous bad actors to sell and profit off of PII that belongs to Plaintiff.

32. But for Defendant's unlawful conduct, scammers would not have access to Plaintiff's and the Class members' contact information. Defendant's unlawful conduct has directly and proximately resulted in widespread digital attacks against Plaintiffs and the Class.

**Out of Pocket Costs**

33. Plaintiff is now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiff anticipates spending out of pocket expenses to pay for these services.

34. Upon information and Belief, Defendant also used Plaintiff's PII for profit, and continued to use Plaintiff's PII to target Plaintiff, and share their information with various third parties for Defendant's own benefit.

**Summary of Actual Economic and Noneconomic Damages**

35. In sum, Plaintiff and similarly situated consumers were injured as follows:

i. Theft of their PII and the resulting loss of privacy rights in that information;

ii. Improper disclosure of their PII;

iii. Loss of value of their PII;

iv. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

v. Defendant's retention of profits attributable to Plaintiffs' and other customers' PII that Defendant failed to adequately protect;

vi. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs are now exposed to;

vii. Ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach;

viii. Overpayments of Defendant's products and/or services which Plaintiffs purchased;

ix. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

**CLASS ALLEGATIONS**

36. Plaintiff brings this action on his own behalf and on behalf of all other persons similarly situated. The Class which Plaintiff seeks to represent comprises:

> "All persons who purchased or used Comcast products and services in the United States and whose PII was accessed, compromised, or stolen in the data breach announced by Comcast on December 19, 2023."

Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

37. The California Subclass which Plaintiff seeks to represent comprises:

> "All persons who purchased or used Comcast products and services in the California and whose PII was accessed, compromised, or stolen in the data breach announced by Comcast on December 19, 2023" (the "California Subclass").

Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

38. The Class is comprised of millions of consumers throughout the United States and the state of California. The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

39. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the Class was exposed to the same common and uniform false and misleading advertising and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

b. Whether Defendant's conduct is an unfair business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

c. Whether Defendant's advertising as to their security practices is untrue or misleading within the meaning of Business and Professions Code section 17500, *et seq*.;

d. Whether Defendant's conduct is in violation of California Civil Code Sections 1709, 1710;

e. Whether Defendant's failure to implement effective security measures to protect Plaintiff's and the Class's PII negligent;

f. Whether Defendant breached express and implied warranties of security to the Class;

g. Whether Defendant represented to Plaintiff and the Class that they would protect Plaintiff's and the Class members' PII;

h. Whether Defendant owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

i. Whether Defendant breached a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

j. Whether Class members' PII was accessed, compromised, or stolen in the breach;

k. Whether Defendant's conduct caused or resulted in damages to Plaintiff and the Class;

l. Whether Defendant failed to notify the public of the breach in a timely and adequate manner;

m. Whether Defendant knew or should have known that its systems were vulnerable to a data breach;

n. Whether Defendant adequately addressed the vulnerabilities that allowed for the data breach; and

o. Whether, as a result of Defendant's conduct, Plaintiff and the Class are entitled to damages and relief.

40. Plaintiff's claims are typical of the claims of the proposed Class, as Plaintiff and the members of the Class were harmed by Defendant's uniform unlawful conduct.

41. Plaintiff will fairly and adequately represent and protect the interests of the proposed Class. Plaintiff has retained competent and experienced counsel in class action and other complex litigation.

42. Plaintiff and the Class have suffered injury in fact as a result of Defendant's false, deceptive, and misleading representations.

43. Plaintiff would not have created an Xfinity account but for the reasonable belief that Defendant would safeguard their data and PII.

44. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

45. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it

impracticable or impossible for proposed members of the Class to prosecute their claims individually.

46. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by Defendant's conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

47. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendant.

48. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class members' claims, few, if any, Class members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, the Class members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

## COUNT ONE

## VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW

## BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.*

**(ON BEHALF OF THE CALIFORNIA SUBCLASS AND NATIONWIDE CLASS)**

49. Plaintiff, individually and on behalf of the Class, herein repeats, realleges and fully incorporates all allegations in all preceding paragraphs.

