UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

ROBERT M. ROSEMAN, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

COMCAST CORPORATION, d/b/a XFINITY

Defendant.

CASE NO. 2:24-cv-00271

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Robert M. Roseman ("Plaintiff") brings this action individually and on behalf of a class of all others similarly situated against the Defendant, Comcast Corporation. ("Comcast" or "Defendant" or "Xfinity") and alleges the following:

I. NATURE OF THE ACTION

1. Plaintiff brings this action, individually and on behalf of all other similarly situated individuals against Defendant Comcast Corporation ("Comcast" or "Defendant") because of Defendant's failure to adequately protect Plaintiff and the Class's sensitive personal identifiable information ("PII") which includes personal and confidential information of millions of customers including, but not limited to, usernames, account passwords, home and email addresses, telephone numbers, dates of birth, and Social Security numbers.

2. This information was compromised in a massive security breach of Comcast's Xfinity systems ("Xfinity") that occurred between October 16th and 19th of 2023 (the "Data Breach" or "Breach").[1] Xfinity is the tradename Comcast uses for its TV and internet service provided to consumers. However, the Breach was only publicly disclosed on December 18, 2023.[2] While the true extent of the Breach is still unknown, it implicates millions of customers who utilize Comcast throughout the United States.

3. While Comcast notified customers of the Breach, these notifications came almost two full months after the breach occurred and more than a month after it was discovered.[3] In the interim, Plaintiff and other affected Class Members have been deprived of the opportunity to quickly take the necessary measures to protect their PII and minimize potential harm caused by the Breach.

[1] https://www.businesswire.com/news/home/20231218979935/en/Notice-To-Customers-of-Data-Security-Incident.
[2] Id.
[3] Id.

II. THE PARTIES

A. Plaintiff

4. Plaintiff Robert M. Roseman is an adult individual and at all relevant times herein was a resident and citizen of the Commonwealth of Pennsylvania. Comcast sent Mr. Roseman a "Notice of Data Security Incident" informing him that his PII data was breached.

5. Plaintiff was unaware of the Data Breach until receiving that letter.

6. Like millions of other Comcast Xfinity customers, Plaintiff entered several pieces of PII required to utilize and pay for Xfinity services.

7. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

8. Plaintiff would not have given Comcast his PII if he had known that Comcast employed inadequate cybersecurity safeguards and that such information was vulnerable to cyberattack.

B. Defendant

9. Defendant Comcast Corporation is a publicly traded company that is incorporated in Pennsylvania. It is headquartered in Philadelphia.

III. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5

million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Comcast. See 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

11. This Court has personal jurisdiction over Comcast because Comcast is a citizen of the Commonwealth of Pennsylvania and headquartered at 1701 JFK Boulevard, Philadelphia, Pennsylvania 19103. Furthermore, Comcast conducts substantial business in the Commonwealth.

12. Venue properly lies in this district pursuant to 28 U.S.C. §1392(b)(1) because, as noted above, Comcast is a citizen of the Commonwealth of Pennsylvania.

IV. GENERAL ALLEGATIONS

A. Defendant Collects and Stores Plaintiffs' Information

13. Comcast is one of the most well-known media and technology companies in the world. Indeed, Comcast commands a global presence through the operation and distribution of national, regional, and international cable networks; participation in film and television studio production and distribution; provision of video, broadband, voice, and wireless phone services.

14. As of December 2022, Comcast boasted a total of 31.8 million residential Xfinity customers. Xfinity provides broadband, video, voice, and wireless services to these customers.

15. As part of its operations, Comcast collects a massive amount of its customers' sensitive personal information, including credit and debit card numbers, expiration dates, cardholder names, three or four-digit security codes (commonly referred to as "CVV" codes), and PII such as home addresses, dates of birth, and Social Security numbers. Indeed, customers who wish to subscribe to Xfinity internet, cable, or streaming services, like Plaintiff, must create an account and provide Comcast with this information. All of this sensitive data is stored on

Comcast's information technology network.

16. PII is incredibly valuable because it is essential to conduct everyday business – from applying for employment or government benefits, to securing financing for major purchases such as a home or vehicle. In the wrong hands, it can allow a person to commit harmful and serious crimes such as financial fraud and identity theft. Thus, Plaintiff and Class Members take measures to safeguard this data and to prevent its misuse, including concealing their usernames and passwords from the public sphere and avoiding disclosing their PII on suspicious or unsafe websites.

