

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION**

BRITTANY HAMMOND and TAMIA
CHARLES, on behalf of themselves and all
others similarly situated,

Plaintiffs,

v.

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

Defendants.

Case No.: _____

CLASS ACTION

DEMAND FOR A JURY TRIAL

Plaintiffs Brittany Hammond and Tamia Charles ("Plaintiffs") bring this class action against Defendants Citrix Systems, Inc. ("Citrix") and Comcast Cable Communications, LLC d/b/a Xfinity ("Comcast") (collectively, "Defendants") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Defendants' failure to implement reasonable and industry standard data security practices.
2. Citrix is a Florida-based software corporation that provides software products and services to its clients that allow those clients to seamlessly manage and monitor their internal applications, including those that allow access to confidential consumer information.

3. Comcast is a limited liability company that provides “broadband, mobile, and entertainment” products and services to its customers.¹

4. Plaintiffs bring this Complaint against Defendants for their failure to properly secure and safeguard the sensitive information that they collected and maintained as part of their regular business practices, including, but not limited to: names, usernames, password information, contact information, dates of birth, secret questions and answers, and Social Security numbers (“personally identifying information” or “PII”).

5. Upon information and belief, former and current Comcast customers are required to entrust Defendants with sensitive, non-public PII, without which Defendants could not perform their regular business activities, in order to obtain products and/or services from Comcast. Defendants retain this information for at least many years and even after the relationship has ended.

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

7. According to the Notice of Data Security Incident email that Comcast sent to Plaintiffs and other impacted Class Members (the “Notice Letter”), 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.”² Subsequently, Comcast “conducted an investigation into the nature and scope of the incident[]” and concluded that “there was

¹ <https://corporate.comcast.com/company>

² The “Notice Letter”. A sample copy is available at <https://apps.web.maine.gov/online/aewviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml>

unauthorized access to some of [Comcast's] internal systems that we concluded was a result of this vulnerability.”³

8. Defendants failed to adequately protect Plaintiffs' and Class Members' PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect Comcast's customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. In breaching their duties to properly safeguard Comcast's customers' PII and give customers timely, adequate notice of the Data Breach's occurrence, Defendants' conduct amounts to negligence and/or recklessness and violates federal and state statutes.

10. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

11. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by their IT vendors to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an

³ *Id.*

unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

12. Plaintiffs and Class Members have suffered injuries as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

13. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Comcast's customers' PII from a foreseeable and preventable cyber-attack.

14. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiffs, is a citizen of a state different from Defendants.

16. This Court has personal jurisdiction over Defendants because Citrix's principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

17. Venue is proper under 18 U.S.C. § 1391(b)(1) because Citrix's principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

PARTIES

18. Plaintiff Brittany Hammond is a resident and citizen of Sicklerville, New Jersey. Ms. Hammond received the Notice Letter, via email, from Comcast, dated December 18, 2023. Ms. Hammond provided her PII to Defendants on the condition that it be maintained as confidential and with the understanding that Defendants would employ reasonable safeguards to protect her PII. If Ms. Hammond had known that Defendants would not adequately protect her PII, she would not have entrusted Defendants with her PII or allowed Defendants to maintain or use this sensitive PII.

19. Plaintiff Tamia Charles is a resident and citizen of Alexandria, Virginia. Ms. Charles received the Notice Letter, via email, from Comcast, dated December 18, 2023. Ms. Charles provided her PII to Defendants on the condition that it be maintained as confidential and

with the understanding that Defendants would employ reasonable safeguards to protect her PII. If Ms. Charles had known that Defendants would not adequately protect her PII, she would not have entrusted Defendants with her PII or allowed Defendants to maintain or use this sensitive PII.

20. Defendant Citrix is a corporation organized under the state laws of Delaware with its principal place of business located in Fort Lauderdale, Florida.

21. Defendant Comcast is a limited liability company organized under the state laws of Delaware with its principal place of business located in Philadelphia, Pennsylvania.

FACTUAL ALLEGATIONS

Defendants' Business

22. Citrix is a Florida-based software corporation that provides software to its clients that allows seamless integration of digital applications, including those that allow access to confidential consumer information.