50. For all Class members outside of the California Subclass, these claims are brought under the relevant consumer protection statute for the state in which they reside. For each state, the relevant statutes are as follows: Alabama—Deceptive Trade Practices Act (Ala. Code § 8-19-

1, *et seq.*); Alaska—Unfair Trade Practices and Consumer Protection Act (Alaska Stat. § 45.50.471, *et seq.*); Arizona—Consumer Fraud Act (Ariz. Rev. Stat. Ann. § 44-1521, *et seq.*); Arkansas—Deceptive Trade Practices Act (Ark. Code Ann. § 4-88-101, *et seq.*); Colorado—Consumer Protection Act (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut—Connecticut Unfair Trade Practices Act (Conn. Gen. Stat. § 42-110a, *et seq.*); Delaware—Consumer Fraud Act (Del. Code Ann. tit. 6, § 2511, *et seq.*); District of Columbia—D.C. Code § 28-3901, *et seq.*; Florida—Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.20, *et seq.*); Georgia—Fair Business Practices Act (Ga. Code Ann. § 10-1-390, *et seq.*); Hawaii—Haw. Rev. Stat. § 480-1, *et seq.*); Idaho—Consumer Protection Act (Idaho Code Ann. § 48-601, *et seq.*); Illinois—Consumer Fraud and Deceptive Business Practices Act (815 Ill. Comp. Stat. 505/1, *et seq.*); Indiana—Deceptive Consumer Sales Act (Ind. Code § 24-5-0.5-1, *et seq.*); Iowa—Iowa Code § 7.14.16, *et seq.*); Kansas—Consumer Protection Act (Kan. Stat. Ann. § 50-623, *et seq.*); Kentucky—Consumer Protection Act (Ky. Rev. Stat. Ann. § 367.110, *et seq.*); Louisiana—Unfair Trade Practices and Consumer Protection Law (La. Rev. Stat. Ann. § 51:1401, *et seq.*); Maine—Unfair Trade Practices Act (Me. Rev. Stat. Ann. tit. 5, § 205A, *et seq.*); Maryland—Maryland Consumer Protection Act (Md. Code Ann., Com. Law § 13-101, *et seq.*); Massachusetts—Regulation of Business Practice and Consumer Protection Act (Mass. Gen. Laws Ann. ch. 93A, §§ 1-11); Minnesota—False Statement in Advertising Act (Minn. Stat. § 8.31, Minn. Stat. § 325F.67), Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68, *et seq.*); Mississippi—Consumer Protection Act (Miss. Code Ann. § 75-24, *et seq.*); Missouri—Merchandising Practices Act (Mo. Rev. Stat. § 407.010, *et seq.*); Montana—Unfair Trade Practices and Consumer Protection Act (Mont. Code. Ann. § 30-14-101, *et seq.*); Nebraska—Consumer Protection Act (Neb. Rev. Stat. § 59-1601); Nevada—Trade Regulation and Practices Act (Nev. Rev. Stat. § 598.0903, *et seq.*, Nev Rev. Stat. § 41.600); New Hampshire—Consumer Protection Act (N.H. Rev. Stat. Ann. § 358-A:1, *et seq.*); New Jersey—N.J. Stat. Ann. § 56:8-1, *et seq.*); New Mexico—Unfair Practices Act (N.M. Stat. § 57-12-1, *et seq.*); New York—N.Y. Gen. Bus. Law §§ 349, 350, N.Y. Exec. Law § 63(12); North Carolina—N.C. Gen. Stat. § 75-1.1, *et seq.*); North Dakota—N.D. Cent. Code § 51-15-01, *et seq.*); Ohio—

