UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JACLYN REMARK and NOAH BIRKETT, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, v. COMCAST CABLE COMMUNICATIONS, LLC d/b/a XFINITY and CITRIX SYSTEMS, INC., Defendants.	Case No. 2:24-cv-00793 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Upon personal knowledge as to their own acts, and based upon their investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiffs Jaclyn Remark and Noah Birkett (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, allege as follows:

SUMMARY OF THE ACTION

1. Plaintiffs bring this class action against Comcast Cable Communications, LLC d/b/a Xfinity ("Comcast") and Citrix Systems, Inc. ("Citrix") (collectively, "Defendants") for their failure to adequately secure and safeguard Plaintiffs' and nearly 36 million other individuals' personally identifying information ("PII"), including their names, contact information, dates of birth, portions of Social Security numbers, account usernames and hashed passwords, and security question prompts and answers, among other potentially sensitive, private, and confidential data.

2. Comcast is one of the largest telecommunications companies, and provides internet services and products, cable television, a mobile 5G network, and landline telephone services and products to individuals and businesses across the United States. To obtain Xfinity's services and

products, customers are required to entrust Comcast with their PII and other private information, which Comcast uses to perform its regular business activities.

3. Thus, Comcast maintains extensive files, servers, and networks containing its customers' PII, and owes these individuals an affirmative duty to adequately protect and safeguard this private information against theft, misuse, and unauthorized access and disclosure. Despite such duties created by statute, regulation, and common law, at all relevant times, Comcast utilized deficient data security practices—including by relying on Citrix's flawed software applications—thereby allowing tens of millions of persons' sensitive and private data to fall into the hands of strangers and criminals.

4. Citrix is a networking, cloud computing, and virtualization technology company. Due to a critical security hole in Citrix's software called CVE-2023-4966 ("Citrix Bleed"), two core Citrix software products Netscaler Gateway and Netscaler ADC were extremely vulnerable to cyberattacks. Hackers had been exploiting this flaw, which carries a severity rating of 9.4 out of a possible 10, since at least August 2023.

5. On October 10, 2023, Citrix alerted its clients—including Comcast—of Citrix Bleed and provided them with an accompanying software patch to fix the security vulnerability. Comcast failed to immediately heed this dire warning and Citrix's guidance, and waited at least six to nine days to act. By then, it was already too late.

6. Between October 16, 2023 and October 19, 2023, Comcast lost control over the highly sensitive and confidential PII of Plaintiffs and the Class Members (defined herein) by failing to timely mitigate the Citrix Bleed in a massive and preventable data breach committed by cybercriminals (the "Data Breach"). To perpetrate the Data Breach, hackers exploited the

unpatched Citrix Bleed security flaw to access Comcast's internal systems during this four-day window and exfiltrate massive amounts of valuable PII.

7. The Data Breach was directly and proximately caused by Comcast's and Citrix's collective failure to implement basic, reasonable, and industry-standard data security practices necessary to protect their systems, software, and networks from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive PII of at least 35,879,455 individuals is now in the hands of cybercriminals, who target this sensitive data for its value to identity thieves. Plaintiffs and Class Members now must contend with the fallout from their PII and other private information being in the hands of unauthorized actors. They are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes. Moreover, Plaintiffs and Class Members have lost the inherent value of their private data.

8. By aggregating information obtained from the Data Breach with other sources or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names and other personal information to open new financial accounts, incur credit charges, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it. Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

9. Despite the Data Breach being first detected on October 25, 2023, Comcast only began notifying impacted persons ***nearly two months later***, on December 18, 2023, exacerbating the damages and risks to Class Members, and in violation of various state data breach notification statutes. The data breach notice letters issued by Comcast also obscure the true nature of the cyberattack and threat it posed—failing to adequately inform Plaintiffs and Class Members how many people were impacted, how the cybercriminals accessed Comcast's systems and the root cause of the Data Breach, whether all of the exfiltrated information was encrypted or anonymized, why it took so long for Comcast to determine PII had been compromised and then notify victims, whether Comcast or law enforcement have apprehended or even identified the hackers who accessed Comcast's systems, or what specific remedial steps Comcast has taken to safeguard PII within its systems and networks (or otherwise purge unnecessary information) and to prevent further cyberattacks going forward. Without these critical details, Plaintiffs and Class Members cannot meaningfully mitigate the resulting effects of the Comcast and Citrix Data Breach.

10. Plaintiffs Remark and Birkett are both current Xfinity customers and subscribers and are victims of the Data Breach.

11. Plaintiffs, on behalf of themselves and all others similarly situated, herein allege claims for negligence, negligence *per se*, breach of implied contract, breach of third-party beneficiary contract, unjust enrichment or quasi-contract, and declaratory and injunctive relief. Plaintiffs, on behalf of themselves and the Class, seek: (i) actual damages, economic damages, statutory damages, and nominal damages; (ii) punitive damages; (iii) fees and costs of litigation; (iv) injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII in Defendants' custody, care, and control in order to prevent incidents like the Data Breach from recurring in the future and for Comcast and Citrix to provide long-term identity theft protective

services and credit monitoring to Plaintiffs and Class Members; and (v) such other relief as the Court deems just and proper.

PARTIES

A. Plaintiffs

12. Plaintiff Jaclyn Remark is a resident and citizen of the Commonwealth of Pennsylvania. Since Plaintiff Remark is, and has been a customer of Comcast, Plaintiff Remark's PII was maintained within Comcast's networks and servers.

