UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

ROBERT SMITH, individually and on behalf of all others similarly situated, Plaintiff(s), v. COMCAST CABLE COMMUNICATIONS, LLC d/b/a XFINITY and CITRIX SYSTEMS, INC., Defendants.	CASE NO.: 2:24-cv-258 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Robert Smith ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendant Comcast Cable Communications, LLC d/b/a Xfinity ("Xfinity") and Defendant Citrix Systems, Inc. ("Citrix") (collectively, "Defendants"), on behalf of himself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to his own actions and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. On December 18, 2023, Xfinity, a Philadelphia-based telecommunications business and the largest home internet provider and cable provider in the United States, disclosed that it was the subject of a massive data breach through a vulnerability in Citrix' software whereby hackers gained unauthorized access to its networks between October 16 and October 19, 2023 (the "Data Breach"). Initial reports suggest the Data Breach impacted nearly 36 million former and current Xfinity customers.

2. The hackers compromised former and current customers' highly-sensitive information stored on Xfinity's servers, including names, Social Security numbers, usernames and

hashed passwords, dates of birth, and secret questions and answers (collectively, "PII"), which Xfinity collected as a condition for use of its services and transferred to Citrix, and for failing to provide timely, accurate and adequate notice to Plaintiff and other class members that their PII had been stolen and precisely what types of information were stolen, and for Defendant Xfinity's near two-week delay in resolving the network vulnerability after being put on notice.

3. The Data Breach occurred because Defendants failed to implement reasonable security procedures and practices, failed to disclose material facts surrounding their deficient data security protocols, failed to timely notify the victims of the Data Breach, and failed to timely remedy the vulnerability in Xfinity's internal systems.

4. As a result of Defendants' failure to protect the PII it was entrusted to safeguard, Plaintiff and class members now face a significant risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

5. Plaintiff Robert Smith is a resident of Delaware, Ohio whose PII was compromised from Xfinity.

6. Defendant Comcast Cable Communications, LLC d/b/a Xfinity is a telecommunications business organized and existing under the laws of the State of Delaware, having its principal place of business in Philadelphia, Pennsylvania.

7. Defendant Citrix Systems, Inc. is a cloud computing company organized and existing under the laws of the State of Delaware, having its principal place of business in Ft. Lauderdale, Florida.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and at least some members of the proposed Class have a different citizenship from Defendants. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

9. This Court has jurisdiction over Xfinity because it maintains and operates its headquarters in this District. Defendant Xfinity is authorized to conduct business in this District and is subject to general personal jurisdiction in this state.

10. This Court has jurisdiction over 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 this State, including substantial marketing and sales of services and products—including Citrix's NetScaler software used by Xfinity in connection with the Data Breach—within this State.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events and omissions giving rise to this action occurred in this District, including unknown actors accessing, copying, and exfiltrating the PII of Xfinity's customers.

FACTUAL ALLEGATIONS

Defendants' Privacy Practices

12. Xfinity 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 information, including but not limited to names, Social Security numbers, dates of birth, and financial information. As a result, when consumers contract Xfinity's services, their highly sensitive PII is stored on Xfinity's network servers.

13. Citrix is a major technology company, specializing in digital workspace solutions and "App Delivery and Security solutions, which deliver the applications and data employees need across any network with security, reliability and speed."[1] Citrix offers its NetScaler software that purportedly improves the efficiency and speeds of applications ("NetScaler ADC" or "Citrix ADC") and consolidates remote access infrastructure by providing a single-sign-on across all applications ("NetScaler Gateway").

14. Given the amount and sensitive nature of the data they collect, Defendants maintain policies explaining their privacy practices handling consumers' personal information. Through these policies, Defendants represent to consumers and the public that they possess robust security features to protect PII and that they their responsibility to protect PII seriously.