17. Comcast is well aware of the value of its customers' PII. In fact, the Xfinity Privacy page states "[w]e know you rely on us to stay connected to the people and things you care about most. And your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure…"[4] Thus Comcast knew the importance of safeguarding this information against misappropriation and that it was responsible for maintaining reasonable safeguards to protect its customers' PII from unauthorized access or use. Furthermore, Comcast knew that in providing this information, its customers were entitled to, and did in fact rely on, Comcast to keep that PII secure from would-be data thieves.

B. The Data Breach

18. The Defendant makes several representations to its customers regarding the strength of its cybersecurity infrastructure, including that Comcast "help[s] protect you with multiple layers of security that automatically detect and block hundreds of thousands of cyber events every second," and "follow[s] industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we

[4] https://www.xfinity.com/privacy.

collect and maintain."[5]

19. However, Comcast fell far short of meeting its duty to safeguard the millions of pieces of customer PII.

20. Comcast became aware of a vulnerability in one of the software products used by Xfinity on October 10, 2023 and was advised to patch the software *as soon as possible* to prevent serious cybersecurity breaches.[6] However, Comcast failed to take sufficient preventative and protective measures in time, and between October 16 and 19, 2023, unauthorized persons accessed millions of customer PII stored on Xfinity systems.[7] Comcast belatedly performed the recommended patches on October 23, mere days after the Breach occurred.

21. Even after performing the software patch, it was only "during a routine cybersecurity exercise on October 25" that Comcast discover the cyberattack.[8]

22. Upon information and belief, *nearly all* Xfinity customers in the U.S. had their PII accessed during this Breach.[9]

23. Only in mid-December, more than *two months* after the Breach occurred, did Comcast belatedly publish a general Notice regarding the incident (the "Notice"), despite conducting an investigation and concluding as early as November 16, 2023 that customer PII had been accessed.

24. According to the Notice, Comcast "notified federal law enforcement and conducted an investigation into the nature and scope of the incident" but to date it is wholly unclear what such investigative efforts involved. Upon information and belief, the investigation

[5] https://www.xfinity.com/privacy/
[6] https://www.theverge.com/2023/12/18/24007082/xfinity-data-breach-hack-notice-citrix
[7] https://www.businesswire.com/news/home/20231218979935/en/Notice-To-Customers-of-Data-Security-Incident
[8] Id.
[9] See https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml; see also https://www.usatoday.com/story/tech/2023/12/20/xfinity-data-breach-comcast-hack/71982101007/

is still ongoing.

25. The Notice indicated that the hackers accessed and acquired account usernames, hashed passwords, and customer names, contact information, last four digits of social security numbers, dates of birth and secret questions and answers.

26. The Notice is sparse; it does not provide any substantive details about who accessed the system, the exact date of the Breach, the software involved, or Xfinity's efforts to prevent the Breach. Thus, Plaintiff and Class Members are at a disadvantage in trying to determine what actions to take in response to Xfinity's negligent handling of their PII.

27. Due to the ongoing nature of the investigation, it is highly possible that the hackers accessed other pieces of PII, such as bank account and debit or credit information stored on customers' accounts for payment.

28. Not only did the Defendant fail to notify Xfinity customers of the Breach in a timely manner or with any meaningful information, but the "solutions" offered to customers are, at best, inadequate and at worst, moot. First, Comcast required customers to reset their passwords and enable two-factor authentication. However, resetting an account password does nothing to protect the PII that had already been accessed by nonauthorized persons. The Plaintiff's, or any Class Member's, PII could have already been sold or otherwise used for any number of nefarious purposes.

29. Comcast also advised customers to routinely monitor and review financial and other accounts, as well as credit reports.[10] This is no simple task, as Plaintiff and other Class Members have many accounts, online and otherwise, that could be accessed with the PII that was stolen from Xfinity's systems. Such monitoring requires time and effort that Plaintiffs would

[10] https://assets.xfinity.com/assets/dotcom/learn/Data_Incident.pdf

otherwise not have expended on these matters. Furthermore, given the scant details Comcast has provided about the Breach as it continues its investigation, the burden of discovering possible fraudulent transactions has been shifted to Xfinity customers.

30. Notably, Xfinity has not offered free credit monitoring or identity fraud protection to those impacted by the Breach, which firms typically offer their customers following a serious data breach. Thus, Comcast indicates an unwillingness to assist or protect its customers from the potential consequences of its own negligence.

