UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION

RANDALL HUFFMAN and BRYAN QUERRY, on behalf of themselves and all others similarly situated, Plaintiffs, v. COMMSCOPE, INC. OF NORTH CAROLINA, and COMMSCOPE HOLDING COMPANY, INC., Defendants.	Case No. 5:23-cv-132-KDB-SCR **DEMAND FOR JURY TRIAL**

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Randall Huffman and Bryan Querry ("Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following against the above-captioned Defendant CommScope Inc. of North Carolina and CommScope Holding Company (collectively, "Defendant" or "CommScope") upon personal knowledge as to themselves and their own actions, and upon information and belief, including the investigation of counsel, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession, custody and/or control of Defendant (the "Data Breach"). The number of total breach victims is unknown, but on information and belief, the Data Breach has impacted at least thousands of former and current employees.

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of former and current employees' highly personal information, including names, Social Security numbers, address, emails, phone numbers, and financial account number ("personally identifying

information" or "PII").

3. On information and belief, the Data Breach occurred on March 27, 2023. However, CommScope did not become aware of suspicious activity on its network until "recently," providing cybercriminals unfettered access to its network system until CommScope discovered the Breach.

4. CommScope struggled to identify what information and which individuals were impacted by the Data Breach and took until April 24, 2023, to complete their internal investigation.

5. On May 12, 2023, CommScope finally began notifying Class Members about the widespread Data Breach ("Notice Letter"). The Notice Letter Plaintiffs received is attached as Exhibit A. However, CommScope has not completed notification of Class Members and continues to do so.

6. Due to CommScope deliberately obfuscating this information in their breach notice, it is unknown how many months CommScope waited before finally informing Class Members of the Breach, even though Plaintiffs and Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

7. CommScope's Breach Notice also obfuscated the nature of the breach and the threat it posted—refusing to tell its former and current employees how many people were impacted, how the breach happened, or why CommScope delayed notifying victims that hackers had gained access to highly sensitive PII.

8. Defendant's failure to timely detect and report the Data Breach made its employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect Plaintiffs' and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its employees.

11. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiffs are former employees of CommScope (and/or its subsidiary) and are Data Breach victims.

13. Plaintiff Randall Huffman worked for a subsidiary of CommScope from 2004-2010. And Plaintiff Bryan Querry worked for CommScope (and/or its subsidiary) from 1993-2003, as a maintenance technician.

14. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

15. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, employees' private information was exactly that—private. Not anymore. Now, employees' private information is forever exposed and unsecure.

PARTIES

16. Plaintiff, Randall Huffman, is a natural person and citizen of Nebraska, where he intends to remain. Plaintiff is a Data Breach victim, receiving the Breach Notice on May 12, 2023.

17. Plaintiff, Bryan Querry, is a natural person and citizen of North Carolina, where he intends to remain. Plaintiff is a Data Breach victim, having received the Breach Notice in May 2023.

18. Defendant, CommScope Inc. of North Carolina, is a North Carolina Corporation, with its principal place of business at 1100 CommScope Place, SE Hickory, NC 28602-3619.

19. Defendant, CommScope Holding Company, is a Delaware Corporation with its principal place of business at 1100 CommScope Place, SE Hickory, NC 28602-3619.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Plaintiffs and Defendant are citizens of different states.

21. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

22. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

CommScope

23. CommScope is a network infrastructure provider that creates "the world's most advanced networks"[1] by designing, manufacturing, and installing hardware infrastructure and software intelligence. CommScope touts that its infrastructure services provide "leading solutions that solve for tomorrow's possibilities." CommScope boasts an annual of $9.2 billion.[2]

24. On information and belief, CommScope accumulates highly sensitive PII of its employees.

25. On information and belief, CommScope maintains former employees' PII for years—even decades—after the employee-employer relationship is terminated.