15. For example, Xfinity claims that consumers "are in control of [their] data" and that it only shares consumers' personal information to credit reporting agencies, on direction of the consumer, when required by law or to respond to legal process, and to protect Xfinity and its rights,

---

[1] *Citrix Systems, Inc. Mar. 2022 Form 10-Q*, SEC.GOV, https://www.sec.gov/archives/edgar/data/877890/000087789022000060/ctxs-20220331.htm (last visited Jan. 17, 2024).

safety of employees, customers, and other individuals.[2] Xfinity also boasts that it follows "industry-standard practices to secure the information [it] collects[s] to prevent the unauthorized access, use, or disclosure of any personal information" that it collects and maintains.[3] Furthermore, Xfinity represents that although it retains personal information for different lengths of time depending on certain circumstances, Xfinity "destroy[s], de-identif[ies], or anonymize[s] the information when it is no longer needed in identifiable form."[4]

16. Citrix also maintains a privacy policy explaining its treatment of PII. Citrix represents it "do[es] not sell or otherwise disclose personal information about [consumers,]" unless there is some lawful reason.[5] Aside from the privacy policy, Citrix promises that its NetScaler Gateway software is "simple to configure, ***secure*** and a better connectivity experience…" [6]

17. Given Defendants avowed experience in their field handling highly sensitive personal information, they understood the need to protect consumers' PII and prioritize data security.

The Data Breach

18. Between October 16 and October 19, 2023, hackers infiltrated Xfinity's networks and accessed highly sensitive PII stored on its servers. On December 18, 2023, Xfinity disclosed in a letter to the Office of the Maine Attorney General that on October 10, 2023, Citrix notified

---

[2] *Our Privacy Policy*, XFINITY, https://www.xfinity.com/privacy/policy#privacy-when (last visited Jan. 17, 2024).

[3] *Id.*

[4] *Id.*

[5] *Privacy Policy*, CLOUD.COM, https://www.cloud.com/privacy-policy (last visited Jan. 17, 2024).

[6] Akhilesh Dhawan, *Simple, Secure & Better Connectivity with Net Scaler Gateway Service*, https://www.citrix.com/blogs/2017/08/04/simple-secure-better-connectivity-with-netscaler-gateway-service/ (Aug. 9, 2017) (emphasis added).

Xfinity that its Citrix's NetScaler software contained a vulnerability.[7] This vulnerability has been coined as "Citrix Bleed." At this same time as Citrix's notification to Xfinity, Citrix also released a "patch" to fix the vulnerability.[8] As of October 10, 2023, Citrix had not noted active exploitation of the vulnerability. By October 18, 2023, security researchers at Mandiant reported that the vulnerability was under "active" exploitation,[9] and on October 23, 2023, Citrix disclosed that it was aware of targeted attacks.[10]

19. Despite possessing knowledge of the vulnerability and potential solutions as early as October 10, 2023, Xfinity waited weeks to "patch" its systems against this serious vulnerability.

20. Xfinity's delay proved to be catastrophic. During that time, Xfinity's internal systems were accessed by hackers between October 16 and October 19, 2023. It was not until November 16, 2023, that Xfinity "determined that information was likely acquired." The Data Breach impacted 35,879,455 individuals, suggesting that the breach impacted almost all its customer as its Q2 2023 earnings report indicated that the company had 32 million broadband customers.[11]

---

[7] *See Notice to Customers of Data Security Incident*, XFINITY.COM, https://assets.xfinity.com/assets/dotcom/learn/Data-Incident.pdf (last visited Jan. 16, 2024), attached as **Exhibit A**; *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/me/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml (last visited Jan. 16, 2024).

[8] *Id.*

[9] MANDIANT, *Remediation for Citrix NetScaler ADC and Gateway Vulnerability (CVE-2023-4966)*, https://www.mandiant.com/resources/blog/remediation-netscaler-adc-gateway-cve-2023-4966 (last updated Oct. 18, 2023).

[10] Anil Shetty, *CVE-2023-4966: Critical security update now available for NetScaler ADC and NetScaler Gateway*, https://www.netscaler.com/blog/news/cve-2023-4966-critical-security-update-now-available-for-netscaler-adc-and-netscaler-gateway/ (Oct. 23, 2023).

[11] *Comcast Reports 2nd Quarter 2023 Results*, CMCSA.COM, https://www.cmcsa.com/news-releases/news-release-details/comcast-reports-2nd-quarter-2023-results (last visited Jan. 17, 2024).

21. On December 6, 2023, Xfinity learned that consumers' information, including usernames and hashed passwords, names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers.[12] The Notice Letter further disclosed that Xfinity's "data analysis is continuing" and that it "will provide additional notices as appropriate."

