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

JESSICA DURHAM, individually and on behalf of all others similarly situated, Plaintiff, v. COMCAST CABLE COMMUNICATIONS LLC, Defendant.	Case No.: 2:24-cv-639 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Jessica Durham ("Plaintiff") brings this Class Action Complaint against Defendant Comcast Cable Communications LLC ("Comcast" or "Defendant"), individually and on behalf of all others similarly situated, and alleges as follows, upon information and belief, investigation of counsel, and her own personal knowledge.

NATURE OF THE ACTION

1. Plaintiff brings this action against Comcast for its failure to properly secure and safeguard highly valuable, protected, personally identifiable information including, among other things, 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"), failure to comply with industry standards to protect information systems that contain PII, and failure to provide adequate notice to Plaintiff and other members of the Class that their PII had been accessed and compromised.

2. Comcast owns and operates Xfinity – 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.

3. In order to obtain Xfinity's services, customers are required to entrust Comcast with their PII, which Comcast uses in order to perform its regular business activities.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. Between October 16 and October 19, 2023, hackers exploited a critical-rated, unpatched security vulnerability, accessed Comcast's internal systems, and accessed the PII of approximately 36 million Xfinity customers (the "Data Breach" or "Breach").

6. As a direct and proximate result of Comcast's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of cybercriminals.

7. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the disclosure of their private information; (v) failure to receive the benefit of their bargains with Defendant related to their financial products; (vi) nominal damages; and (vii) the continued and certainly increased risk to their PII, and damages in an amount equal to the cost of securing identity theft products to assisting in monitoring and protecting them from identity theft, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain

backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

8. As such, on behalf of herself and all others similarly situated, Plaintiff brings claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment, seeking damages and injunctive relief.

PARTIES

9. Plaintiff Jessica Durham ("Plaintiff" or "Durham") is a resident and citizen of Illinois. Plaintiff has been a customer of Comcast for approximately fifteen years and currently uses Comcast's Xfinity internet service.

10. On December 22, 2023, Plaintiff received an email notice from Defendant informing her of the Data Breach and the exposure of her PII. The email notice informed Plaintiff that her username and hashed password was taken, and that some customers had their names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers taken by unauthorized third parties.

11. Since the announcement of the Data Breach, Plaintiff has been required to spend her valuable time monitoring her various accounts in an effort to detect and prevent any misuses of her PII – time which he would not have had to expend but for the Data Breach.

12. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

13. Defendant Comcast Cable Communications LLC ("Defendant" or "Comcast") is a Delaware limited liability company that maintains its headquarters at Comcast Center, 1701 JFK Boulevard, Philadelphia, Pennsylvania 19103.

14. Upon information and belief, Comcast Corporation is the only member of Comcast Cable Communications LLC.

15. Comcast Corporation is a Pennsylvania corporation with its principal place of business in Philadelphia, Pennsylvania.

16. Defendant is a citizen of each state in which its members is a citizen. As such, Defendant is a citizen of Pennsylvania.

17. Plaintiff will amend her Complaint should additional limited liability company members be revealed.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action pursuant to 28 U.S.C. §1332(d), the Class Action Fairness Act, because Plaintiff and at least one member of the Class, as defined below, are citizens of a different state than Defendant, there are more than 100 members of each of the Classes, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendant because Defendant is a citizen of the Commonwealth of Pennsylvania.

20. This Court is the proper venue for this action pursuant to 28 U.S.C. §1391(b)(1), because Defendant is located in this District, a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District, Defendant conducts substantial business within this District, and Defendant has harmed Class Members residing in this District.