13. Plaintiff Noah Birkett is a resident and citizen of the State of Louisiana. Since Plaintiff Birkett is, and has been a customer of Comcast, Plaintiff Birkett's PII was maintained within Comcast's networks and servers.

14. Had Plaintiffs known that Comcast would not adequately protect their and Class Members' PII, they would not have paid for and received services from Comcast or any of its affiliates and would not have provided their PII to Comcast or any of its affiliates, or would have paid considerably less for such Comcast services. This expectation and mutual understanding extended to software providers, like Citrix, that Comcast uses for business purposes.

15. Plaintiffs and Class Members are, or were, customers of Comcast. To obtain products and/or services, consumers like Plaintiffs and Class Members are required to directly provide Comcast with sensitive PII. In the regular course of its business, Comcast collects, stores, and maintains the PII it receives from consumers who utilize Comcast's products and or/services.

16. By creating and maintaining massive repositories of PII, Comcast has provided a particularly lucrative target for data thieves looking to obtain, misuse, or sell such data.

17. In response and as a result of the Data Breach, Plaintiffs and Class Members have spent significant time and effort researching the Data Breach and reviewing and monitoring their accounts for fraudulent activity.

18. Plaintiff and Class Members suffered damages as a result of the failures of Defendants to adequately protect the sensitive information entrusted to them, including, without limitation, experiencing fraud or attempted fraud, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiffs and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

19. As a result of the Data Breach, Plaintiffs and Class Members have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending and is not speculative given the highly sensitive nature of the PII compromised by the Data Breach.

B. Defendants

20. Defendant Comcast Cable Communications, LLC d/b/a Xfinity is a telecommunications business organized and existing under the laws of the State of Delaware, with its principal place of business located at Comcast Center, 1701 John F. Kennedy Blvd., Philadelphia, Pennsylvania 19103. Comcast is registered to do business with the Pennsylvania Department of State.

21. Defendant Citrix Systems, Inc. is a cloud solutions computing company organized and existing under the laws of the State of Delaware, with its principal place of business located

at 851 Cypress Creek Rd., Fort Lauderdale, Florida 33309. Citrix is registered to do business with the Pennsylvania Department of State.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because at least one member of the putative Class, as defined below, is a citizen of a state other than that of Defendants, there are more than 100 putative Class Members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

23. This Court has general personal jurisdiction over Defendants because each are registered to do business with the Pennsylvania Department of State.

24. This Court has general personal jurisdiction over Defendant Comcast because it maintains its principal place of business in Philadelphia, Pennsylvania and regularly conducts business in Pennsylvania, and has sufficient minimum contacts in Pennsylvania, such as to not offend traditional notions of fair play and substantial justice.

25. This Court has specific personal jurisdiction over Defendant Citrix because Citrix has committed acts within the Eastern District of Pennsylvania giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Citrix would not offend traditional notions of fair play and substantial justice. Citrix has engaged in continuous, systematic, and substantial activities within Pennsylvania, including substantial marketing and sales of services and products—including Citrix's NetScaler software used by Comcast in connection with the Data Breach—within Pennsylvania.

26. Venue in this District is proper under 28 U.S.C. § 1391(b) because Defendant Comcast resides in this District and a substantial part of the conduct giving rise to Plaintiffs' claims

occurred in this District, including Comcast collecting or storing the PII of Plaintiffs and the putative Class Members.

FACTUAL BACKGROUND

A. Comcast and Citrix Collect, Store, and Maintain Huge Amounts of Personally Identifiable Information

27. Comcast is an American telecommunications business and subsidiary of Comcast Corporation. Xfinity is the largest provider of home internet and cable services in the United States. In connection with providing its entertainment and services, Xfinity requires consumers to provide personal and private information, including, but not limited, to names, Social Security numbers, dates of birth, financial information, and security question answers. As a result, when consumers contract for Xfinity's services, their highly sensitive PII is stored on Comcast's networks, servers, and systems.

28. Citrix provides cloud computing services to over 16 million users and thousands of organizations. Its diverse range of services include, but are not limited to, server technologies, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing technologies. With a diverse client portfolio, Citrix caters to thousands of companies globally. Its services extend across various sectors such as education, energy and utility, financial services, government and public sector, healthcare, insurance, manufacturing, childcare, professional services, retail, technology, telecommunications, and transportation. Comcast is among is customers and clients. Through contracts with these clients, including Comcast, Citrix accumulates and stores the PII and other private information of tens of millions of individuals in its databases, networks, servers, and systems.

29. Comcast understands that data cybersecurity is critical. It tells customers that "Your privacy matters to us," it is "committed to protecting your privacy," and that it is "always working

to keep your personal information secure."[1] Comcast goes on to explain that "We believe strong cybersecurity is essential to privacy," and claims to employ "multiple layers of security that automatically detect and block hundreds of thousands of cyber events every second and a team of security experts who work to protect you 24 hours a day, 365 days a year."[2] Comcast's separate Privacy Policy acknowledges that "We know you care about your privacy and the protection of your personal information."[3] It claims to follow "industry-standard practices to secure the information" it collects from its customers to prevent unauthorized access, use, or disclosure thereof.[4] Finally, Comcast assures customers that it "takes the responsibility of safeguarding your personal information seriously."[5]

30. In a similar vein, Citrix boasts that "[f]or almost 30 years, our customers have trusted our ability to handle their data with care and respect."[6] Like Comcast, Citrix also claims to "respect your concerns about privacy."[7] Under the heading "How We Protect Personal Information," Citrix's Privacy Policy asserts that it "maintain[s] administrative, technical and physical safeguards, consistent with legal requirements where the personal information was obtained, designed to protect against unlawful or unauthorized … use or disclosure of, or access

---

[1] *See* https://www.xfinity.com/privacy (last visited Feb. 20, 2024).