26. In collecting and maintaining its employees' PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII.

27. Indeed, CommScope assures its employees that "your personal data is stored [by CommScope] strictly to the extent necessary for the performance of our obligations and strictly for the time necessary to achieve the purposes for which the Personal Data is collected, in accordance with applicable data protection laws." CommScope further promises that when it "no longer needs to use your personal data, we will remove it from our systems and records and/or take steps to properly render it unintelligible it *(sic)* so that you can no longer be identified from it".[3]

---

[1] About us, Commscope, https://www.commscope.com/about-us/ (last visited August 3, 2023).
[2] CommScope Revenue, Zippia, https://www.zippia.com/commscope-careers-2722/revenue/#:~:text=CommScope's%20revenue%20is%20%249.2%20billion.&text=CommScope%20has%2030%2C000%20employees%2C%20and,%2C%201.79%25%20growth%20from%202020 (last visited August 3, 2023).
[3] CommScope Recruiting Data Protection Notice, CommScope, https://www.commscope.com/about-us/commscope-recruiting-data-protection-notice/ (last visited August 3, 2023).

28. In collecting and maintaining employees' PII, CommScope agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII.

29. Despite recognizing its duty to do so, on information and belief, CommScope has not implemented reasonably cybersecurity safeguards or policies to protect its former and current employees' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, CommScope leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' PII.

The Data Breach

30. Plaintiffs are former employees of CommScope or its subsidiaries.

31. As a condition of employment with CommScope, employees were required to disclose their PII to Defendant and its subsidiaries, including but not limited to, their names, Social Security numbers, address, and financial account information. Defendant used that PII to facilitate employment of Plaintiffs, including payroll, and required Plaintiffs to provide that PII to obtain employment and payment for that employment.

32. On information and belief, CommScope collects and maintains former and current employees' unencrypted PII in its computer systems.

33. In collecting and maintaining the PII, CommScope implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

34. According to the Breach Notice, CommScope "recently became aware of a cybersecurity incident that involved the deployment of malware on certain systems". Following an internal investigation, CommScope discovered that "on March 26, 2023, an unauthorized party was able to remove some data from the network". Ex. A.

35. In other words, CommScope's investigation revealed that Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its former and current employees' highly sensitive PII.

36. Additionally, Defendant admitted that Plaintiffs' and the Class's PII were actually stolen during the Data Breach, confessing that victims' information was not just accessed but that the cybercriminals were "**able to remove** some data" from Defendant's network. Ex. A.

37. Upon information and belief, the notorious Vice Society ransomware gang was responsible for the cyberattack. Known as one of the most notorious and active ransomware actors that regularly makes headlines for their cyber-hacking actions[4], Vice Society has perpetrated multiple high-profile breaches in the last year alone and is infamous for targeting manufacturing