FACTUAL BACKGROUND

A. Defendant Provides Technology Services Involving Highly Sensitive Data

21. Comcast provides telecommunications and internet connectivity services in the United States to residential and business customers through Xfinity.[1]

22. Xfinity provides a range of WiFi options, from gig-speed WiFi that takes fewer than 13 milliseconds to load, to its "Internet Essentials" low-cost internet.[2] Xfinity also provides nationwide coverage through access to more than 20 million hotspots.[3]

23. Xfinity, which claims to be the "largest internet provider in the U.S.," has an extremely large customer base.[4]

24. According to its 2022 Annual Report, Comcast provides its various cable communications services to more than 34 million customers.[5] While Comcast primarily serves residential customers, Comcast boasts that its business division is growing as well, and "approaching $10 billion in annual revenue."[6]

25. In order to use Comcast's Xfinity services, customers must create an online account with Defendant. In doing so, customers provide, and Comcast routinely acquires and stores on its systems, PII.

---

1 Comcast Corp., Annual Report (Form 10-K) (Feb. 3, 2023), https://www.cmcsa.com/static-files/156da323-653e-4cc6-9bb4-d239937e9d2f. (last visited Feb. 8, 2024).

2 *Overview*, XFINITY, https://www.xfinity.com/overview (last visited Feb. 8, 2024).

3 *Id.*

4 *Connectivity & Platforms*, COMCAST, https://corporate.comcast.com/company/connectivity-platforms (last visited Feb. 8, 2024).

5 Annual Report, *supra* note 1.

6 *Supra* note 4.

26. Customers are entitled to security of their PII. As a vendor storing sensitive data, Comcast has a duty to ensure that such information is not disclosed or disseminated to unauthorized third parties.

B. The Xfinity Data Breach

27. On December 18, 2023, Comcast began to disseminate notice to customers about the Data Breach (the "Notice").[7]

28. In the Notice, Comcast described the circumstances surrounding the Breach as follows:

> On October 10, 2023, one of Xfinity's software providers, Citrix, announced a vulnerability in one of its products used by Xfinity and thousands of other companies worldwide. At the time Citrix made this announcement, it released a patch to fix the vulnerability. Citrix issued additional mitigation guidance on October 23, 2023. We promptly patched and mitigated our systems.
>
> However, we subsequently discovered that prior to mitigation, between October 16 and October 19, 2023, there was unauthorized access to some of our internal systems that we concluded was a result of this vulnerability. We notified federal law enforcement and conducted an investigation into the nature and scope of the incident. On November 16, 2023, it was determined that information was likely acquired.[8]

29. The delay in Comcast's implementation of the patch allowed hackers to have unauthorized access to Comcast's systems.

---

[7] *Notice to Customers of Data Security Incident*, XFINITY (Dec. 18, 2023), https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf?INTCMP=dsi-12152023 (last visited Feb. 8, 2024).

[8] *Id*.

30. Once able to access Comcast's systems, these malicious third-party hackers stole information including usernames and hashed passwords, names, contact information, last four digits of social security numbers, dates of birth, and secret security questions and answers.[9]

31. The information obtained in the Data Breach contains the PII of approximately 36 million individuals.[10]

C. Defendant Obtains, Collects, and Stores Plaintiff's and Class Members' PII

32. In the ordinary course of doing business with its customers, Comcast regularly requires Plaintiff and Class Members to provide their PII. In its Privacy Policy, Comcast declares it "follow[s] industry-standard practices to secure the information [Comcast] collect[s] to prevent the unauthorized access, use, or disclosure of any personal information [Comcast] collect[s] and maintain[s]."[11]

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Comcast assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

34. Plaintiff and Class Members reasonably expect that service providers such as Comcast will use the utmost care to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

---

9 *Id*.

10 Data Breach Notifications, ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml (last visited Feb. 8, 2024).

11 *Privacy*, XFINITY, https://www.xfinity.com/privacy (last visited Feb. 8, 2024).

35. Comcast acknowledges its obligation to keep its customers' PII confidential, stating, "Your privacy matters to us," and, "We are committed to protecting your privacy."[12]

36. Plaintiff and Class Members had a reasonable expectation, based in part on Comcast's own statements, that their sensitive personal information would be protected. However, despite Comcast's stated commitment to data security, Comcast failed to adopt reasonable measures to prevent the unauthorized access to Plaintiff's and Class Members' PII, and allowed for the release of said information to unauthorized bad actors.