C. Defendant Knew or Should Have Known That its Systems were Vulnerable to Cyberattack

31. Comcast was on notice of the vulnerabilities in its cybersecurity systems. It admits that it received notice approximately two weeks before the Breach that its software was vulnerable to attack.[11]

32. Independent of this explicit knowledge, the frequent occurrence of cyberattacks against corporations that collect and store customer PII continues to increase year-over-year, a fact that should have alerted Comcast to potential vulnerabilities and the need to ensure the robustness of its cybersecurity infrastructure.

33. According to the Identity Theft Resource Center, the number of data compromises reported in the first six months of 2023 was higher than the *total* number of compromises reported every year except one in between 2005 and 2020.[12]

34. In fact, several major communications corporations have reported massive recent data breaches, including US Cellular in January 2023, AT&T and Verizon in March 2023, and T-Mobile in 2021. These corporations provide the same types of services as Comcast and Xfinity.

[11] https://assets.xfinity.com/assets/dotcom/learn/Data_Incident.pdf
[12] https://www.idtheftcenter.org/wp-content/uploads/2023/07/20230712_H1-2023-Data-Breach-Analysis.pdf

Thus, Comcast knew or should have known that the PII it collects and stores from its customers is the type that hackers are constantly trying to access and misappropriate.

35. Comcast has demonstrated an acute awareness of both the value of customer PII and the importance of securing this PII throughout its Privacy Policy.

D. Defendant Failed to Implement Reasonable and Appropriate Measures to Prevent the Breach

36. PII of the type involved in the Breach is highly valuable to both its owners and bad actors. Customers use this information to conduct essential daily business such as apply for employment or government benefits, secure financing for major purchases, and engage in other commercial activities with public and private entities. In the wrong hands, it can allow a person to commit harmful and serious crimes such as fraud and identity theft, drain bank accounts, or steal tax refunds. Thus, it is essential that any entity entrusted with such information maintain robust security measures to protect it.

37. Comcast is, and at all relevant times has been, aware that the PII it collects and maintains on behalf of its customers is highly sensitive and requires safeguarding. In fact Comcast explicitly states that it "know[s] [customers] care about [their] privacy and the protection of [their] personal information" [13] and is "committed to protecting [customers'] privacy".[14] And a spokesperson for Xfinity commented that "[w]e take the responsibility to protect our customers very seriously".[15] This is confirmed in the Xfinity Privacy page where it states "[w]e know you rely on us to stay connected to the people and things you care about most. And your privacy is essential when you use our products and services. That's why we're always

[13] https://www.xfinity.com/privacy/policy
[14] https://www.xfinity.com/privacy/policy
[15] https://www.theverge.com/2023/12/18/24007082/xfinity-data-breach-hack-notice-citrix

working to keep your personal information secure…"[16]

38. Comcast's Privacy Policy explicitly states that it employs "technical, administrative, and physical safeguards."[17]

39. Indeed, as a sophisticated international conglomerate, Comcast was, at all relevant times, aware of the importance of safeguarding its customers' PII from the foreseeable and serious consequences that would occur if its data security systems and computer servers were breached.

40. Yet despite this awareness, Comcast's safeguards were inadequate and failed on or around October 16, 2023.

41. Comcast acted negligently in failing to implement adequate safeguards to protect customers' personal information, even after being notified of the risk of a Breach. This failure runs afoul of industry best practices, which include, but are not limited to, regularly testing security systems, ensuring that security updates and patches are routinely implemented,

42. Furthermore, through its failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, Comcast has violated Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. The Federal Trade Commission's ("FTC") document "Protecting Personal Information: A Guide for Business" highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks. These guidelines advise businesses to take the following steps to establish reasonable data security practices: protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; understand their network's vulnerabilities; and implement policies for installing vendor-

[16] https://www.xfinity.com/privacy/
[17] Xfinity Privacy Policy, https://www.xfinity.com/privacy/policy

approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

E. Plaintiff and Class Members Have Been Injured by Comcast's Negligence

43. Comcast's failure to prevent and timely detect the Breach led to the compromise of millions of pieces of PII for millions of customers. As discussed, the Breach has serious real-world implications for Plaintiffs such as identity theft and financial fraud.

44. But Comcast's proposed remedies do not necessarily prevent actual fraud. Because criminals can use the PII from the Breach to commit a litany of crimes such as drain bank accounts, identity theft, or open utility accounts, Plaintiff and Class Members must employ heightened scrutiny to ensure that their PII is not being misappropriated.