The Data Breach was Foreseeable and Preventable

22. Following the Data Breach, Xfinity stated that it "can't emphasize enough how seriously" it is taking this matter and that it takes its responsibility to protect customers' information seriously.

23. But Defendants, like any company of their size that stores massive amounts of sensitive PII, should have had robust protections in place to detect and terminate a successful intrusion long before access and exposure of customer data. Defendants' failure to prevent the breach is inexcusable given their knowledge that they were prime targets for cyberattacks.[13]

24. In 2022, the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) coauthored the joint Cybersecurity Advisory explicitly highlighting "[t]elecommunications and network service prover targeting" by cyber actors.[14] The Advisory explains how cyber actors exploit and access telecommunication organizations and network service providers though the use of open-source tools "that allows for the scanning of IP addresses for vulnerabilities." Once these cyber actors

---

[12] *See* Ex. A.

[13] *See* Sam Sabin, *Wave of telecom data breaches highlight industry's weaknesses*, AXIOS, https://www.axios.com/2023/03/17/telecom-data-breaches-t-mobile-att (Mar. 17, 2023).

[14] *People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices*, CISA.GOV, https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF (last visited Jan. 17, 2024).

gain an initial foothold, they identify "critical users and infrastructure including systems critical to maintaining the security of authentication, authorization, and accounting." In a table displaying top network device common vulnerabilities and exposures, the Advisory identifies a vulnerability in Citrix's NetScaler ADC and NetScaler Gateway. According to Citrix, "if exploited, [this vulnerability] could allow an unauthenticated attacker to perform arbitrary code execution."[15]

25. Xfinity recognized this risk in its own regulatory filings. For instance, in its 2022 Annual Report, Xfinity acknowledge the business risk of suffering a cyber security incident:

> **A cyber attack, information or security breach, or technology disruption or failure may negatively impact our ability to conduct our business or result in the misuse of confidential information, all of which could adversely affect our business, reputation and results of operations.**
>
> Network and information systems and other technologies, including those that are related to our network management, customer service operations and programming delivery and are embedded in our products and services, are critical to our business activities. In the ordinary course of our business, there are constant attempts by third parties to cause systems-related events and security incidents and to identify and exploit vulnerabilities in security architecture and system design. These incidents include computer hackings, cyber attacks, computer viruses, worms or other destructive or disruptive software, denial of service attacks, phishing attacks, malicious social engineering, and other malicious activities. Incidents also may be caused inadvertently by us or our third-party vendors, such as process breakdowns and vulnerabilities in security architecture or system design.
>
> Cyber threats and attacks are constantly evolving and are growing in sophistication and frequency, which increases the difficulty of detecting and successfully defending against them. Some cyber attacks have had, and in the future can have, cascading impacts that unfold with increasing speed across networks, information systems and other technologies across the world and create latent vulnerabilities in our and third-party vendors' systems and other technologies. Moreover, as we also obtain certain confidential, proprietary and personal information about our customers, personnel and vendors, and in some cases provide this information to third party vendors who agree to protect it, we face the risk that this information

---

[15] *CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance*, CITRIX.COM, https://support.citrix.com/article/CTX267027/cve201919781-vulnerability-in-citrix-application-delivery-controller-citrix-gateway-and-citrix-sdwan-wanop-appliance (last modified Oct. 22, 2020).

> may become compromised through a cyber attack or data breach, misappropriation, misuse, leakage, falsification or accidental release or loss of information. Due to the nature of our businesses, we may be at a disproportionately heightened risk of these types of incidents occurring because we maintain certain information necessary to conduct our business in digital form. We also incorporate third-party software (including extensive open-source software), applications, and data hosting and cloud-based services into many aspects of our products, services and operations, as well as rely on service providers to help us perform our business operations, all of which expose us to cyber attacks on such third-party suppliers and service providers.[16]

26. Aside from warnings from federal regulatory agencies, Defendants previously struggled to safeguard PII. In 2021, hackers gained access to Citrix's internal network and exfiltrating personal information pertaining to 24,316 of Citrix's employees, their dependents or beneficiaries, and third parties. Citrix ultimately reached a $2.3 million deal to settle claims arising from that data breach, including agreeing to contractual business commitments designed to prevent another data breach from occurring.[17]