Consumer Sales Practices Act (Ohio Rev. Code Ann. § 1345.01, *et seq.*); Oklahoma—Consumer Protection Act (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon—Unlawful Trade Practices Law (Or. Rev. Stat. § 646.605, *et seq.*); Pennsylvania—Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. Ann. § 201-1, *et seq.*); Rhode Island—Unfair Trade Practice and Consumer Protection Act (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Carolina—Unfair Trade Practices Act (S.C. Code Ann. § 39-5-10, *et seq.*); South Dakota—Deceptive Trade Practices and Consumer Protection Law (S.D. Codified Laws § 37-24-1, *et seq.*); Tennessee—Consumer Protection Act (Tenn. Code Ann. § 47-18-101, *et seq.*); Texas—Deceptive Trade Practices—Consumer Protection Act (Tex. Bus. & Com. Code Ann. § 17.41, *et seq.*); Utah—Consumer Sales Practices Act (Utah Code Ann. § 13-11-1, *et seq.*); Vermont—Consumer Fraud Act (Vt. Stat. Ann. tit. 9, § 2451, *et seq.*); Virginia—Consumer Protection Act (Va. Code Ann. § 59.1-196, *et seq.*); Washington—Consumer Protection Act (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia—W. Va. Code § 46A-6-101, *et seq.*); Wisconsin—Wis. Stat. § 100.18, 100.20; Wyoming—Consumer Protection Act (Wyo. Stat. Ann. § 40-12-101, *et seq.*).

**A. "Unfair" Prong**

51. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, *et seq.*, a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

52. Defendant's conduct as alleged herein does not confer any benefit to consumers. It is especially questionable why Defendant would continue to store individual's data when it is unnecessary information for the handling of payments. Mishandling this data and a failure to archive and purge unnecessary data shows blatant disregard for customers' privacy and security.

53. Defendant did not need to collect the private data from its consumers to allow consumers' use of the products. It did so to track and target its customers and monetize the use of the data to enhance its already exorbitant profits. Defendant utterly misused this data and PII.

54. Defendant's conduct as alleged herein causes injuries to consumers, who do not receive a product consistent with their reasonable expectations.

55. Defendant's conduct as alleged herein causes injuries to consumers, entrusted Defendant with their PII and whose PII was leaked as a result of Defendant's unlawful conduct.

56. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

57. Consumers cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

58. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

59. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

60. Defendant could have furthered its legitimate business interests in ways other than by unfair conduct.

61. Defendant's conduct threatens consumers by misleadingly advertising their systems as "secure" and exposing consumers' PII to hackers. Defendant's conduct also threatens other companies, large and small, who play by the rules. Defendant's conduct stifles competition and has a negative impact on the marketplace and reduces consumer choice.

62. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

63. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

64. Plaintiff and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs relied on and made their purchasing decision in part based on Defendant's representations regarding their security measures and trusted that Defendant would keep their PII safe and secure. Plaintiffs accordingly provided their PII to Defendant reasonably believing and expecting that their PII would be safe and secure. Plaintiffs paid an unwarranted premium for the purchased products and services. Specifically, Plaintiffs paid for products and services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class would not have purchased the products and services, or would not have given Defendant their PII, had they known that their PII was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' PII. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

**B. "Fraudulent" Prong**

65. California Business and Professions Code Section 17200, *et seq.* considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992).

66. Defendant's advertising and representations that they adequately protect consumer PII is likely to deceive members of the public into believing that Comcast can be entrusted with their PII, and that PII gathered by Comcast is not in danger of being compromised.

67. Defendant's representations about their products and services, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes fraudulent conduct.

68. Defendant knew or should have known of its fraudulent conduct.

69. As alleged in the preceding paragraphs, the material misrepresentations by Defendant detailed above constitute a fraudulent business practice in violation of California Business & Professions Code Section 17200.

70. Defendant could have implemented robust security measures to prevent the data breach but failed to do so.

71. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

72. Pursuant to Business & Professions Code Section 17203, Plaintiff and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its practice of false and deceptive advertising about the strength or adequacy of its security systems. Likewise, Plaintiff and the Class seek an order requiring Defendant to disclose such misrepresentations.

73. Plaintiff and the Class have suffered injury in fact and have lost money as a result of Defendant's fraudulent conduct. Plaintiffs paid an unwarranted premium for the products and services. Plaintiffs would not have purchased the products, nor have used the services, if they had known that their use would put their PII at risk.