45. Nor do these measures ensure protection from fraud going forward. For example, Comcast customers' stolen PII may be sold on the "dark web" at some undetermined point in the future.

46. Furthermore, Comcast' failure to adequately protect its customers' PII has resulted in customers having to undertake various tasks (e.g., obtaining credit monitoring, checking credit reports, monitoring accounts, etc.) that require time and effort that they would otherwise not have expended on these tasks. At the same time, Comcast has provided only sparse details about the Breach as it conducts its investigation and is putting the burden on the consumer to discover

[18] FEDERAL TRADE COMMISSION, Protecting Personal Information: A Guide for Business (October 2016), available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Jan. 19, 2024).

possible fraudulent transactions.

V. CLASS ALLEGATIONS

47. Plaintiff brings this action on behalf of themself, as representative of the Class defined below, pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), and seeks certification of the following Nationwide Class:

All persons in the United States whose PII was compromised due to the Data Breach to Xfinity systems announced on December 18, 2023 by Comcast Corporation.

48. Plaintiff reserves the right to revise the above Class definitions and any of the averments of fact herein based on facts adduced in discovery.

49. The Class is so numerous that joinder of all members in this action is impracticable. There are millions of geographically dispersed Class members.

50. The Class members, moreover, can be readily identified and notified in an administratively feasible manner using, among other information, Comcast's electronic records.

51. Plaintiff's claims are typical of those of the Class. Plaintiff and all members of the Class were injured by Comcast's uniform negligence. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each Class Member had their PII compromised in the same way by the same conduct by Comcast.

52. Plaintiff will fairly and adequately protect and represent the interests of Class members. The interests of Plaintiff and Plaintiff's counsel are fully aligned with, and not antagonistic to, the interests of the Class members. Plaintiff is willing and able to dispatch the duties incumbent upon a class representative to protect the interests of all Class members. In addition, Plaintiff's counsel has significant experience successfully prosecuting complex class

actions and possesses the necessary resources to vigorously litigate the case on behalf of the Class.

53. There are multiple questions of law and fact that are common to the Class, including, but not limited to:

a. Whether Defendant's data security systems complied with applicable state and federal laws and regulations;

b. Whether Defendant's data security systems met minimum industry and FTC standards;

c. Whether Defendant knew or should have known that its data security systems were inadequate and vulnerable to cyberattack;

d. Whether Defendant owed duties to Plaintiff and members of the Class to protect their PII and to provide timely and accurate notice of the Breach to Plaintiff and the Class, and whether it breached these duties;

e. Whether Defendant wrongfully failed to inform Plaintiff and members of the Class that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard consumers' PII;

f. Whether Defendant has taken adequate preventive and precautionary measures to ensure Plaintiff and Class members will not experience further harm;

g. Whether Defendant violated the FTC Act;

h. Whether Plaintiff and members of the Class suffered injury as a proximate result of Defendant's conduct or failure to act; and

i. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the Class.

54. Questions of law and fact common to the members of the Class will predominate over any individualized questions of law or fact. Defendant has acted and refused to act on grounds generally applicable to the Class.

55. Class treatment is the superior method for the fair and efficient adjudication of this controversy. It will allow the scores of Class members to prosecute their common claims,

and for Defendant to defend itself against these claims, in front of a single court simultaneously and efficiently before ultimately reaching resolution without the unnecessary duplication of effort and expense that separate actions would present. The benefits of proceeding with this procedural mechanism, including providing injured persons with a method of obtaining redress for claims that might not be practicable for them to pursue individually, substantially outweigh any difficulties that may arise in the management of this case as a class action.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

56. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

57. Comcast collected PII from Plaintiff and Class members throughout the United States.

58. Comcast owed a duty to Plaintiff and the Class to maintain the confidentiality of and to exercise reasonable care in safeguarding and protecting the PII in Comcast' possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Comcast's networks and data security systems to ensure that Plaintiff's and Class members' PII in Comcast's possession was adequately protected while stored on Xfinity systems.

59. Comcast owed a duty to Plaintiff and Class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks adequately protected the PII of Plaintiff and Class members whose confidential data Comcast obtained and maintained.

60. Comcast knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and Class members' PII and the critical importance of providing adequate security for that information.

61. Comcast's conduct created a foreseeable risk of harm to Plaintiff and Class members. This conduct included, but was not limited to, Comcast's failure to take the measures to prevent the Breach and its decision not to comply with industry standards for the safekeeping and maintenance of Plaintiff's and Class members' PII.