37. Had Comcast maintained its data security network and worked diligently to correct vulnerabilities, remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Comcast could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

D. The Value of Private Information and Effects of Unauthorized Disclosure

38. Comcast was well aware that the protected PII which it acquires is highly sensitive and of significant value to those who would use it for wrongful, nefarious purposes.

39. Comcast also knew that a breach of its computer systems, and exposure of the PII therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

40. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[13] Indeed, a robust "cyber black market" exists in which criminals openly post

---

12 *Id.*

13 *What To Know About Identity Theft*, FED. TRADE COMM'N (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Feb. 8, 2024).

stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

41. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

42. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[14]

43. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[15]

44. The ramifications of Comcast's failure to keep Plaintiff's and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

45. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information,

---

14 *Data Breach Report: 2021 Year End*, RISK BASED SEC. (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last visited Feb. 8, 2024).

15 *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Feb. 8, 2024).

> including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[16]

46. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

47. A poll of security executives predicted an increase in attacks over the near term from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[17]

48. Due to high-profile data breaches at other companies, Comcast knew or should have known that its computer systems would be targeted by cybercriminals.

49. Comcast also knew or should have known the importance of safeguarding the PII with which it was entrusted and of the foreseeable consequences if its data security systems were

---

[16] Erika Harrell, *Victims of Identity Theft, 2018*, U.S. DEP'T OF JUST. (Apr. 2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited Feb. 8, 2024).

[17] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited Feb. 8, 2024).

breached. Comcast failed, however, to take adequate cybersecurity measures to prevent the Data Breach and release of its customers' PII from occurring.

E. FTC Guidelines

50. Comcast is prohibited by the Federal Trade Commission Act, 15 U.S.C. §45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("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.

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

52. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[19]

53. The FTC recommends that businesses:

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a

[18] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Feb. 8, 2024).

[19] *Supra* note 16.

certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

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

55. Upon information and belief, Comcast failed to properly implement one or more of the basic data security practices described above. Comcast's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the

unauthorized release of Plaintiff's and Class Members' PII to threat actors. Further, Comcast's failure to implement basic data security practices constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

56. Comcast was, at all times, fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII and storing payment information. Comcast was also aware of the significant repercussions that would result from its failure to do so.

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

F. Plaintiff and Class Members Suffered Damages

58. The ramifications of Comcast's failure to keep user PII secure are long lasting and severe. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time.[20]

59. In 2021 alone, identity theft victims in the United States had financial losses totaling $16.4 billion.[21]

60. Besides the monetary damage sustained, consumers may also spend anywhere from one day to more than six months resolving identity theft issues.[22]

61. Ultimately, the time that victims spend monitoring and resolving identity theft issues takes an emotional toll. Approximately 80% of victims of identity theft experienced some

---

[20] Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics (last visited Feb. 8, 2024).

[21] Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, U.S. DEP'T OF JUST. (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf (last visited Feb. 8, 2024).

[22] *Supra* note 20.

type of emotional distress, and more than one-third of victims experienced moderate or severe emotional distress.[23]

62. Plaintiff values her privacy and sensitive personal information, especially regarding her financial information. Plaintiff has taken reasonable steps to maintain the confidentiality of her PII, and she has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

63. Plaintiff only allowed Defendant to maintain, store, and use her PII because she believed that Defendant would use basic security measures to protect her PII. As a result, Plaintiff's PII was within the possession and control of Defendant at the time of the Data Breach.

64. Plaintiff's Comcast bill was linked to her US Bank account.

65. On December 21, 2023, Plaintiff contacted the Lake County Sheriff's Office Criminal Investigations Division to report fraudulent activity on her US Bank credit card. According to the related police report, Plaintiff stated that on December 20, 2023 she received a phone call from her bank in reference to unusual transactions on her credit card. Plaintiff informed the bank that she did not make those purchases or authorize anyone to do so. Plaintiff also stated that an unknown person had submitted a change of address form in her name without permission. The bank froze all of her accounts to prevent further fraudulent activity. Plaintiff contacted the sheriff's office on two additional occasions with further information.