[2] *Id.*

[3] Our Privacy Policy, Comcast (Jan. 1, 2024), *available at* https://www.xfinity.com/privacy/policy.

[4] *See id.*

[5] *Id.*

[6] Privacy and Certifications, Citrix Trust Center, https://www.citrix.com/about/trust-center/privacy-compliance/ (last visited Feb. 20, 2024).

[7] Privacy Policy, Cloud Software Group (Sept. 29, 2023), *available at* https://www.cloud.com/privacy-policy.

to, the personal information provided to us."[8] In its Data Processing Addendum, Citrix promises to "implement and maintain appropriate administrative, technical, and organizational practices designed to protect Personal Data against any misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data."[9]

31. Despite these strong proclaimed proactive policies and approaches to data security and privacy for their customers and clients, Comcast and Citrix failed to adequately secure, encrypt, and safeguard their systems, networks, servers, and software from a foreseeable and preventable cyberattack. This conduct proximately resulted in the Data Breach and significant harm to Plaintiffs and the Class.

B. Hackers Exploited Known Vulnerabilities in Citrix's Applications and Exposed Valuable PII and Other Private Information in the Data Breach

32. Comcast and Citrix collected and maintained Plaintiffs' and the Class's PII and other private information in their computer systems, servers, software, and networks. In accepting, collecting, and maintaining Plaintiffs' and the Class's PII, Defendants agreed that they would protect and safeguard that data by complying with state and federal laws and regulations and applicable industry standards. Comcast and Citrix were in possession of Plaintiffs' and the Class's PII and other private information before, during, and after the Data Breach.

33. On October 10, 2023, Citrix notified its clients and customers, including Comcast, of a network vulnerability in its Netscaler Gateway and Netscaler ADC software products. The same day, Citrix issued an accompanying software patch to Comcast to fix the security vulnerability. Hackers had already been exploiting this severe flaw, Citrix Bleed, since at least

[8] *Id.*

[9] Data Processing Addendum, Cloud Software Group (Oct. 31, 2023), *available at* https://www.cloud.com/content/dam/cloud/documents/legal/cloud-software-group-data-processing-addendum-oct-2023.pdf.

August 2023. Citrix Bleed has been connected to several other cyberattacks, including against Boeing and Toyota. According to cybersecurity experts, Citrix Bleed is "very easy to exploit," and allows threat actors to hijack legitimate user sessions by bypassing password requirements and multifactor authentication.[10] Despite this knowledge, Comcast did not heed Citrix's dire warning. Comcast did not patch its network until October 16, 2023 at the earliest, and October 19, 2023 at the latest—an unexplained and inexcusable lapse of six to nine days.

34. According to Comcast, "prior to mitigation" of Citrix Bleed, "there was unauthorized access to some of our internal systems that we concluded was a result of this vulnerability" between October 16, 2023 and October 19, 2023.[11] Comcast claims to have first learned of this "suspicious activity" on its networks and servers days later on October 25, 2023, "during a routine cybersecurity exercise."[12] It took three weeks more weeks, until November 16, 2023, for Comcast to merely conclude that its customers' PII and other private information was "likely acquired" in the cyberattack and then almost another three weeks, until December 6, 2023, for Comcast to actually determine which types of customer information had been compromised.[13] Beginning on December 18, 2023—two months after the Data Breach occurred—Comcast then publicly disclosed the Data Breach and reported it to various governmental agencies and attorneys general. It has since issued additional Data Breach notices to affected persons.

---

[10] Pieter Arntz, *Citrix Bleed Widely Exploited, Warn Government Agencies*, MALWAREBYTES (Nov. 24, 2023), https://www.malwarebytes.com/blog/news/2023/11/citrix-bleed-widely-exploitated-warn-government-agencies.

[11] *See* Exhibit 1, Notice of Data Security Incident, Comcast.

[12] Notice to Customers of Data Security Incident, Comcast (Dec. 18, 2023), https://www.businesswire.com/news/home/20231218979935/en/Notice-To-Customers-of-Data-Security-Incident.

[13] *See id.*

35. Despite Defendants' duties and commitments to safeguard sensitive and private information, Comcast and Citrix failed to follow industry-standard practices in securing Plaintiffs' and the Class Members' PII and other private information, as evidenced by the Data Breach.

36. In responding to the Citrix Bleed security flaw, Comcast contends that it "promptly patched and mitigated the Citrix vulnerability,"[14] but offers no explanation for why it failed to immediately act on October 10, 2023 when Citrix issued the software patch. Nor does Citrix explain why the Citrix Bleed issue went wholly unsolved for several months before it issued the patch in October 2023.

37. In response to the Data Breach, Comcast required its customers to reset passwords and encouraged all users to enable two-factor or multi-factor authentication to secure their Xfinity accounts. Comcast has not disclosed what additional cybersecurity measures, if any, it has adopted in the wake of the Data Breach to prevent a similar event for occurring in the future. Additionally, although Comcast indicated that it notified federal law enforcement of the Data Breach, the Data Breach letters do not state whether the criminals responsible for the Data Breach have been identified or apprehended.

38. As of December 18, 2023, Comcast reported to the Maine Attorney General's Office that the total number of persons affected by the Data Breach was 35,879,455.

39. Comcast's Data Breach Letters reveal that a treasure trove of information from Plaintiffs and the Class was stolen in the cyberattack, including, at least: names, contact information, dates of birth, portions of Social Security numbers, account usernames and hashed passwords, and security question prompts and answers.