23. Comcast is a limited liability company that provides “broadband, mobile, and entertainment” products and services to its customers.⁴

24. Plaintiffs and Class Members are current and former customers at Comcast.

25. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

26. Upon information and belief, in the course of collecting PII from Comcast’s customers, including Plaintiffs, Comcast promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

⁴ <https://corporate.comcast.com/company>

27. Indeed, the Privacy Policy posted on Comcast’s website provides that: “[w]e follow industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain. These security practices include technical, administrative, and physical safeguards, which may vary, depending on the type and sensitivity of the information.”⁵

28. Plaintiffs and the Class Members, as former and current customers of Comcast, relied on these promises and on these sophisticated business entities to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers, in general, demand security to safeguard their PII, especially when their Social Security numbers and other sensitive PII is involved.

29. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

30. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Moreover, Comcast had a duty to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have a legal duty to keep Comcast’s customers’ PII safe and confidential.

⁵ <https://www.xfinity.com/privacy/policy>

31. Defendants had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

32. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendants could not perform the services they provide.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

The Data Breach

34. On or about December 18, 2023, Comcast began sending Plaintiffs and other Data Breach victims a Notice of Data Security Incident email (the "Notice Letter"), informing them that:

What Happened? 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.

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

⁶ The "Notice Letter". A sample copy is available at <https://apps.web.maine.gov/online/aewviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml>

35. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

36. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach’s critical facts. Without these details, Plaintiffs’ and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

37. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Comcast failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

38. The attacker accessed and acquired files Defendants shared with a third party containing unencrypted PII of Plaintiffs and Class Members. Plaintiffs’ and Class Members’ PII was accessed and stolen in the Data Breach.

39. Plaintiffs further believe that their and Class Members’ PII was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

40. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members or by

Comcast exercising due diligence in selecting their IT vendors and properly auditing those vendor's security practices.

41. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

42. The unencrypted PII of Class Members may end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

43. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁷

44. To prevent and detect cyber-attacks and/or ransomware attacks Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

⁷ How to Protect Your Networks from RANSOMWARE, at 3, *available at*: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁸

45. To prevent and detect cyber-attacks or ransomware attacks Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

⁸ *Id.* at 3-4.

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].⁹

46. Given that Defendants were storing the PII of Comcast’s current and former customers, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

47. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach

⁹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

and the exposure of the PII of more than thirty-five million individuals, including that of Plaintiffs and Class Members.

Defendants Acquire, Collect, And Store Comcast's Customers' PII

48. Defendants acquire, collect, and store a massive amount of PII on Comcast's customers, former customers, and other personnel.

49. As a condition of obtaining products and/or services from Comcast, Defendants require that customers, former customers, and other personnel entrust Defendants with highly sensitive personal information.

50. By obtaining, collecting, and using Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

51. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members.

52. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendants absent a promise to safeguard that information.

53. Upon information and belief, in the course of collecting PII from customers, including Plaintiffs, Comcast promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

54. Indeed, the Privacy Policy posted on Comcast's website provides that: "[w]e follow industry-standard practices to secure the information we collect to prevent the unauthorized access, use, or disclosure of any personal information we collect and maintain. These security practices

include technical, administrative, and physical safeguards, which may vary, depending on the type and sensitivity of the information.”¹⁰

55. Plaintiffs and the Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

56. Defendants’ negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendants Knew, Or Should Have Known, of the Risk Because Cable and Software companies In Possession Of PII Are Particularly Susceptible To Cyber Attacks

57. Defendants’ data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting cable and software companies that collect and store PII, like Defendants, preceding the date of the breach.

58. Data breaches, including those perpetrated against cable and software companies that store PII in their systems, have become widespread.

59. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals’ personal information being compromised.¹¹

60. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

¹⁰ <https://www.xfinity.com/privacy/policy>

¹¹ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

61. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹²

62. Additionally, as companies became more dependent on computer systems to run their business,¹³ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁴

63. Defendants knew and understood unprotected or exposed PII in the custody of cable and software companies, like Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

64. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendants’ data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

¹² https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

¹³ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁴ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

65. Plaintiffs 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.

66. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

67. The ramifications of Defendants' failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

68. As a cable company and software company in custody of Comcast's customers' PII, Defendants knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiffs and Class Members, and of the foreseeable consequences if their data security system were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifying Information

69. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁵ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

¹⁵ 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁶

70. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.¹⁷ For example, Personal Information can be sold at a price ranging from \$40 to \$200.¹⁸ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁹

71. For example, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁰

¹⁶ *Id.*

¹⁷ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

¹⁸ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

¹⁹ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

²⁰ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>

72. What’s more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

73. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²¹

74. Moreover, the compromise of an individual’s last four digits of a Social Security number is particularly problematic because the last four digits are frequently used by companies to verify identities and access to customer accounts.²²

75. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information

²¹ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>

²² “The numbers were given based on the geographic region, which meant that the first numbers would tell you where someone was from. Meanwhile, the middle two digits are random. But nowadays, a lot of companies ask for the last four digits of the SSN, as they probably think that this is less likely for someone to steal identities.