62. Comcast knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Comcast knew or should have known that hackers would attempt or were attempting to access the PII contained on the Xfinity systems.

63. Comcast breached the duties it owed to Plaintiff and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class members' PII, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiff and Class members.

64. As a direct and proximate result of Comcast' negligent conduct, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

65. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

66. Pursuant to the FTC Act, 15 U.S.C. § 45, Comcast had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class

members' PII.

67. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Comcast, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Comcast's duty to protect Plaintiff's and Class members' sensitive information.

68. Comcast violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein.

69. Comcast had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class members' PII.

70. Comcast breached its duties to Plaintiff and Class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

71. Comcast' violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence per se.

72. But for Comcast's wrongful and negligent breach of its duties owed to Plaintiff and Class members would not have been injured.

73. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Comcast's breach of its duties. Comcast knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and Class members to suffer the foreseeable harms associated with the exposure of their PII.

74. Had Plaintiff and Class members known that Comcast did and does not

adequately protect customers' PII, they would not have given their PII to Comcast.

75. As a direct and proximate result of Comcast's negligence per se, Plaintiff and Class members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Class)

76. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

77. Plaintiff and Class members who gave their PII to Comcast during the period in which the Breach occurred had contracts with Comcast.

78. Specifically, Plaintiff and Class members entered their PII into Comcast databases to obtain various products and services from Comcast. In exchange, Comcast agreed, among other things: (l) to provide various services to Plaintiff and Class members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) to protect Plaintiff's and Class members' PII in compliance with federal and state laws and regulations and industry standards.

79. The Xfinity Privacy page explicitly states;

"[w]e know you rely on us to stay connected to the people and things you care about most. And your privacy is essential when you use our products and services. That's why we're always working to keep your personal information secure…"

80. Thus, Comcast knew that its uniform contracts with its customers required it to

safeguard this information against misappropriation and that it was responsible for maintaining reasonable security measures to protect its customers' PII from unauthorized access or use. This contractual obligation includes, at a minimum, promptly taking action after Citrix announced a vulnerability in software used by Defendant.

81. Protection of PII is a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Comcast, on the other hand. Indeed, as set forth, supra, Comcast recognized the importance of data security and the privacy of customers' sensitive financial information in its Privacy Policy. Had Plaintiff and Class members known that Comcast would not adequately protect its customers' PII, they would not have given their PII to Comcast.

82. Comcast did not satisfy its promises and obligations to Plaintiff and Class members under the implied contracts because it did not take reasonable measures to keep their PII secure and confidential, and did not comply with applicable laws, regulations, and industry standards.

83. Comcast materially breached its implied contracts with Plaintiff and Class members by failing to implement adequate data security measures.

84. Plaintiff and Class members fully performed their obligations under their implied contracts with Comcast.

85. Comcast's failure to satisfy its obligations led directly to the successful intrusion of Xfinity systems and stored data and led directly to unauthorized parties' access to and exfiltration of Plaintiff's and Class members' PII.

86. Comcast breached these implied contracts because of its failure to implement appropriate, sufficient security measures.

87. Also, as a result of Comcast' failure to implement necessary security measures,

Plaintiff and Class members have suffered actual damages resulting from the theft of their PII and remain at imminent risk of suffering additional damages in the future.

88. Accordingly, Plaintiff and Class members have been injured as a proximate result of Comcast' breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

PRAYER FOR RELIEF

Plaintiff, on behalf of themself and the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action, appoint Plaintiff as Class representative and their counsel as Class counsel;

B. Enter judgment in favor of Plaintiff and the other members of the Class, and against Comcast under the legal theories alleged herein;

C. Award Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, and restitution;

D. Award Plaintiff and the Class equitable, injunctive, and declaratory relief as may be appropriate;

E. Award Plaintiff and the Class reasonable attorneys' fees and costs as allowable; and.

F. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMAND

Plaintiff demands a jury trial under Federal Rule of Civil Procedure 38(b) on all triable issues.

Dated: January 19, 2024

Respectfully submitted,

BY: /s/ *John A. Macoretta*

John A. Macoretta
Jeffrey L. Kodroff
Diana J. Zinser
SPECTOR ROSEMAN & KODROFF, P.C.
2001 Market Street, Suite 3410
Philadelphia PA 19103
jmacoretta@srkattorneys.com
jkodroff@srkattorneys.com
dzinser@srkattorneys.com

Attorneys for Plaintiff and the Class