[14] *Id.*

40. Through its Data Breach notice letters to Plaintiffs and Class Members, Comcast also recognized the actual imminent harm and injury that flowed from the Data Breach by encouraging them to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[15] The fraudulent activity resulting from the Data Breach may not come to light for years. Yet, Comcast's December 2023 Data Breach letters did not offer any compensation or complimentary third-party credit monitoring or identity theft protection services to affected persons. Thus, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII and other private information remain very high.

C. Telecommunications and Cloud Computing Companies Are Increasingly Susceptible to Data Breaches, Giving Comcast and Citrix Ample Notice That They Were Likely Cyberattack Targets

41. Large telecommunications and cloud computing companies like Defendants are well-aware of the numerous largescale data breaches that have occurred throughout the United States and internationally, and of their responsibility for safeguarding the PII and other private customer information in their possession. Such breaches have become frequent and widespread. Thus, at all relevant times, Defendants knew, or should have known, that the PII and other private information they were entrusted with was a target for malicious actors. In particular, Defendants knew this given the unique type and the significant volume of data on their networks, software, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm. As custodian of Plaintiffs' and Class Members' PII, Comcast and Citrix knew or should have known the importance of protecting their PII, and of the foreseeable consequences and harms to such persons if any data breach occurred.

[15] *See* Exhibit 1.

42. In 2023 alone, 3,205 data breaches occurred, resulting in over 353 million individuals' sensitive records in the United States being exposed.[16] The 3,205 reported data breaches are a sharp increase from 2022, when 1,802 data breaches occurred.[17] With the surging number of such attacks, Comcast and Citrix should have known that they were at a high risk of a cyberattack and should have taken additional and stronger precautions and preemptive measures.

43. Additionally, in light of recent high profile data breaches at other industry leading companies, including MOVEIt (90 million records, June 2023), LastPass/GoTo Technologies (30 million records, August 2022), Neopets (69 million records, July 2022), WhatsApp (500 million records, November 2022), Twitter (5.4 million records, July 2022), Cash App (8.2 million users, April 2022), LinkedIn (700 million records, April 2021), Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estée Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), Advanced Info Service (8.3 billion records, May 2020), and others, Defendants knew or should have known that the PII that they collected and maintained would also be specifically targeted by cybercriminals.

44. Furthermore, Citrix's knowledge and notice is amplified by a prior March 2019 data security incident wherein hackers gained access to its networks and exploited vulnerabilities therein to steal valuable PII and other information relating to over 20,000 of its current and former employees, among other persons. As part of a settlement of resulting class action litigation in *In re Citrix Data Breach Litig.*, No. 19-cv-61350-RKA (S.D. Fla.), Citrix agreed to enhance its data

[16] Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2023, STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited Feb. 20, 2024).

[17] *See id.*

security policies, monitoring, and cybersecurity training, among other remedial measures to prevent future data breaches.

D. Comcast and Citrix Breached Their Duties to Plaintiffs and the Class, and Failed to Comply with Regulatory Requirements and Industry Best Practices

45. Because Defendants were entrusted with PII and other private information at all times herein relevant, Comcast and Citrix owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII in their care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems. Defendants also owed a duty to safeguard PII and other private information because they were on notice that they were handling highly valuable data and knew there was a significant risk it would be targeted by cybercriminals. Furthermore, Comcast and Citrix knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

46. Security standards commonly accepted among businesses like Comcast and Citrix that store PII and other private information include, without limitation:

i. Maintaining a secure firewall configuration;

ii. Monitoring for suspicious or irregular traffic to servers or networks;

iii. Monitoring for suspicious credentials used to access servers or networks;

iv. Monitoring for suspicious or irregular activity by known users;

v. Monitoring for suspicious or unknown users;

vi. Monitoring for suspicious or irregular server requests;

vii. Monitoring for server requests for PII or other private information;

viii. Monitoring for server requests from VPNs; and

ix. Monitoring for server requests for Tor exit nodes.

47. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[18] and protection of PII which includes basic security standards applicable to all types of businesses.[19]

48. The FTC recommends that businesses:

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

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

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

iv. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

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

---

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

[19] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

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

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

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

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

49. As described further below, Defendants owed a duty to safeguard PII and other private information under statute, including the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act"), to ensure that all information they received, maintained, and stored was secure. The FTC Act was enacted to protect Plaintiffs and the Class Members from the type of conduct in which Defendants engaged, and the resulting harms Defendants proximately caused Plaintiffs and the Class Members.

50. Under the FTC Act, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiffs and Class Members.

51. Defendants breached their duty to exercise reasonable care in protecting Plaintiffs' and Class Members' PII by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII within their systems and networks, failing to monitor their systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII no longer necessary for their provision of telecommunications and software services to their clients and customers, failing to timely act upon data security warnings and alerts in a timely manner, allowing unmonitored and unrestricted access to unsecured PII, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Members' confidential and private information. Additionally, Defendants breached their duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Comcast further breached its duties to Plaintiffs and Class Members by sharing PII and other private customer information with other entities such as Citrix that maintained sub-standard data security systems, as well as by not auditing, monitoring, or verifying the integrity of its information technology vendors and affiliates. Through these actions, Comcast and Citrix also violated their duties under the FTC Act.

52. Defendants failed to prevent the Data Breach. Had Comcast and Citrix properly maintained and adequately protected their software, systems, servers, and networks, the Data Breach would not have occurred.

53. Additionally, the law imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of PII to Plaintiffs and Class Members so that they can take

appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Comcast and Citrix further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendants actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members.