74. **Injunction**. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court compelling Defendant to implement adequate safeguards to protect consumer PII retained by Defendant. This includes, but is not limited to: improving security systems, deleting data that no longer needs to be retained by Defendant, archiving that data on secure servers, and notifying all affected consumers in a timely manner.

### C. "Unlawful" Prong

75. California Business and Professions Code Section 17200, *et seq.*, identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

76. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq*.

77. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

78. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law. Defendant failed to notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

79. Defendant knew or should have known of its unlawful conduct.

80. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

81. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

82. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

83. Pursuant to Business and Professions Code Sections 17203, Plaintiff and the Class seeks an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

84. Plaintiff and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiff paid an unwarranted premium for the products and services he purchased. Specifically, Plaintiff paid for products and services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected

vulnerabilities that led to a data breach. Plaintiff and the Class would not have purchased the products and services, or would not have given Defendant their PII, had they known that their PII was vulnerable to a data breach. Likewise, Plaintiff and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' PII. Additionally, Plaintiff and the members of the Class seek and request an order awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

**COUNT TWO**

**VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT**

**CALIFORNIA CIVIL CODE SECTION 1750, *et seq.***

**(ON BEHALF OF THE CALIFORNIA SUBCLASS)**

85. Plaintiff repeats and re-alleges the allegations set forth in the preceding paragraphs, and incorporates the same as if set forth herein at length.

86. The CLRA prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of goods.

87. Defendant's unlawful conduct described herein was intended to increase sales to the consuming public and violated and continue to violate Section 1770(a)(5), (a)(7), and (a)(9) of the CLRA by representing that the products and services have characteristics and benefits which they do not have.

88. Defendant fraudulently deceived Plaintiff and the California Subclass by representing that its products and services have certain characteristics, benefits, and qualities which they do not have, namely data protection and security. In doing so, Defendant intentionally misrepresented and concealed material facts from Plaintiff and the California Subclass, specifically by advertising secure technology when Defendant in fact failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiff and the California Subclass and depriving them of their legal rights and money.

89. Defendant's claims about the products and services led and continues to lead consumers like Plaintiff to reasonably believe that Defendant has implemented adequate data security measures when Defendant in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access consumers' PII.

90. Defendant knew or should have known that adequate security measures were not in place and that consumers' PII was vulnerable to a data breach.

91. Plaintiff and the California Subclass have suffered injury in fact as a result of and in reliance upon Defendant's false representations.

92. Plaintiff and the California Subclass would not have purchased the products or used the services, or would have paid significantly less for the products and services, had they known that their PII was vulnerable to a data breach.

93. Defendant's actions as described herein were done with conscious disregard of Plaintiff's rights, and Defendant was wanton and malicious in its concealment of the same.

94. Plaintiff and the California Subclass have suffered injury in fact and have lost money as a result of Defendant's unfair, unlawful, and fraudulent conduct. Specifically, Plaintiff paid for products and services advertised as secure, and consequentially entrusted Defendant with his PII, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff and the California Subclass would not have purchased the products and services, or would not have provided Defendant with their PII, had they known that their PII was vulnerable to a data breach.

95. Defendant should be compelled to implement adequate security practices to protect consumers' PII. Additionally, Plaintiff and the members of the California Subclass lost money as a result of Defendant's unlawful practices.

96. At this time, Plaintiff seeks injunctive relief under the CLRA pursuant to Cal. Civ. Code 1782(d); but he anticipates the need to amend the complaint and seek restitution.

## COUNT THREE

## VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

**CAL. CIV. CODE SECTION 1798.150, *et seq.***

**(ON BEHALF OF THE CALIFORNIA SUBCLASS)**

97. Plaintiff repeats and re-alleges the allegations set forth in the preceding paragraphs, and incorporates the same as if set forth herein at length.

98. Defendant is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over $121 billion.

99. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140.

100. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and the California Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

101. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and California Subclass Members' PII. As detailed herein, Defendant failed to do so.