27. And in mid-December 2022, Xfinity customers reported that their account information had been changed, and they could not access their accounts.[18] According to New Jersey's Cybersecurity team, unknown threat actors bypassed Xfinity's two-factor authentication system and set up a secondary email using the on users' accounts and changed their passwords. Several customers reported that even after resetting passwords and regaining access to their accounts, their accounts were again breached multiple times. Despite Xfinity's representation that

---

[16] *Comcast Corporation Dec. 31, 2022 Form 10-k*, CMCSA.COM, https://www.cmcsa.com/static-files/156da323-653e-4cc6-9bb4-d239937e9d2f (last visited Jan. 17, 2024).

[17] Lauren Berg, *Judge Greenlights Altered $2.3M Citrix Data Breach Deal*, LAW360, https://www.law360.com/articles/1348749/judge-greenlights-altered-2-3m-citrix-data-breach-deal (Jan. 26, 2021, 6:58 PM).

[18] *Comcast Xfinity Accounts Compromised in Extensive 2FA Bypass Attack*, NJCCIC, https://www.cyber.nj.gov/alerts-advisories/comcast-xfinity-accounts-compromised-in-extensive-2fa-bypass-attack (Dec. 29, 2022).

it takes the protection of customers' personal information seriously, Xfinity swept this intrusion under the rug as it "neither notified customers nor publicly announced the incident."

28. Considering recent high profile data breaches at other telecommunications companies, such as T-Mobile (37,000,000 impacted, announced January 2023); AT&T (9,000,000 impacted, announced March 2023); .and US-Cellular (52,000 impacted, announced March 2023), among others, Defendants knew or should have known that their data and consumers' PII would be, or had already been, targeted by cybercriminal.

29. To prevent unauthorized access, CISA encourages organizations to:

- Conduct regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patch and update software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensure devices are properly configured and that security features are enabled;
- Employ best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disable operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[19]

30. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[20]

---

[19] CISA Guide at 4.

[20] *Id.* at 5.

31. Furthermore, the Citrix Bleed "affected products contain[ing] a buffer overflow vulnerability."[21] A buffer overflow occurs when a program attempts to input more data than it can hold.[22] Under these circumstances, an area of computing memory set aside to hold the overflow data (i.e., a buffer) temporarily stores the data as it is transferred between locations.[23] This creates a vulnerability that can be exploited by hackers to gain unauthorized access to internal system and "is one of the best-known software security vulnerabilities yet remains fairly common."[24]

32. Consequently, Defendants knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if their data security system was breached, including the significant costs that would be imposed on customers as a result of a breach.

33. But despite all of the publicly available knowledge of the continued compromises of PII and despite holding the PII of millions of customers, Defendants failed to use reasonable care in maintaining the privacy and security of the PII of Plaintiff and Class members.

34. Had Defendants implemented industry standard security measures, adequately invested in data security, and promptly "patched" the vulnerabilities, unauthorized parties likely would not have been able to access Defendants' systems and the Data Breach would have been prevented or much smaller in scope.

---

[21] *Guidance for Addressing Citrix NetScaler ADC and Gateway Vulnerability CVE-2023-4966, Citrix Bleed*, CISA.GOV, https://www.cisa.gov/guidance-addressing-citrix-netscaler-adc-and-gateway-vulnerability-cve-2023-4966-citrix-bleed#_ftn1 (last visited Jan. 17, 2024).

[22] *Buffer Overflow*, OWASP.ORG, https://owasp.org/www-community/vulnerabilities/Buffer_Overflow (last visited Jan. 17, 2024).

[23] *Id.*

[24] *Buffer Overflow*, FORTINET, https://www.fortinet.com/resources/cyberglossary/buffer-overflow#:~:text=Buffer%20overflow%20is%20a%20software,vulnerabilities%20yet%20remains%20fairly%20common. (last visited Jan. 17, 2024).

Value of PII

35. The PII of consumers remains of high value to criminals, as evidenced by the continued sale and trade of such information on underground markets found on the "dark web"—which is a part of the internet that is intentionally hidden and inaccessible through standard web browsers.

36. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[25] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[26] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[27] Other sources show sensitive private information selling for as much as $363 per record.[28]

37. Data sets that include PII demand a much higher price on the black market. For example, the information likely exposed in the Data Breach is significantly more valuable than the

---

[25] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITALTRENDS, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (Oct. 16, 2019).

[26] Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACYAFFIARS.COM, https://www.privacyaffairs.com/dark-web-price-index-2021/ (Jun. 10, 2023).

[27] *For Sale in the Dark*, VPN OVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 17, 2024).

[28] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (July 27, 2015).

loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[29] The information likely disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

38. There is also an active and robust *legitimate* market for PII. In 2021, the data brokering industry alone was valued at $319 billion.[30] 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.[31] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[32]

39. Because their PII has independent value, Plaintiff and Class members must take measures to protect it including by, as Xfinity's online notice instructs, placing "freezes" and "alerts" with credit reporting agencies, changing passwords, and reviewing and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect.

Allegations Relating to Plaintiff Robert Smith

40. Plaintiff Robert Smith lives and resides in Delaware, Ohio and is a former customer of Xfinity.

---

[29] *See* Jesse Damiani, *Your Social Security Number Costs $4 on the Dark Web, New Report Finds,* FORBES, https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-darkweb-new-report-finds/?sh=770cee3a13f1 (Mar. 25, 2020).

[30] Devan Burris, *How grocery stores are becoming data brokers*, CNBC, https://www.cnbc.com/2023/12/10/how-grocery-stores-are-becoming-data-brokers.html#:~:text=In%202021%20the%20data%20broker,better%20idea%20of%20consumer%20trends. (Dec. 10, 2023, 12:00 PM).

[31] https://datacoup.com/#first-stop (last visited Jan. 17, 2024).

[32] *Nielsen Computer & Mobile Panel, Frequently Asked Questions*, NIELSEN, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 17, 2023).

41. Before moving to Ohio in 2013, Mr. Smith lived in Pittsburgh, Pennsylvania where he contracted with Xfinity (then Comcast Cable) for cable services between 2010 and 2013.

42. In connection with obtaining Xfinity's cable services, Mr. Smith was required to provide highly sensitive personal information, such as his contact information, date of birth, Social Security number, financial information, and so on. Xfinity also prompted Mr. Smith to create login credentials to access his account.

43. Xfinity shared Mr. Smith's information with Citrix through the NetScaler software.

44. In December 2023, Mr. Smith received a notification email from Xfinity stating that he was a victim of the Data Breach. The email stated that: "[w]e are notifying you of a recent data security incident involving your personal information."

45. The email recommended that Mr. Smith take certain action like resetting his password and monitoring credit reports for suspicious activity and to detect errors. Furthermore, the email recommended that Mr. Smith place a "fraud alert" or "security freeze," if not both, on his credit report to detect any possible misuse of personal information.

46. As a result of the Data Breach, Ms. Smith has spent time and effort researching the breach and reviewing his financial statements for evidence of unauthorized activity, which he will continue to do indefinitely.

47. In addition, Mr. Smith also experienced fraud about three weeks after the Data Breach. On November 11, 2023, an unknown actor attempted to open a credit card with JPMorgan Chase under Mr. Smith's account. After receiving the alert from JPMorgan Chase, Mr. Smith spent a considerable amount of time on the phone with Allstate Identity Protection and JPMorgan Chase to stop the fraudulent activity on his account.

48. Along with experiencing fraud, Mr. Smith also suffered emotional distress knowing that his highly personal information, such as his financial information and Social Security number, is no longer confidential and can be used for extortion, theft or fraud, and any number of additional harms against him for the rest of his life.

49. Because Xfinity continues to store and share Plaintiff's and Class Members' PII in the regular course of its business, they have a continuing interest in ensuring that the PII is Protected and safeguarded from additional authorized access.

Defendants Failed to Comply with Federal Law and Regulatory Guidance

50. Federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission (FTC) has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[33]

51. The FTC's publication Protecting Personal Information: A Guide for Business sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[34] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct

---

[33] *Start with Security: A Guide for Business*, FTC.GOV, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 17, 2024).