When someone wants to steal the identity of a person, they will do whatever it takes to do it. So, only having the last four digits is not going to stop them. They can even use those digits to take your identity away.

Because of this, in certain states, there are some limitations regarding how companies can use your SSN. In places like Rhode Island, for instance, you will not be asked for your last four digits.” Frank Gogol, *Why are the Last 4 Digits of an SSN Important?*, Stilt (Nov. 3, 2023), available at <https://www.stilt.com/immigrants/last-4-digits-of-an-ssn/#:~:text=When%20someone%20wants%20to%20steal,to%20take%20your%20identity%20a way.>

compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security numbers, dates of birth, and names.

76. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²³

77. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

78. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁴

79. Plaintiffs 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.

²³ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

²⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

Defendants Fail To Comply With FTC Guidelines

80. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which 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.

81. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.²⁵

82. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting 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.²⁶

83. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

²⁵ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

²⁶ *Id.*

84. 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 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

85. These FTC enforcement actions include actions against cable and software companies, like Defendants.

86. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants’ duty in this regard.

87. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices, and Comcast failed to audit, monitor, or ensure the integrity of its vendor’s data security practices. Defendants’ failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs’ and Class Members’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

88. Upon information and belief, Defendants were at all times fully aware of their obligations to protect the PII of Comcast’s customers, Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants’ conduct was particularly unreasonable given the nature and amount of PII they obtained and stored

and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendants Fail To Comply With Industry Standards

89. As noted above, experts studying cyber security routinely identify cable and software companies in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

90. Several best practices have been identified that a minimum should be implemented by cable and software companies in possession of PII, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

91. Other best cybersecurity practices that are standard in the cable and software industries include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

92. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

93. These foregoing frameworks are existing and applicable industry standards for cable and software companies. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

94. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

Data Breaches Increase Victims' Risk Of Identity Theft

95. The unencrypted PII of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

96. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

97. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

98. Plaintiffs' and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

99. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.²⁷

²⁷ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

100. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

101. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

102. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiffs and the other Class Members.

103. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

104. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

105. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud.

Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

106. Thus, due to the actual and imminent risk of identity theft, Comcast, in its Notice Letter, instructs Plaintiffs and Class Members to “remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports.”²⁸

107. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

108. Plaintiffs’ mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”²⁹

109. Plaintiffs’ mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁰

110. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches

²⁸ Notice Letter.

²⁹ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

³⁰ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

(“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”^[4]

Diminution of Value of PII

111. PII is a valuable property right.³¹ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

112. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.³²

113. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.³³

114. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{34,35}

115. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁶

³¹ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

³² See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

³³ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

³⁴ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

³⁵ <https://datacoup.com/>

³⁶ <https://digi.me/what-is-digime/>

116. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

117. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

118. The fraudulent activity resulting from the Data Breach may not come to light for years.

119. Plaintiffs 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.

120. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to more than thirty-five million individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

121. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

122. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

123. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

124. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

125. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from the Data Breach.

Loss Of Benefit Of The Bargain

126. Furthermore, Defendants’ poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Comcast for products and/or services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PII, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class Members received

products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Comcast.

Plaintiff Brittany Hammond's Experience

127. Plaintiff Brittany Hammond is a former customer at Comcast, which, upon information and belief, contracted with Citrix for services.³⁷

128. As a condition of obtaining products and/or services at Comcast, she was required to provide her PII to Defendants, including her name, date of birth, contact information, Social Security number, and other sensitive information.

129. At the time of the Data Breach—October 16, 2023 through October 19, 2023—Defendants retained Plaintiff's PII in their systems.

130. Plaintiff Hammond is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendants had she known of Defendants' lax data security policies.

131. Plaintiff Brittany Hammond received the Notice Letter, by email, from Comcast, dated December 18, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, username, password information, contact information, date of birth, and/or secret questions and answers.

132. As a result of the Data Breach, and at the direction of Comcast's Notice Letter, which instructs her to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports[,]"³⁸ Plaintiff made reasonable efforts to

³⁷ See Notice Letter.