54. At all relevant times, Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

E. The Experiences of Plaintiffs Remark and Birkett

55. In the course of using Comcast's services, Plaintiffs Remark and Birkett were required to provide their PII and other private information to Defendants, including their names, Social Security numbers, dates of birth, contact information, and financial information. Plaintiffs Remark and Birkett are Data Breach victims. Their PII and other private information was among the data accessed by unauthorized third parties in the Data Breach.

56. Following the Data Breach, Remark and Birkett have already experienced suspicious activity on their various accounts and instances of fraud.

57. In January 2024, Remark was alerted of an unauthorized person using her private information. This criminal opened two credit cards in her name, and the incident caused her other credit cards to be frozen. The criminal also gained access to Remark's Google Drive account, where additional private information, including pictures of her family, was hosted. Remark filed a police report thereafter. Remark believes the January 2024 fraud, which cost Remark around $200 to remediate, was caused by the Data Breach. Later in January 2024, Remark was alerted to additional suspicious activity on her accounts by criminals located in Singapore. Remark spent several hours to address and resolve both incidents. Following the Data Breach, Remark has also

experienced several unsuccessful attempts of unauthorized individuals attempt to access her Venmo, Facebook, and Amazon accounts.

58. In late January 2024, Birkett was alerted of an unauthorized person using his private information to secure a loan through Cash America in his name. Birkett was able to thwart the loan, but the incident caused Birkett to place a security freeze on his credit reports through the three major credit reporting bureaus.

59. Additionally, in the months following the Data Breach, Birkett has experienced a significant uptick in phishing emails, texts, and phone calls, which he believes may have resulted from the Data Breach. Now, Birkett is bombarded with constant spam phone calls, test, and emails, man of which attempt to lure Birkett dubious financial activities or transactions. In the months following the Data Breach, Remark has also experienced an uptick in phishing texts and spam telephone calls, which she believes resulted from the Data Breach.

60. As a proximate result of the Data Breach, Birkett and Remark have already spent many hours each week dealing with its consequences, including time self-monitoring their accounts to monitor for potentially suspicious and fraudulent activity. This time has been lost forever and cannot be recaptured. Additionally, Birkett and Remark will spend time protecting themselves from identity theft resulting from the Data Breach for the foreseeable future and beyond.

61. Remark has and is experiencing extreme stress, fear, must remain on high alert for future data security incidents, and feels physically ill and violated as a consequence of her private information being compromised in the Data Breach. She describes the experience as a "nightmare." Likewise, Birkett has and is experiencing anxiety, stress, and extreme frustration because his sensitive information was stolen in the Data Breach and in dealing with resulting

increase in spam phone calls, emails, and texts. This goes beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

62. Remark and Birkett suffered actual injuries in the form of damages to and diminution in the value of their PII—a form of intangible property was entrusted to Comcast and Citrix, which was compromised in and as a proximate result of the Data Breach.

63. Remark and Birkett have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from their PII and other private information being obtained by unauthorized third parties and possibly cybercriminals.

64. Remark and Birkett have a continuing interest in ensuring that their PII and other private information, which remains within Defendants' possession and control, is protected and safeguarded against future data breaches and other cybersecurity risks.

65. Defendants deprived Remark and Birkett of the earliest opportunity to guard themselves against the Data Breach's harmful effects by failing to promptly notify them about it. Instead, ***Comcast waited almost two months***.

F. Plaintiffs Remark and Birkett and the Class Suffered Actual and Impending Injuries Resulting From the Data Breach

66. As a proximate result of Defendants' completely unreasonable security practices, identity thieves now possess the sensitive PII of Remark, Birkett, and the Class. Private information is valuable property. Once stolen, PII can be used in a number of different malicious ways. That information is extraordinarily valuable on the black market and incurs direct costs to Remark, Birkett, and the Class. Indeed, the link between a data breach and risk of identity theft is simple, well-established, and strong. On the dark web—an underground Internet black market—

criminals openly buy and sell stolen PII to create "identity kits" worth up to $2,000 each that can be used to create fake IDs, gain access to bank accounts, social media accounts, and credit cards, file false insurance claims or tax returns, or rack up other kinds of expenses.[20] And, "[t]he damage to affected [persons] may never be undone."[21]

67. Unlike the simple credit-card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more pernicious than credit card fraud. Criminals' ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity. The U.S. Department of Justice has reported that in 2021, identity theft victims spent on average about four hours to resolve problems stemming therefrom and that the average financial loss experienced by an identity theft victim was $1,160 per person.[22] Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.[23]

68. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult to change. The

---

[20] Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity* (Jun. 7, 2021), FORBES, https://www.forbes.com/sites/forbestechcouncil/2021/06/07/ increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh= ca928c05650d.

[21] *Id.*

[22] Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF STATISTICS (Oct. 2023), *available at* https://bjs.ojp.gov/document/vit21.pdf.

[23] *Id.*

Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> Identity theft is one of the fastest growing crimes in America. 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, when 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.[24]

69. Even when an injured person successfully goes through the cumbersome and time-consuming process of changing their Social Security number following identity theft, the Social Security Administration cautions individuals to "[k]eep in mind that a new number probably won't solve all your problems" and "can't guarantee you a fresh start."[25]

70. Class Members' credit profiles can be destroyed before they even realize what happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

---

[24] Identity Theft and Your Social Security Number, U.S. SOCIAL SECURITY ADMINISTRATION (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.

[25] *Id.*

71. Additionally, Class Members will spend significant amounts of time on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach and in navigating its effects.