[34] *Protecting Personal Information: A Guide for Business*, FTC.ORG, https://www.ftc.gov/businessguidance/resources/protecting-personal-information-guide-business (last visited Jan. 17, 2024).

security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[35]

52. Additionally, the FTC recommends that organizations 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.[36]

53. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, 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, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[37]

54. Defendants were fully aware of their obligation to implement and use reasonable measures to protect customers' PII but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Defendants' failure to employ reasonable measures to protect against unauthorized access to customer information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[35] *Id.*

[36] *Start with Security: A Guide for Business*, FTC.GOV, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 17, 2024).

[37] FTC, *Privacy and Security Enforcement*, FTC.GOV, https://www.ftc.gov/news-events/media-resources/protecting-consumerprivacy/privacy-security-enforcement (last visited Jan. 17, 2024).

55. Though limited detail is available on the Data Breach, how it occurred, and the extent of the information involved, Defendants' failure to safeguard customers' PII suggests Defendants failed to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, encryption, and intrusion detection and prevention.

The Impact of the Data Breach on Victims

56. Defendants' failure to keep Plaintiff and Class members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, date of birth, Social Security numbers, and potentially financial account information—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class members now and into the indefinite future. Customers like Mr. Smith have already reported experiencing fraud associated with PII provided to Xfinity.

57. As a result, Plaintiff and Class members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

58. As discussed above, the PII likely exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial accounts, open

new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."[38]

59. Further, malicious actors may wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

60. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

61. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% report problems with family members as a result of the breach;
- 10% reported feeling suicidal.[39]

[38] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

[39] 2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces, https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Jan. 17, 2024).

62. Identity theft can also exact a physical toll on its victims. A similar survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[40]

63. The unauthorized disclosure of the sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[41]

64. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

---

[40] *Identity Theft: The Aftermath 2017*, https://www.idtheftcenter.org/wp-content/uploads/images/pagedocs/Aftermath_2017.pdf (last visited Jan. 17, 2024).

[41] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

65. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the value of the explicit and implicit promises of data security;

c. identity theft and fraud resulting from the theft of their PII;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. anxiety, emotional distress, and loss of privacy;

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

66. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

67. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law 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 has 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."[42]

68. Plaintiff and Class members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[43]

[42] http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 17, 2024).
[43] https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Jan. 17, 2024).

69. Because of the value consumers place on data privacy and security, telecommunication businesses with robust data security practices are viewed more favorably by consumers and can command higher prices than those who do not. Consequently, had customers known the truth about Defendants' data security practices—that they did not adequately protect and store their PII—they would not have sought contracted with Xfinity or would have paid significantly less. As such, Plaintiff and Class members did not receive the benefit of their bargain with Xfinity because they paid for the value of services they did not receive.

70. Plaintiff and Class members have a direct interest in Defendants' promises and duties to protect their PII, *i.e.*, that Defendants *not increase* their risk of identity theft and fraud. Because Defendants failed to live up to its promises and duties in this respect, Plaintiff and Class members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Defendants' wrongful conduct. Through this remedy, Plaintiff and Class members seek to restore themselves and class members as close to the same position as they would have occupied but for Defendants' wrongful conduct, namely their failure to adequately protect Plaintiff's and Class members' PII.

71. Plaintiff and Class members further seek to recover the value of the unauthorized access to their PII permitted through Defendants' wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-

practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

72. Xfinity's deficient notice letter also caused Plaintiff and Class members harm. For example, the objective of almost every data breach is to gain access to an organization's sensitive data so that the data can be misused for financial gain. Furthermore, the letter did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. Xfinity's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting months to disclose the Data Breach, Xfinity prevented victims from taking meaningful, proactive, and targeted mitigation measures that could help protect them from harm.

73. Because Defendants continue to hold the PII of customers, Plaintiff and Class members have an interest in ensuring that their PII is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

74. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff brings this action on behalf of himself and the Class defined as: All individuals whose personal information was compromised in the Data Breach announced by Defendants in or about December 2023 (the "Class").

75. Specifically excluded from the Class are Defendants; their officers, directors, or employees; any entity in which Defendants have a controlling interest; and any affiliate, legal representative, heir, or assign of Defendants. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

76. Class Identity: The members of the Class are readily identifiable and ascertainable. Defendants and/or their affiliates, among others, possess the information to identify and contact class members.

77. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. Xfinity's disclosures reveal that the Class contains nearly 36 million individuals whose PII was compromised in the Data Breach.

78. Typicality: Plaintiff's claims are typical of the claims of the members of the Class because all class members had their PII compromised in the Data Breach and were harmed as a result.

79. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no known interest antagonistic to those of the Class and his interests are aligned with Class members' interests. Plaintiff was subject to the same Data Breach as class members, suffered similar harms, and faces similar threats due to the Data Breach. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including data breach cases involving multiple classes and data breach claims.

80. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common

questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

a. Whether Defendants owed Plaintiff and Class members a duty to implement and maintain reasonable security procedures and practices to protect their PII;

b. Whether Defendants received a benefit without proper restitution making it unjust for Defendants to retain the benefit without commensurate compensation;

c. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class members' PII;

d. Whether Defendants acted negligently in failing to "patch" the vulnerability when it first received notice;

e. Whether Defendants violated its duty to implement reasonable security systems to protect Plaintiff's and Class members' PII;

f. Whether Defendants' breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class members;

g. Whether Defendants adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

h. Whether Plaintiff and Class members are entitled to damages to pay for future protective measures like credit monitoring and monitoring for misuse of personal information;

i. Whether Defendants provided timely notice of the Data Breach to Plaintiff and Class members; and

j. Whether Class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

81. Defendants have engaged in a common course of conduct and Plaintiff and Class members have been similarly impacted by Defendants' failure to maintain reasonable security procedures and practices to protect consumers' PII, as well as Defendants' failure to timely alert affected customers to the Data Breach, and their failure to timely "patch" the systems.

82. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

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

83. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

84. Defendant Xfinity required Plaintiff's and Class members' PII as a condition to receiving cable services. Xfinity collected and stored this PII for commercial gain. Xfinity used Citrix's software in connection with Plaintiff's and Class members' PII.

85. Defendants owed Plaintiff and Class members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access. Defendants acknowledged this duty in privacy policies, where they promised not to disclose PII without authorization.

86. Defendants owed a duty of care to Plaintiff and Class members to provide adequate data security, consistent with industry standards, to ensure that Defendants' systems and networks adequately protected the PII.

87. Defendants owed a duty of care to Plaintiff and Class members to remedy any flaws within their system without undue delay so as to alleviate the risk of compromising Plaintiff's and Class members' PII.

88. Defendant's duty to use reasonable care in protecting PII arises because of the parties' relationship, as well as common law and federal law, including the FTC regulations described above and Defendants' own policies and promises regarding privacy and data security.

89. Defendants knew, or should have known, of the risks inherent in collecting, storing, and transferring PII in a centralized location, Defendants' vulnerability to network attacks, and the importance of adequate security.

90. Defendants breached its duty to Plaintiff and class members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff and Class members;

b. Failing to comply with industry standard data security measures for the telecommunications industry leading up to the Data Breach;

c. Failing to comply with their own privacy policies;

d. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of Defendants' network and systems;

f. Failing to recognize in a timely manner that PII had been compromised;

g. Failing to timely and adequately disclose the Data Breach; and

h. Failing to timely "patch" the vulnerability in Defendants' internal system before the Data Breach occurred.

91. Plaintiff's and Class members' PII would not have been compromised but for Defendants' wrongful and negligent breach of its duties.

92. Defendants' failure to take proper security measures to protect the sensitive PII of Plaintiff and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access, copying, and exfiltrating of PII by unauthorized third parties. Given that telecommunications businesses are prime targets for hackers, Plaintiff and Class members are part of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by Defendants.

93. It was also foreseeable that Defendants' failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and Class members.

94. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have and will suffer damages including: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi)

anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

95. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

96. Section 5 of the Federal Trade Commission Act ("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 PII. 15 U.S.C. § 45(a)(1).

97. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

98. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. Defendants' conduct was unreasonable given the nature and amount of PII they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and Class members.

99. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

100. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

101. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. 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 Plaintiff and Class members. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members sustained actual losses and damages as alleged herein. Plaintiff and Class members alternatively seek an award of nominal damages.

COUNT III
Breach of Contract
(On Behalf of Plaintiff and the Class Against Defendant Xfinity)

102. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

103. Xfinity disseminated a "Privacy Policy" to its customers that constitutes an agreement between Xfinity and persons who provided their PII to Xfinity, including Plaintiff and Class members.