³⁸ See Notice Letter.

mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

133. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

134. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

135. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

136. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

137. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

138. Plaintiff Brittany Hammond has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Tamia Charles' Experience

139. Plaintiff Tamia Charles is a current customer at Comcast, which, upon information and belief, contracted with Citrix for services.³⁹

140. As a condition of obtaining products and/or services at Comcast, she was required to provide her PII to Defendants, including her name, date of birth, contact information, Social Security number, and other sensitive information.

141. At the time of the Data Breach—October 16, 2023 through October 19, 2023—Defendants retained Plaintiff's PII in their systems.

142. Plaintiff Charles is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendants had she known of Defendants' lax data security policies.

143. Plaintiff Charles received the Notice Letter, by email, from Comcast, dated December 18, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, username, password information, contact information, date of birth, and/or secret questions and answers.

³⁹ See Notice Letter.

144. As a result of the Data Breach, and at the direction of Comcast’s Notice Letter, which instructs her to “remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports[,]”⁴⁰ Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter as well as changing passwords and resecuring her own computer network. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

145. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants’ possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

146. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

⁴⁰ See Notice Letter.

147. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

148. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

149. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

150. Plaintiff Tamia Charles has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

151. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

152. The Class that Plaintiffs seek to represent are defined as follows, subject to amendment as appropriate:

Nationwide Class

All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Comcast in December 2023 (the "Class").

153. Additionally, Plaintiff Hammond seeks to represent the following Subclass, subject to amendment as appropriate:

New Jersey Subclass

All individuals residing in the state of New Jersey whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Comcast in December 2023 (the "New Jersey Subclass").

154. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

155. Plaintiffs reserves the right to amend the definitions of the Class and/or New Jersey Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

156. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. According to the breach report submitted to the Office of the Maine Attorney General, at least 35,000,000 Class Members were impacted in the Data Breach.⁴¹ The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by Comcast sending them breach notification emails).

157. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

- a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;
- b. Whether Defendants had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

⁴¹ See <https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml>

- c. Whether Defendants had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;
- e. Whether and when Defendants actually learned of the Data Breach;
- f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;
- h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;
- k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

158. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

159. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the

Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenges of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

160. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiffs has retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

161. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

162. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure

to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

163. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

164. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

165. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

166. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

167. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants failed to timely notify the Plaintiffs and the class of the Data Breach;
- b. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence

(On Behalf of Plaintiffs and the Class against both Defendants)

168. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 167, as if fully set forth herein, and bring this claim against both Defendants.

169. Defendants require Comcast's customers, including Plaintiffs and Class Members, to submit non-public PII to Defendants in the ordinary course of providing their services.

170. Defendants gathered and stored the PII of Plaintiffs and Class Members as part of their businesses of soliciting their services to their customers and clients, which solicitations and services affect commerce.

171. Plaintiffs and Class Members entrusted Defendants with their PII with the understanding that Defendants would safeguard their information.

172. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

173. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach. Comcast's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

174. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

175. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks adequately protected the PII.

176. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a necessary part of being customers at Comcast.

177. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

178. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

179. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Comcast's former customers' PII they were no longer required to retain pursuant to regulations.

180. Moreover, Defendants had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

181. Defendants had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

182. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Allowing unauthorized access to Class Members' PII;
- d. Failing to detect in a timely manner that Class Members' PII had been compromised;
- e. Failing to remove Comcast's former customers' PII they were no longer required to retain pursuant to regulations,
- f. Failing to audit, monitor, or ensure the integrity of their vendor's data security practices;
- g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure their stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

183. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

184. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

185. Defendants' violations of Section 5 of the FTC Act constitutes negligence.

186. The FTC has pursued 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 as that suffered by Plaintiffs and the Class.

187. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

188. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the cable and software industry.

189. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

190. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendants' systems or transmitted through third party systems.

191. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

192. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

193. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

194. Defendants' duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

195. Defendants have admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

196. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

197. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

198. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii)

statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

199. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

200. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

201. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence Per Se

(On Behalf of Plaintiffs and the Class against both Defendants)

202. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 167, as if fully set forth herein, and bring this claim against both Defendants.

203. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

204. Defendants breached their duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

205. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

206. Plaintiffs and Class Members are within the class of persons that the FTCA intended to protect and the harm to Plaintiffs and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

207. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

208. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that by failing to meet their duties, Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their PII.

209. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied contract
(On Behalf of Plaintiffs and the Class against Defendant Comcast)

210. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 167, as if fully set forth herein, and bring this claim against solely against Defendant Comcast.

211. Plaintiffs and Class Members were required to provide their PII to Comcast as a condition of receiving products and/or services from Comcast.