66. Plaintiff has spent hours of her time dealing with the fraudulent bank withdrawals, contacting the bank's fraud department, the sheriff's office and credit monitoring services such as Transunion. Her fraud case remains open.

---

[23] *Id.*

67. Plaintiff has seen a dramatic increase in spam email solicitations and phone calls since the Data Breach.

68. In addition to closing all her US Bank accounts, Plaintiff was forced to cancel and re-do all her autopay bills that were attached to the closed accounts.

69. The timing of the fraud in the days ahead of the Christmas holiday caused Plaintiff worry and distress, as she suddenly had no access to her US Bank accounts. Plaintiff did not regain access to any funds until December 27, 2023, when the bank provided her with a provisional credit. She continues to suffer stress, fear and anxiety about the actual and potential wrongful access and use of her PII.

70. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

71. As a result of Comcast's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their highly valuable PII; the imminent and certainly impending injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII with which it was entrusted.

CLASS ALLEGATIONS

72. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the Comcast Data Breach which occurred on or around October 2023.

73. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

74. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

75. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach. Based upon public filings, the number of people impacted is approximately 36 million.

76. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether and to what extend Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII;

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

h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

i. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

j. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

77. **Typicality.** Plaintiff's claims are typical of the claims of the Class Members. The claims of Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard their PII. Plaintiff and Class Members entrusted Defendant with their PII, and it was subsequently released to an unauthorized third party.

78. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

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

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

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

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

82. Plaintiff restates and realleges all proceeding allegations as if fully set forth herein.

83. Comcast owed a duty under common law to Plaintiff 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.

84. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Comcast's security systems to ensure that Plaintiff's and Class Members' PII in Comcast's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

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

86. Comcast had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Comcast was obligated to act with reasonable care to protect against these foreseeable threats.

87. Comcast admits that it has the responsibility to protect the customer data with which it was entrusted. Yet, Comcast did not live up to that responsibility.

88. Comcast breached the duties owed to Plaintiff and Class Members and thus was negligent. Comcast breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) promptly disclose that Plaintiff's and Class Members' PII in Comcast's possession had been or was reasonably believed to have been, stolen or compromised.

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

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

a. Theft of their PII;

b. Costs associated with requesting credit freezes;

c. Costs associated with the detection and prevention of identity theft;

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

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

f. 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;

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

h. Damages to and diminution in value of their PII entrusted to Comcast with the mutual understanding that Comcast would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; and

i. 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 Plaintiff and Class Members.

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

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

92. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

93. 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 PII. Various FTC publications and orders also form the basis of Comcast's duty.

94. Comcast violated Section 5 of the FTC Act by failing to use reasonable measures to protect 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.

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

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

97. 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 Plaintiff and Class Members.

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

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

99. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

100. Comcast required Plaintiff and Class Members to provide their PII as a condition for using Xfinity's services.

101. In doing so, Plaintiff and Class Members entered into implied contracts with Comcast by which Defendant agreed to safeguard and protect such PII, keep such PII secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their PII had been breached, compromised, or stolen.

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

103. Indeed, implicit in these exchanges was a promise by Defendant to ensure the PII of Plaintiff and Class members in its possession would be used to provide the agreed-upon services and that Comcast would take adequate measures to protect Plaintiff's and Class Members' PII and timely notify them in the event of a data breach.

104. It is clear by these exchanges that the parties intended to enter into implied agreements supported by mutual assent. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of services. Conversely, Comcast presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members services through Xfinity.

105. Plaintiff and Class Members would not have provided their PII to Comcast had they known that Defendant would not safeguard their PII as promised, or provide timely notice of a data breach.