104. Plaintiff and Class members formed a contract with Xfinity and complied with all obligations under such contract when they provided PII to Xfinity subject to the Privacy Policy.

105. Xfinity promised in its Privacy Policy that it would "follow industry-standard practices to secure the information [it] collect[s] to prevent the unauthorized access, use, or disclosure of any personal information [it] collect[s] and maintain[s]" and that it would only share consumers' personal information to credit reporting agencies, on direction of the consumer, when required by law or to respond to legal process, and to protect Xfinity and its rights, safety of employees, customers, and other individuals.

106. Xfinity also promised that if an individual no longer subscribes to Xfinity's services, then it "still may need that [PII] for business and legal requirements, such as to protect against fraud, calculate taxes, or respond to legal requests" but that it will "destroy, de-identify, or anonymize the information when it is no longer needed in identifiable form."

107. Xfinity breached its agreements with Plaintiff and Class members when Xfinity allowed for the disclosure of Plaintiff's and Class members' PII without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in Privacy Policy, as well as when it failed to maintain the confidentiality of Plaintiff's and Class members' PII.

108. As a direct and proximate result of these breaches, Plaintiff 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. Plaintiff and Class members alternatively seek an award of nominal damages.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Class Against Defendant Xfinity)

109. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs and asserts this claim in the alternative to his breach of contract claim to the extent necessary.

110. Plaintiff and Class members were required to provide their PII to Xfinity as a condition to receiving cable services.

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

112. Additionally, Xfinity implicitly promised to retain this PII only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure or access.

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

114. Plaintiff and Class members would not have provided and entrusted their PII to Xfinity or would have paid less for Xfinity's services in the absence of the implied contract between them and Xfinity. The safeguarding of Plaintiff's and Class members' PII was critical to realizing the intent of the parties.

115. The nature of Xfinity's implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and Class members' PII in order to prevent harm and prevent present and continuing increased risk.

116. Xfinity breached its implied contract with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII, which was compromised as a result of the Data Breach.

117. As a direct and proximate result of Xfinity's breaches, Plaintiff 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. Plaintiff and Class members alternatively seek an award of nominal damages.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

118. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

119. Plaintiff and Class members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by the Defendants and which was stolen in the Data Breach. This information has independent value.

120. Plaintiff and Class members conferred a monetary benefit on Defendants in the form of payments for cable services, including those paid indirectly by Plaintiff and Class members to Defendants.

121. Defendants appreciated and had knowledge of the benefits conferred upon them by Plaintiff and Class members.

122. The price for cable services that Plaintiff and Class members paid (directly or indirectly) to Defendants should have been used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

123. Likewise, in exchange for receiving Plaintiff's and Class members' valuable PII, which Defendants were able to use for their own business purposes and which provided actual value to Defendants, Defendants were obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

124. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages as described herein. Under principles of equity and good conscience, Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds they received from Plaintiff and Class members, including damages equaling the difference in value between cable services that included implementation of

reasonable data privacy and security practices that Plaintiff and Class members paid for and the services without reasonable data privacy and security practices that they actually received.

COUNT VI
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

125. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

126. 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 grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

127. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class members from further cyberattacks and data breaches that could compromise their PII.

128. Defendants still possesses PII pertaining to Plaintiff and Class members, which means their PII remains at risk of further breaches because Defendants' data security measures remain inadequate. Plaintiff and Class members continue to suffer injuries as a result of the compromise of their PII and remain at an imminent risk that additional compromises of their PII will occur in the future.

129. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) Defendants' existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Defendants must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited

to, those listed at (ii), (a)-(i), *infra*, and must comply with those policies and procedures; (2) Defendants must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and Class members' PII if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security 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 on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

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

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Encrypting PII and segmenting PII by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner PII not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. Routinely and continually conducting 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.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and Class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: January 19, 2024

By: /s/ *Charles E. Schaffer*

Charles E. Schaffer
Nicholas J. Elia
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com

Norman E. Siegel*
J. Austin Moore*
Stefon J. David*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
david@stuevesiegel.com
**Pro Hac Vice Forthcoming*

Counsel for Plaintiff and the Class