212. Plaintiffs and the Class entrusted their PII to Comcast. In so doing, Plaintiffs and the Class entered into implied contracts with Comcast by which Comcast agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

213. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Comcast's data security practices complied with relevant laws and regulations and were consistent with industry standards.

214. Implicit in the agreement between Plaintiffs and Class Members and the Comcast to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

215. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Comcast, on the other, is demonstrated by their conduct and course of dealing.

216. Comcast solicited, offered, and invited Plaintiffs and Class Members to provide their PII as part of Comcast's regular business practices. Plaintiffs and Class Members accepted Comcast's offers and provided their PII to Comcast.

217. In accepting the PII of Plaintiffs and Class Members, Comcast understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

218. On information and belief, at all relevant times Comcast promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

219. On information and belief, Comcast further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

220. Plaintiffs and Class Members paid money to Comcast with the reasonable belief and expectation that Comcast would use part of its earnings to obtain adequate data security. Comcast failed to do so.

221. Plaintiffs and Class Members would not have entrusted their PII to Comcast in the absence of the implied contract between them and Comcast to keep their information reasonably secure.

222. Plaintiffs and Class Members would not have entrusted their PII to Comcast in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

223. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Comcast.

224. Comcast breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

225. As a direct and proximate result of Comcast's breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

226. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

227. Plaintiffs and Class Members are also entitled to injunctive relief requiring Comcast to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and the Class against Defendant Citrix)

228. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 167, as if fully set forth herein, and bring this claim against solely against Defendant Citrix..

229. Upon information and belief, Citrix entered into virtually identical contracts with its clients, including Comcast, to provide software products and/or services, which included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be entrusted to it.

230. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their PII that Citrix agreed to receive and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

231. Citrix knew that if they were to breach these contracts with its clients, Plaintiffs and the Class would be harmed.

232. Citrix breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Citrix failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

233. As foreseen, Plaintiffs and the Class were harmed by Citrix's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their PII.

234. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class against both Defendants)

235. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 167, as if fully set forth herein, and bring this claim against both Defendants.

236. Plaintiffs bring this Count in the alternative to the breach of implied contract count above.

237. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they paid money to Comcast for products and/or services as well as provided Defendants with their PII. In exchange, Plaintiffs and Class Members should have received the services that were the subject of the transaction and had their PII protected with adequate data security.

238. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the PII entrusted to it.

Defendants profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' PII for business purposes.

239. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

240. Defendants acquired the PII through inequitable record retention as they failed to investigate and/or disclose the inadequate data security practices previously alleged.

241. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendants or obtained products and/or services at Comcast.

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

243. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

244. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further

unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

245. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

246. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
Violation of the Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of Plaintiff and the Class against Defendant Citrix)

247. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 167, as if fully set forth herein, and bring this claim against solely against Defendant Citrix.

248. Citrix engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Comcast obtained Plaintiffs' and Class members' PII through advertising, soliciting, providing, offering, and/or distributing goods and services to its clients, including Comcast, and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

249. As alleged herein this Complaint, Citrix engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

- a. failing to implement adequate data security practices to safeguard PII;

- b. failing to make only authorized disclosures of Citrix's clients' current and former customers' PII;
- c. failing to disclose that their data security practices were inadequate to safeguard PII from theft; and
- d. failing to timely and accurately disclose the Data Breach to Plaintiffs and Class members.

250. Citrix's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Citrix engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Citrix's clients' current and former customers.

251. In committing the acts alleged above, Citrix engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Citrix's clients' current and former customers that they did not follow industry best practices for the collection, use, and storage of PII.

252. As a direct and proximate result of Citrix's conduct, Plaintiffs and Class members have been harmed and have suffered damages including, but not limited to:

253. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs and Class members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

254. Also, as a direct result of Citrix's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and Class members are entitled to injunctive relief, including, but not limited to:

- a. Ordering that Citrix implement measures that ensure that the PII of Citrix’s clients’ current and former customers is appropriately encrypted and safeguarded when stored on Citrix’s network or systems;
- b. Ordering that Citrix purge, delete, and destroy in a reasonable secure manner PII not necessary for their provision of services;
- c. Ordering that Citrix routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- d. Ordering Citrix to meaningfully educate its clients’ current and former customers about the threats they face as a result of the accessibility of their PII to third parties, as well as the steps its clients’ current and former customers must take to protect themselves.