72. Comcast's data breach notices provide no compensation or relief whatsoever to affected persons for its wrongful conduct and actions described herein. After a severe cybersecurity incident such as the one perpetrated here, the breached company typically offers years-long free identity protection services and credit monitoring to affected individuals.

CLASS ACTION ALLEGATIONS

73. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All persons whose PII or other private information was compromised in the Data Breach announced by Comcast in December 2023, including all persons who were sent a notice of the Data Breach (and each person a "Class Member").

74. Excluded from the Nationwide Class are governmental entities, Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

75. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

76. *Numerosity Under Rule 23(a)(1)*. The Nationwide Class is so numerous that the individual joinder of all members is impracticable, and the disposition of the claims of all members of the Nationwide Class in a single action will provide substantial benefits to the parties and the

Court. Although the precise number of members of the Nationwide Class is unknown to Plaintiffs at this time, on information and belief, the proposed Nationwide Class contains at least 35,879,455 individuals, as reported to the Maine Attorney General's Office on December 18, 2023. Discovery will reveal, through Comcast's records, the number of members of the Nationwide Class.

77. *Commonality Under Rule 23(a)(2)*. Common legal and factual questions exist that predominate over any questions affecting only individual members of the Nationwide Class. These common questions, which do not vary among members of the Nationwide Class and which may be determined without reference to any Nationwide Class Member's individual circumstances, include, but are not limited to:

a. Whether Defendants knew or should have known that their computer systems, software, servers, and networks were vulnerable to unauthorized third-party access or a cyberattack;

b. Whether Defendants failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that their computer systems, software, servers, and networks were protected;

c. Whether Defendants failed to take reasonably available steps to prevent and stop the Data Breach from occurring;

d. Whether Defendants acted negligently in failing to "patch" the vulnerability when they first received notice thereof or adequately addressed and fixed the vulnerabilities that caused the Data Breach;

e. Whether Defendants owed a legal duty to Plaintiffs and Class Members to protect their PII and other private information;

f. Whether Defendants breached any duty to protect the PII of Plaintiffs and Class Members by failing to exercise due care in protecting their sensitive and private information;

g. Whether Defendants provided timely, accurate, and sufficient notice of the Data Breach to Plaintiffs and the Class Members;

h. Whether Plaintiffs and Class Members have been damaged by the wrongs alleged and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

i. Whether Plaintiffs and Class Members are entitled to injunctive or equitable relief, including restitution.

78. *Typicality Under Rule 23(a)(3)*. Plaintiffs' claims are typical of the claims of the Nationwide Class. Remark and Birkett, like all proposed members of the Class, had their PII compromised in the Data Breach. Defendants' uniformly unlawful course of conduct injured Remark, Birkett, and Class Members in the same wrongful acts and practices. Likewise, Remark, Birkett, and other Class Members must prove the same facts in order to establish the same claims.

79. *Adequacy of Representation Under Rule 23(a)(4)*. Remark and Birkett are adequate representatives of the Nationwide Class because they are Nationwide Class Members and their interests do not conflict with the interests of the Nationwide Class. Remark and Birkett have retained counsel competent and experienced in complex litigation and consumer protection class action matters such as this action, and Remark and Birkett and their counsel intend to vigorously prosecute this action for the Nationwide Class's benefit and have the resources to do so. Remark and Birkett and their counsel have no interests adverse to those of the other members of the Nationwide Class.

80. *Predominance and Superiority*. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of

each Nationwide Class Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Nationwide Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Even if each Nationwide Class Member could afford individual litigation, the Court system could not. It would be unduly burdensome if tens of thousands of individual cases or more proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it requires individual resolution of common legal and factual questions. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

81. As a result of the foregoing, class treatment under Fed. R. Civ. P. 23(b)(2) and (b)(3) is appropriate.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

82. Plaintiffs and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

83. In the course of providing telecommunications and cloud computing services to its clients and customers, Defendants solicited, gathered, and stored the PII of Plaintiffs and Class Members. Because Defendants were entrusted with such PII at all times herein relevant, Comcast and Citrix owed to Plaintiffs and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII in their care, control,

and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems. This duty arose independently from any contract.

84. Defendants knew, or should have known, of the risks inherent in collecting and storing massive amounts of PII, including the importance of adequate data security and the high frequency of cyberattacks and well-publicized data breaches. Comcast and Citrix owed duties of care to Plaintiffs and Class Members because it was foreseeable that Defendants' failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that sensitive information. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's PII by failing to limit access to this information to unauthorized third parties and by not properly supervising both the way the PII was stored, used, and exchanged, and those in their employ responsible for such tasks.

85. Defendants owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Comcast and Citrix also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and circumstances of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

86. Defendants also had a common law duty to prevent foreseeable harm to others. Defendants had full knowledge of the sensitivity and high value of the PII that they stored and the types of foreseeable harm and injury-in-fact that Plaintiffs and Class Members could and would

suffer if that PII were wrongfully disclosed, leaked, accessed, or exfiltrated. Defendants' conduct created a foreseeable and unreasonable risk of harm to Plaintiffs and Class Members, who were the foreseeable victims of Defendants' inadequate data security practices.

87. Defendants violated their duties to implement and maintain reasonable security procedures and practices, including through Citrix's failure to promptly identify and provide patch solutions to the Citrix Bleed vulnerability and Comcast's failure to promptly implement such remedial measures to its networks, servers, and files that held tens millions of individuals' PII or encrypt or anonymize such data. Defendants' duties included, among other things, designing, maintaining, and testing Defendants' information security controls to ensure that PII in their possession was adequately secured by, for example, encrypting or anonymizing sensitive personal information, installing intrusion detection and deterrent systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

88. Defendants' duties of care also arose by operation of statute. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII of Plaintiffs and Class Members.