106. Plaintiff and Class Members fully performed their obligations under their implied contracts with Xfinity.

107. Xfinity breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

108. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the PII;

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

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

f. 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;

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

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant

would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others; and

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

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

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

110. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

111. Plaintiff brings this claim in the alternative to their breach of implied contract claim.

112. By engaging in the conduct described in this Complaint, Comcast has knowingly obtained and derived benefits from Plaintiff and Class Members at Plaintiff's 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.

113. By engaging in the acts and failures to act described in this Complaint, Comcast has been knowingly enriched by the savings in costs that should have been reasonably expensed to protect the PII of Plaintiff and the Class. Defendant 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.

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

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

116. Plaintiff and Class Members have no adequate remedy at law. As a direct and proximate result of Comcast's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

117. Comcast should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

118. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

119. 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.

120. Comcast owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' PII.

121. Comcast still possesses PII regarding Plaintiff and Class Members.

122. Plaintiff alleges that Comcast's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of his PII, and the risk remains that further compromises of their PII will occur in the future.

123. 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 and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act; and

b. Comcast continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class Members' PII.

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

125. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Comcast. The risk of another such breach is real, immediate, and substantial. If another breach at Comcast occurs, Plaintiff 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.

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

127. 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, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

SIXTH CAUSE OF ACTION
VIOLATION OF PENNSYLVANIA'S UNFAIR TRADE PRACTICES ACT
(On Behalf of Plaintiff and the Class)

128. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

129. As a consumer of Defendant's services, directly or indirectly, Plaintiff is authorized to bring a private action under Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"). 73 P.S. §201-9.2.

130. Plaintiff is a "person" within the meaning of 73 P.S. §201-2(2).

131. Plaintiff and Class Members provided their PII to Defendant pursuant to transactions in "trade" and "commerce" as meant by 73 P.S. §201-2(3), for personal, family, and/or household purposes.

132. The UTPCPL prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." 73 P.S. §201-3.

133. This Count is brought for Defendant's unfair and deceptive conduct, including Defendant's unlawful and unfair and deceptive acts and practices, which "creat[ed] a likelihood of confusion or of misunderstanding" for Plaintiff and Class Members as meant by 73 P.S. §201-2(4)(xxi).

134. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale and advertisement of the goods purchased by Plaintiff and the Class in violation of 73 P.S. §201-3, including but not limited to the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members PII, which was a proximate and direct 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. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify Plaintiff and Class Members of the Data Breach;

e. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Class Members' PII; and

f. 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 and Class Members' PII, including duties imposed by the FTC Act and the Graham Leach Bliley Act.

135. The above unfair and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

136. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and Class Members' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing, and reckless with respect to the rights of Plaintiff and Class Members.

137. Plaintiff and Class Members relied on Defendant's unfair and deceptive acts and practices when they paid money in exchange for goods and services and provided their PII to Defendant.

138. Plaintiff and Class Members relied on Defendant to safeguard and protect their PII and to timely and accurately notify them if their data had been breached and compromised.

139. Plaintiff and Class Members would not have paid for Defendant's services, or would have paid less, had they known that Defendant did not implement reasonable data security policies and procedures.

140. Plaintiff and Class Members seek all available relief under the UTPCPL, 73 P.S. §201-1 *et seq*.

PRAYER FOR RELIEF

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

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

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such

information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of the network is compromised, hackers cannot gain access to other portions of its systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant 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 the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor its information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from its servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant'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 with compliance of the Court's final judgment.

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands that this matter be tried before a jury.

Dated: February 13, 2024

Respectfully submitted,

LEVIN SEDRAN & BERMAN LLP

/s/ Charles E. Schaffer
Charles E. Schaffer, Esquire
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone (215) 592-1500
cschaffer@lfsblaw.com

SCOTT+SCOTT ATTORNEYS AT LAW LLP

Joseph Guglielmo
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Tel.: (212) 223-6444
Fax: (212) 223-6334
jguglielmo@scott-scott.com

Erin Green Comite
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Tel.: (860) 537-5537
Fax: (860) 537-4432
ecomite@scott-scott.com

Attorneys for Plaintiff