COUNT VII

**Violation Of The New Jersey Consumer Fraud Act
NJ STAT. ANN. § 56:8-1 *et seq.***

(On Behalf of Plaintiff Hammond and the New Jersey Subclass against both Defendants)

255. Plaintiff Hammond (“Plaintiff” for the purposes of this count) re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 167, as if fully set forth herein, and brings this claim against both Defendants.

256. The New Jersey Consumer Fraud Act (New Jersey CFA) makes unlawful “[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with

the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby.” N.J. STAT. ANN. § 56:8-2. 134.

257. By the acts and conduct alleged herein, Defendants committed unfair or deceptive acts and practices by:

- a. failing to maintain adequate computer systems and data security practices to safeguard Plaintiff’s and New Jersey Subclass Members’ PII;
- b. failing to disclose that their computer systems and data security practices were inadequate to safeguard Plaintiff’s and New Jersey Subclass Members’ PII from theft;
- c. continuing to gather and store Plaintiff’s and New Jersey Subclass Members’ PII after Defendants knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach;
- d. making and using false promises about the privacy and security of PII of Plaintiff and New Jersey Subclass Members, and;
- e. continuing to gather and store Plaintiff’s and New Jersey Subclass members’ PII after Defendants knew or should have known of the Data Breach and before Defendants allegedly remediated the data security incident.

258. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act and the New Jersey CFA.

259. The foregoing deceptive acts and practices were directed at New Jersey consumers/purchasers.

260. Defendants, Plaintiff, and New Jersey Subclass Members are “persons” within the meaning of N.J. STAT. ANN. § 56:8-1(d).

261. Defendants engaged in “sales” of “merchandise” within the meaning of N.J. STAT. ANN. § 56:8-1(c), (d).

262. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the products and services provided, specifically as to the safety and security of PII, to induce consumers to purchase the same.

263. Defendants’ unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiff and members of the New Jersey Subclass, would attach importance to in making their purchasing decisions or conducting themselves regarding the purchase of products and/or services from Comcast.

264. Plaintiff and New Jersey Subclass Members are New Jersey consumers who made payments to Comcast for the furnishing of products and/or services that were primarily for personal, family, or household purposes. Defendants engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of products and/or services to consumers, including Plaintiff and New Jersey Subclass Members.

265. Defendants’ acts, practices, and omissions were done in the course of Defendants’ businesses of marketing, offering to sell, and furnishing products and/or services to consumers in the State of New Jersey.

266. As a direct and proximate result of Defendants’ unlawful conduct, Plaintiff and the New Jersey Subclass Members have suffered an ascertainable loss, damages, and are at present risk of further harm.

267. The injury and harm that Plaintiff and New Jersey Subclass Members suffered (as alleged above) was the direct and proximate result of Defendants’ unlawful conduct.

268. Plaintiff and New Jersey Subclass Members have suffered injury and are entitled to damages in an amount to be proven at trial.

269. On behalf of themselves and other members of the New Jersey Subclass, Plaintiff is entitled to recover legal and/or equitable relief, including an order enjoining Defendants' unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J. STAT. ANN. § 56:8-19, and any other just and appropriate relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

- A. For an Order certifying the Class and New Jersey Subclass, and appointing Plaintiffs and their Counsel to represent the Classes;
- B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendants to delete, destroy, and purge the personal identifying

- information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
- iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;
 - v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
 - vi. prohibiting Defendants from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;
 - vii. requiring Defendants 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 Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
 - viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - ix. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;
 - x. requiring Defendants to segment data by, among other things, creating firewalls and controls so that if one area of Defendants' network is compromised, hackers

- cannot gain access to portions of Defendants' systems;
- xi. requiring Defendants to conduct regular database scanning and securing checks;
 - xii. requiring Defendants 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 Plaintiffs and Class Members;
 - xiii. requiring Defendants 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;
 - xiv. requiring Defendants 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 Defendants' policies, programs, and systems for protecting personal identifying information;
 - xv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
 - xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and
 - xviii. 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 Defendants' 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, nominal, statutory, consequential, and punitive 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

Plaintiffs hereby demands a trial by jury on all claims so triable.

Dated: December 26, 2023

Respectfully Submitted,

By: /s/ Jonathan B. Cohen

Jonathan B. Cohen

FL. Bar No. 27620

**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, LLC**

3833 Central Ave.

St. Petersburg, FL 33713

Telephone: (865) 247-0080

jcohen@milberg.com

*Attorneys for Plaintiffs and
Proposed Class Counsel*