102. As a direct and proximate result of Defendant's acts, Plaintiff's and California Subclass Members' PII, including phone numbers, names, date of birth, addresses, email addresses, and last four digits of social security numbers, was subjected to unauthorized access and exfiltration, theft, or disclosure.

103. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including Plaintiff's and California Subclass Members' PII. Plaintiff and California Subclass Members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

104. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

105. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

106. Plaintiff and the California Subclass seek actual pecuniary damages, including actual financial losses resulting from the unlawful data breach.

## COUNT FOUR

## DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE SECTIONS 1709, 1710

## (ON BEHALF OF THE CALIFORNIA SUBCLASS)

107. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

108. Defendant knew or should have known that its security systems were inadequate to protect the PII of its consumers. Specifically, Defendant had an obligation to disclose to its consumers that its security systems were not adequate to safeguard their PII. Defendant did not do so. Rather, Defendant deceived Plaintiff and the California Subclass by concealing the vulnerabilities in its security system.

109. Even after Defendant discovered the data breach, it concealed it, and waited over a month before announcing it to the public so they could know and take precautions against the data breach.

110. California Civil Code §1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true"; (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact"; or (d) "[a] promise, made

without any intention of performing it." Defendant's conduct as described herein therefore constitutes deceit of Plaintiff and the California Subclass.

111. California Civil Code §1709 mandates that in willfully deceiving Plaintiff and the California Subclass with intent to induce or alter their position to their injury or risk, Defendant is liable for any damage which Plaintiff and the California Subclass thereby suffer.

112. As described above, Plaintiff and the California Subclass have suffered significant harm as a direct and proximate result of Defendant's deceit and other unlawful conduct. Specifically, Plaintiff and the Class have been subject to numerous attacks, including various phishing scams. Defendant is liable for these damages.

**COUNT FIVE**

**NEGLIGENCE**

**(ON BEHALF OF THE NATIONWIDE CLASS)**

113. Plaintiff herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

114. Defendant owed a duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that consumers' PII was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

115. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiff and members of the Class, who were the foreseeable and probable victims of any inadequate security practices.

116. Defendant's duties also arose under Section 5(a) of the Federal Trade Commission Act ("FTC Act") (15 USC § 45) prohibits "unfair or deceptive acts or practices in or affecting commerce." Defendant's failure to protect Plaintiff's and the Class members' PII constitutes an

unfair or deceptive act or practice ("UDAP") because it (a) "causes or is likely to cause substantial injury to consumers;" (b) "cannot be reasonably avoided by consumers"; and (c) "is not outweighed by countervailing benefits to consumers or competition." As interpreted and enforced by the FTC, this includes the failure to use reasonable measures to protect consumers' PII.

117. Defendant knew or should have known that Plaintiff's and the Class members' PII is information that is frequently sought after by hackers.

118. Defendant knew or should have known that Plaintiff and the Class members would suffer harm if their PII was leaked.

119. Defendant knew or should have known that its security systems were not adequate to protect Plaintiff's and the Class members' PII from a data breach, especially in light of the April 2022 data breach.

120. Defendant knew or should have known that adequate and prompt notice of the data breach was required such that Plaintiff and the Class could have taken more swift and effective action to change or otherwise protect their PII. Defendant failed to provide timely notice upon discovery of the data breach. Plaintiff and some of the Class members were informed of the data breach on December 19, 2023. Defendant had learned of the data breach up to two months prior, in October 2023, and learned that consumers' PII was compromised over a month prior, in November 2024.

121. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiff's and the Class members' PII by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Defendant did not implement, design, or maintaining adequate measures to detect a data breach when it occurred.

122. Defendant's conduct as described above constituted an unlawful breach of its duty to provide adequate and prompt notice of the data breach.

123. Defendant and the Class entered into a special relationship when the Class members entrusted Defendant to protect their PII. Plaintiff and the Class purchased Defendant's products

and services, and in doing so provided Defendant with their PII, based upon Defendant's representations that it would implement adequate systems to secure their information. Defendant did not do so. Defendant knew or should have known that their security system was vulnerable to a data breach. Defendant breached their duty in this relationship to implement and maintain reasonable measures to protect the PII of the Class.