89. The FTC Act was enacted to protect Plaintiffs and the Class Members from the type of wrongful conduct in which Defendants engaged.

90. Defendants breached their duties to exercise reasonable care in protecting Plaintiffs' and Class Members' PII by failing to implement and maintain adequate data security measures to safeguard Plaintiffs' and Class Members' sensitive personal information, failing to encrypt or anonymize PII within their systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII no longer necessary for the provision of telecommunications services to their clients and customers,

allowing unmonitored and unrestricted access to unsecured PII, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiffs' and Class Member's confidential and private information. Additionally, Defendants breached their duties by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendants also violated their duties under the FTC Act.

91. The law imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of PII to Plaintiffs and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Comcast and Citrix further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members. In so doing, Defendants actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiffs and Class Members. Timely disclosure was necessary so that Plaintiffs and Class Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud; (iii) purchase or otherwise obtain credit reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public records; (vi) change or update passwords on their various accounts; and (vii) take other meaningful steps to protect themselves and attempt to avoid or recover from identity theft and other harms.

92. Comcast's parent company, Comcast Corporation, has a market cap of over $160 billion and earned over $120 billion in revenue in 2023. Additionally, when it was acquired in February 2022, Citrix was valued at $16.5 billion, and in 2021 it collected over $3.2 billion in revenue. Accordingly, Defendants had the financial and personnel resources necessary to deploy robust cybersecurity protocols and controls, and to prevent the Data Breach. Comcast and Citrix

nevertheless failed to adopt reasonable data security measures, in breach of the duties they owed to Plaintiffs and Class Members.

93. Plaintiffs and Class Members had no ability to protect their PII once it was in Defendants' possession and control. Defendants were in an exclusive position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

94. But for Defendants' breach of their duties to adequately protect Class Members' PII, Class Members' PII would not have been stolen. As a result of Defendants' negligence, Plaintiffs and Class Members suffered and will continue to suffer the various types of damages alleged herein. There is a temporal and close causal connection between Defendants' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs and Class Members.

95. As a direct and traceable result of Defendants' negligence, Plaintiffs and the Class have suffered or will suffer an increased and impending risk of fraud, identity theft, damages, embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to mitigate and remediate the effects of the Data Breach. These harms to Plaintiffs and the Class include, without limitation: (i) loss of the opportunity to control how their personal information is used; (ii) diminution in the value and use of their personal information entrusted to Defendants; (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (vi) unauthorized use of compromised personal information to open new financial and other accounts; (vii) continued risk to their personal information, which remains in Defendants'

possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and (viii) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

96. Defendants' negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity of the private information under Defendants' care, and its failure to take adequate remedial steps, including prompt notification of the victims, following the Data Breach.

97. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

98. Plaintiffs and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

99. Pursuant to the FTC Act, 15 U.S.C. § 45, Comcast and Citrix had a duty to maintain fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII.

100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duties to protect Plaintiffs' and the Class Members' PII.

101. Defendants' duties to use reasonable care in protecting confidential and sensitive 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.

102. Defendants violated their duties under Section 5 of the FTC Act by failing to use reasonable or adequate data security practices and measures to protect Plaintiffs' and the Class's 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 that Comcast and Citrix collected and stored and the foreseeable consequences of a cybersecurity data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

103. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because 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.

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

105. The injuries and harms suffered by Plaintiffs and the Class Members were the reasonably foreseeable result of Defendants' breach of their duties. Comcast and Citrix knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiffs and the Class Members to suffer the foreseeable harms associated with the exposure of their PII.

106. Defendants' various violations and its failure to comply with the applicable laws and regulations referenced above constitutes negligence *per se*.

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

108. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members 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 Comcast and Citrix fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class Against Comcast)

109. Plaintiffs and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

110. Plaintiffs and Class Members were required to provide their PII and other private information to Comcast as a condition to receiving Comcast's services and products.

111. As part of these transactions, Comcast agreed to safeguard and protect the PII and other private information of Plaintiffs and Class Members. Implicit in these transactions between Comcast, Plaintiffs, and Class Members was the obligation that Comcast would use the PII and other private information only for approved business purposes and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

112. Additionally, Comcast implicitly promised to retain this PII and other private information only under conditions that kept such information secure and confidential and therefore

had a duty to reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or access.

113. Plaintiffs and Class Members entered into implied contracts with the reasonable expectation that Comcast's data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class Members believed that Comcast would use part of the monies paid to Comcast under the implied contracts to fund adequate and reasonable data security practices to protect their PII and other private information.

114. Plaintiffs and Class Members would not have provided and entrusted their PII and other private information to Comcast or would have paid less for Comcast's services and products in the absence of the implied contract between them and Comcast. The safeguarding of Plaintiffs' and Class Members' PII and other private information was critical to realizing the intent of the parties.

115. The nature of Comcast's implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiffs' and Class Members' PII and other private information in order to prevent harm and prevent present and continuing increased risks.

116. Comcast breached its implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII and other private information, which was compromised as a result of the Data Breach. Comcast further breached these implied contracts by failing to provide Plaintiffs and Class Members with timely and accurate notice of the Data Breach.

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

118. As a direct and proximate result of Comcast's breaches, Plaintiffs and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

FOURTH CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and the Nationwide Class Against Citrix)

119. Plaintiffs and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

120. Citrix entered into contracts with its clients and customers, including Plaintiffs' telecommunications service provider, Comcast, to provide software products and services—including data security practices, procedures, and protocols sufficient to safeguard the PII and other private information of Plaintiffs and Class Members.