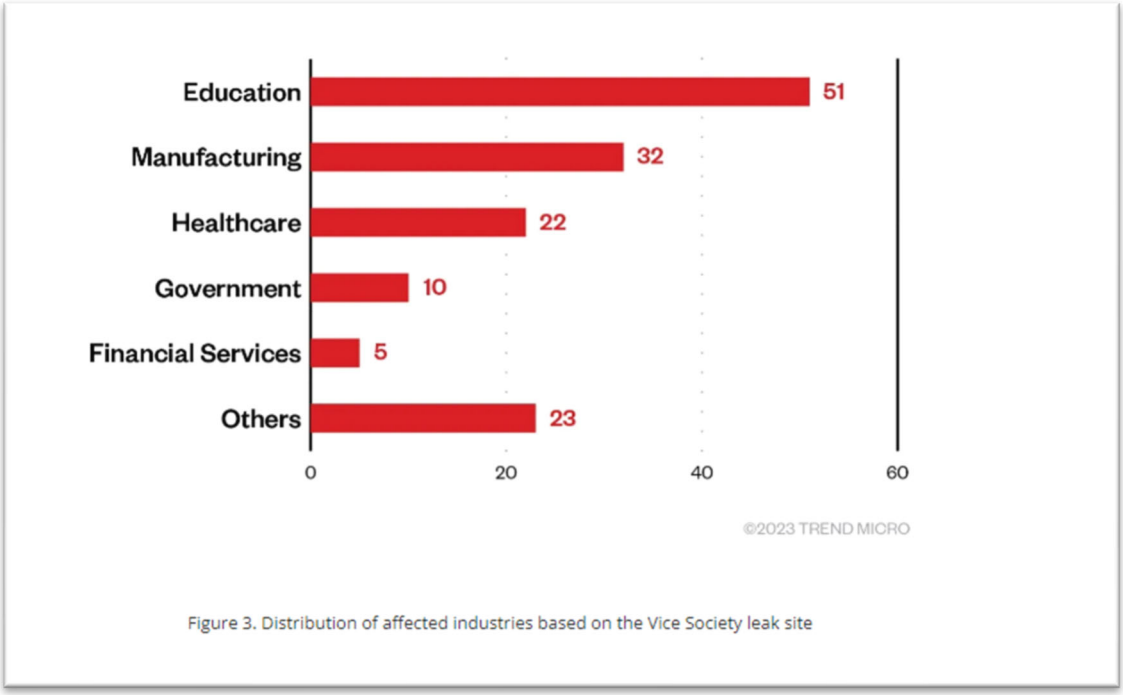

Figure 3. Distribution of affected industries based on the Vice Society leak site

[4] Vice Society Ransomware Gorup Targets Manufacturing Companies, https://www.trendmicro.com/en_us/research/23/a/vice-society-ransomware-group-targets-manufacturing-companies.html (last visited August 3, 2023)

companies like CommScope.[5] Defendant knew or should have known of the tactics that groups like Vice Society employ.

38. With the Sensitive Information secured and stolen by Vice Society, the hackers then purportedly issued a ransom demand to CommScope. However, CommScope has provided no public information on the ransom demand or payment.

39. On April 14 and 15, 2023, the presumed deadline of Vice Society' ransom demand, Vice Society released information obtained from the Breach on a data leak page. On information and belief, all stolen information was released onto the data leak page:

40. On or around May 12, 2023, –almost two months after the Breach first occurred– CommScope finally began notifying Class Members about the Data Breach.

41. Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

42. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing employees' PII, as evidenced by the Data Breach.

[5] *Id.*

43. Through its inadequate security practices, Defendant exposed Plaintiffs' and the Class's PII for theft and sale on the dark web.

Victim Name	CommScope
Victim Website *(if available)*	hXXps://www[.]commscope[.]com/
Description	Founded in 1976, CommScope Holding provides infrastructure solutions for communications networks worldwide. We design, manufacture, install and support the hardware infrastructure and software intelligence that enable our digital society to interact and thrive.

44. In response to the Data Breach, Defendant contends that it has and will "enhance [] our security controls and monitoring practices as appropriate." Ex. A. Although Defendant does not elaborate on what these 'enhancements' are, such enhancements should have been in place before the Data Breach.

45. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "carefully review account statements and credit reports to ensure all of your account activity is valid" and to "remain vigilant for incidents of fraud and identity theft." Ex. A.

46. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

47. On information and belief, CommScope has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

48. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

49. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

50. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the infrastructure and manufacturing adjacent industries preceding the date of the breach.[6]

51. In light of recent high profile data breaches at other manufacturing and infrastructure companies, Defendant knew or should have known that its employees' PII would be targeted by cybercriminals.

[6] 6 Industries Most Affected by Security Breaches, Cobalt, https://www.cobalt.io/blog/industries-most-affected-by-security-breaches (last visited August 3, 2023); *See also* Cost of a Data Breach: Infrastructure, security Intelligencehttps://securityintelligence.com/articles/cost-data-breach-infrastructure/ (last visited August 3, 2023).

52. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[7] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[8]

53. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [9]

54. In 2023, manufacturing and infrastructure adjacent industries were warned to be one of the most-breached sectors[10] and cost, on average, $4.82 million per breach.[11]

55. Cyberattacks on infrastructure companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report cautioned, "Cyber risk in

---

[7] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 13, 2023).

[8] *Id*.

[9] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited June 13, 2023).