124. Plaintiff's and the Class members' PII would have remained private and secure had it not been for Defendant's wrongful and negligent breach of their duties. The leak of Plaintiff's and the Class members' PII, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

125. Defendant's negligence was, at least, a substantial factor in causing the Plaintiff's and the Class's PII to be improperly accessed, disclosed, and otherwise compromised, and in causing the Class members' other injuries because of the data breaches.

126. The damages suffered by Plaintiff and the Class members was the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiffs and the Class members' PII. Defendant knew or should have known that their security for safeguarding Plaintiffs and the Class members' PII was vulnerable to a data breach.

127. Defendant's negligence directly caused significant harm to Plaintiffs and the Class.

## COUNT SIX

## INTENTIONAL MISREPRESENTATION

## (ON BEHALF OF THE NATIONWIDE CLASS)

128. Plaintiff repeats and realleges all of the allegations contained above and incorporate the same as if set forth herein at length.

129. Defendant has represented, through online advertisements and its privacy policy, that Defendant affords robust protection to consumers' PII.

130. Defendant makes representations that its security protections are multifaceted and effective, including the operation of "technical, administrative, and physical safeguards,"[19] and employing "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."[20] Defendant in fact misrepresented the security of its services and products, failed to institute adequate security measures, and neglected vulnerabilities that led to a data breach of sensitive, personal information.

131. Defendant's misrepresentations regarding its security systems are material to a reasonable consumer, as they relate to the privacy of consumers' PII. A reasonable consumer would assign importance to such representations and would be induced to act thereon in making his or her purchase decision.

132. At all relevant times when such misrepresentations were made, Defendant knew or should have known that the representations were misleading.

133. Defendant intended for Plaintiff and the Class to rely on the representations of its security systems, as evidenced by Defendant's intentional marketing of safe and secure services and products.

134. Plaintiff and members of the Class reasonably and justifiably relied on Defendant's intentional misrepresentations when purchasing the products and services, and had they known the truth, they would not have purchased the products and services or would not have given Defendant their PII.

135. Defendant was negligent in its representations that it would provide the highest level of security for consumers.

136. As a direct and proximate result of Defendant's intentional misrepresentations, Plaintiff and members of the Class have suffered injury in fact.

---

[19] *Xfinity Privacy Policy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/policy (Last visited December 19, 2023).

[20] *Xfinity Privacy Center: Safety, Security, and Privacy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/ (Last visited December 19, 2023).

**COUNT SEVEN**

**BREACH OF EXPRESS WARRANTY**

**(ON BEHALF OF THE NATIONWIDE CLASS)**

137. Plaintiff repeats and realleges the allegations set forth above and incorporate the same as if set forth herein at length.

138. Defendant made an express warranty to Plaintiff and members of the Class that its security protections are multifaceted and effective, including the operation of "technical, administrative, and physical safeguards,"[21] and employing "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."[22] In order to pay for the products and services, Plaintiff and the Class were required to provide their personal information which they reasonably believed, based on Defendant's expressed advertising claims, would be kept private and secure.

139. Defendant's express warranty regarding its security standards it made to Plaintiffs and the Class appears throughout its website.[23] The promises of security associated with the products and services describes the products and services, specifically relates to the products/services being purchased, and therefore becomes the basis of the bargain.

140. Plaintiff and the Class purchased the products and services with the expectation that the information they provided would be kept safe, secure, and private in accordance with the express warranties made by Defendant on its website.

141. Defendant breached the express warranty made to Plaintiff and Class members by failing to provide adequate security to safeguard Plaintiff's and the Class's PII. As a result,

---

[21] *Xfinity Privacy Policy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/policy (Last visited December 19, 2023).

[22] *Xfinity Privacy Center: Safety, Security, and Privacy*. (n.d.). Xfinity, from https://www.xfinity.com/privacy/ (Last visited December 19, 2023).