121. These contracts were made expressly for the benefit of Plaintiffs and Class Members given that the transfer of their PII and other private information to Citrix for storage, protection, and safeguarding was the objective of the contracting parties. Therefore, Plaintiffs and Class Members were direct and express beneficiaries of these contracts.

122. Citrix knew that a breach of these contracts with its clients and customers would harm Plaintiffs and Class Members.

123. Citrix breached the contracts with its clients and customers when it failed to utilize adequate computer systems or data security practices to safeguard Plaintiffs' and Class Members' PII and other private information.

124. Plaintiffs and Class Members were directly and proximately harmed by Citrix's breaches in failing to use reasonable security measures to safely store and protect Plaintiffs' and Class Members' PII and other private information.

125. Plaintiffs and Class Members are therefore entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach in an amount to be determined at trial.

FIFTH CAUSE OF ACTION
Unjust Enrichment / Quasi-Contract
(On Behalf of Plaintiffs and the Nationwide Class Against Comcast)

126. Plaintiffs and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

127. This claim is pleaded in the alternative to the breach of implied contract claim.

128. Plaintiffs and Class Members conferred a monetary benefit upon Comcast in the forms of (i) monies paid for services and products, and (ii) the provision of their valuable PII. Indeed, upon acquiring the PII, Comcast was then able to charge money for its services and products, and utilize the PII to "improve [its] Services, develop new products and services, give recommendations, [and] deliver personalized consumer experiences[.]"[26] The PII was thus used to facilitate payment and generate additional revenue for Comcast.

129. Comcast accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Comcast profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

130. Upon information and belief, Comcast, like most other corporate entities, fund its data security measures entirely from its general revenue, which includes money paid by Plaintiffs and Class Members.

131. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is or should have been used to provide a reasonable level of data security.

[26] Our Privacy Policy, *supra* note 3.

132. Comcast enriched itself by saving the costs it reasonably should have expended on data security measures to secure its customers' PII.

133. Instead of providing a reasonable level of security that would have prevented the Data Breach, Comcast calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing less expensive and less effective security measures.

134. As a direct and proximate result of Comcast's failure to provide the requisite security, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

135. Comcast should not be permitted to retain the money belonging to Plaintiffs and Class Members because Comcast failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

136. Comcast should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by it as a result of its conduct and the resulting Data Breach alleged herein.

SIXTH CAUSE OF ACTION
Injunctive / Declaratory Relief
28 U.S.C. §§ 2201, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class Against Defendants)

137. Plaintiffs and Class Members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

138. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statutes and other laws described herein.

139. Defendants owe a duty of care to Plaintiffs and Class Members, which required Comcast and Citrix to adequately monitor and safeguard Plaintiffs' and Class Members' PII.

140. Defendants and their officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII belonging to Plaintiffs and Class Members.

141. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that may compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and the risk remains that further compromises of their private information will occur in the future.

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

a. Defendants owe a legal duty to adequately secure the PII of Plaintiffs and the Class within their care, custody, and control under the common law and Section 5 of FTC Act;

b. Defendants breached their duties to Plaintiffs and the Class by allowing the Data Breach to occur;

c. Defendants' existing data monitoring measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices that are

appropriate to protect the PII of Plaintiffs and the Class within Defendants' custody, care, and control; and

d. Defendants' ongoing breaches of said duties continue to cause harm to Plaintiffs and the Class.

143. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with telecommunications and cloud computing industry standards to protect the PII of Plaintiffs and the Class within their custody, care, and control, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance and protection services to Plaintiffs and Class Members; and

b. Order that, to comply with Defendants' obligations and duties of care, Comcast and Citrix must implement and maintain reasonable security and monitoring measures, including, but not limited to:

a. Engaging 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, networks, and servers on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

ii. Encrypting and anonymizing the existing PII within their servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendants to provide adequate telecommunications and cloud computing services to their clients and customers;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training their security personnel regarding any new or modified procedures;

v. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendants' internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

144. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another Comcast or Citrix data breach or cybersecurity incident occurs, Plaintiffs and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiffs and the Class for the serious risks of future harm.

145. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

146. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent Comcast or Citrix

data breach or cybersecurity incident, thus preventing future injury to Plaintiffs and the Class and other persons whose PII would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

A. Certifying this action as a class action under Fed. R. Civ. P. 23 and appointing Plaintiffs and their counsel to represent the Class;

B. Entering judgment for Plaintiffs and the Class;

C. Granting permanent and appropriate injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendants to adequately safeguard the PII of Plaintiffs and the Class by implementing improved security controls;

D. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

E. Award punitive damages and penalties as allowed by law in an amount to be determined at trial;

F. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of Defendants' unlawful acts, omissions, and practices;

G. Awarding to Plaintiffs and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

I. Granting such further and other relief as may be just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiffs hereby demand a trial by jury.

Dated: February 22, 2024

Respectfully submitted,

/s/ Anthony M. Christina

Amber L. Schubert (*pro hac vice* forthcoming)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel: (415) 788-4220
Email: aschubert@sjk.law

Christian Levis (*pro hac vice* forthcoming)
Amanda G. Fiorilla (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Email: clevis@lowey.com
Email: afiorilla@lowey.com

Anthony M. Christina
PA ID# 322528
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Tel: (215) 399-4770
Email: achristina@lowey.com

Counsel for Plaintiffs Jaclyn Remark and Noah Birkett and the Putative Class