[23] *See supra* notes 5-6.

Plaintiff and members of the Class suffered injury and deserve to be compensated for the damages they suffered.

142. Plaintiff and the members of the Class paid money for the products and services. However, Plaintiff and Class members did not obtain the full value of the advertised products and services. If Plaintiff and other Class members had known that their PII would be exposed, then they would not have purchased the products and services.

143. Plaintiff and the Class are therefore entitled to recover all available remedies for said breach.

## COUNT EIGHT

## BREACH OF IMPLIED WARRANTY

## (ON BEHALF OF THE NATIONWIDE CLASS)

144. Plaintiff repeats and realleges the allegations set forth above and incorporate the same as if set forth herein at length.

145. Unless excluded or modified, a warranty that a good shall be merchantable is implied in a contract for their sale, if the seller is a merchant with respect to goods of that kind.

146. Defendant is a merchant with respect to the product and services, as it provides cable and communication services, including but not limited to, broadband internet and cable access. In exchange, Defendant receives benefits in the form of monetary payments and/or other valuable consideration, *e.g.*, access to consumers' private and personal data.

147. In using Defendant's products and services, Plaintiff and the Class continually provide Defendant with their valuable private and personal information.

148. Defendant acknowledged these benefits and accepted or retained them.

149. Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and the Class Members' sensitive information.

150. All parties understood that such security was an integral and essential part of Defendant's products and services.

151. Defendant breached the implied warranty of merchantability to Plaintiff and the Class in its representations that the purchased product and services would maintain the security of their PII. Contrary to the promise and affirmation of fact, Defendant failed to provide such security.

152. As a result of Defendant's conduct, Plaintiff and the Class did not receive merchantable goods and services as impliedly warranted by Defendant.

153. Defendant did not exclude or modify the products and services implied warranty of merchantability.

154. As a proximate result of Defendant's breach of its implied warranty, Plaintiff and members of the Class incurred damages. Plaintiff and members of the Class were damaged as a result of Defendant's failure to comply with its obligations under the implied warranty, since Plaintiff and members of the Class paid for a product that did not have the promised quality and nature, did not receive the services that they bargained for, paid a premium for the product/service when they could have instead purchased other less expensive alternative products/services, and lost the opportunity to purchase other similar products/services.

155. Plaintiff and the Class are therefore entitled to recover all available remedies for said breach.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, pray for judgment and relief on all cause of action as follows:

A. That the Court determines that this Action may be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;

C. An order:

a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide notice to all affected consumers);

b. Requiring Defendant to implement adequate security protocols and practices to protect consumers' PII consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring Defendant to protect all data collected through its account creation requirements;

e. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j. Requiring Defendant to conduct systematic scanning for data breach related issues;

k. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the PII data; and

l. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

D. That the Court award Plaintiff and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

F. That the Court award Plaintiff and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

G. That the Court award Plaintiff and the Class their reasonable attorneys' fees and costs of suit;

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

**JURY TRIAL DEMANDED**

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs respectfully demand a trial by jury for all claims.

DATED: December 19, 2023

**KOPELOWITZ OSTROW P.A.**

Kenneth Jay Grunfeld, Esq.
65 Overhill Road
Bala Cynwyd, PA 19004
Tel: (954) 525-4100
Email: grunfeld@kolawyers.com

**CLARKSON LAW FIRM, P.C.**
Ryan J. Clarkson (*pro hac vice* forthcoming)
Glenn Danas (*pro hac vice* forthcoming)
Yana Hart (*pro hac vice* forthcoming)
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Email: rclarkson@clarksonlawfirm.com
Email: gdanas@clarksonlawfirm.com
Email: gdanas@clarksonlawfirm.com
Email: yhart@clarksonlawfirm.com

**TYCKO & ZAVAREEI LLP**
Hassan A. Zavareei (*pro hac vice* forthcoming)
1828 L Street NW, Ste. 1000
Washington, DC 20036
Tel: (202) 973-973-0900
Email: hzavareei@tzlegal.com

*Attorneys for Plaintiffs*