[10] 6 Industries Most Affected by Security Breaches, Cobalt, https://www.cobalt.io/blog/industries-most-affected-by-security-breaches (last visited August 3, 2023).

[11] Cost of a Data Breach: Infrastructure, security Intelligencehttps://securityintelligence.com/articles/cost-data-breach-infrastructure/ (last visited August 3, 2023).

the financial system has grown over time as the system has become more digitized, as evidenced by the increase in cyber incidents."[12]

56. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including CommScope.

Plaintiff Randall Huffman's Experience

57. From approximately 2004 until 2010, Plaintiff Huffman was employed by a subsidiary of Defendant.

58. As a condition of employment, CommScope required Plaintiff to provide his PII, including but not limited to his full name, address, Social Security number, and financial account information.

59. Plaintiff provided his PII to CommScope and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

60. Plaintiff Huffman received a Breach Notice on May 12, 2023, from Defendant, indicating that his PII, including at least his full name, address, Social Security number, and financial information, may have been compromised in the Data Breach. In addition to the damages detailed herein, the Data Breach has caused Plaintiff Huffman to be at substantial risk for further identity theft.

61. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for over two months after the Data Breach occurred.

---

[12] Implications of Cyber Risk for Financial Stability, Federal Reserve, https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited July 20, 2023)

62. Plaintiff suffered actual injury from the exposure of his PII —which violates his rights to privacy.

63. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

64. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

65. Defendant also deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it in a timely manner.

66. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

67. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

68. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far 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.

69. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

70. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

71. Indeed, following the Data Breach, Plaintiff began experiencing spam texts and phone calls, suggesting that his PII has been placed in the hands of cybercriminals.

72. Additionally, following the Data Breach, Plaintiff was alerted by Equifax that his phone number was discovered on the dark web, further suggesting that his PII has been placed in the hands of cybercriminals.

73. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Bryan Querry's Experience

74. From approximately 1993 until 2003, Plaintiff Querry was employed by Defendant (or its subsidiary).

75. As a condition of employment, CommScope required Plaintiff to provide his PII, including but not limited to his full name, address, Social Security number, and financial account information.

76. Plaintiff provided his PII to CommScope and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

77. Plaintiff Huffman received a Breach Notice in May 2023, from Defendant, indicating that his PII, including at least his full name, Social Security number, and financial information, may have been compromised in the Data Breach. In addition to the damages

detailed herein, the Data Breach has caused Plaintiff Querry to be at substantial risk for further identity theft.

78. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for over two months after the Data Breach occurred.

79. Plaintiff suffered actual injury from the exposure of his PII—which violates his rights to privacy.

80. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

81. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

82. Defendant also deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it in a timely manner.

83. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

84. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

85. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far 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.

86. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

87. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

88. In fact, in or around May 2023, Plaintiff received a warning from the United Federal Credit Union about suspicious activity including a seemingly fraudulent purchase.

89. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

90. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

91. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended 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 identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

92. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

93. The value of Plaintiffs' and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

94. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

95. One such example of criminals using PII for profit is the development of "Fullz" packages.

96. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

97. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

98. Defendant disclosed the PII of Plaintiffs and the Class for criminals to use in the conduct of criminal activity including theft and sale on the dark web. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

99. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest

ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

100. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

101. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

102. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

104. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable

and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

105. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers, or in this case former and current employees', PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

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

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

108. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems;

protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

109. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

110. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

111. Plaintiffs sues on behalf of themselves and the proposed class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> All individuals residing in the United States whose PII was compromised in the CommScope Data Breach including all those who received notice of the breach.

112. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

113. Plaintiffs reserve the right to amend the class definition.

114. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

115. **Numerosity**. The exact number of Class members is unknown but is estimated to be up to thousands of former and current CommScope employees at this time, and individual joinder in this case is impracticable.

116. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control.

117. **Typicality**. Plaintiffs' claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

118. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

119. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

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

c. Whether Defendant were negligent in maintaining, protecting, and securing PII;

d. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII;

e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Defendant's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

h. What the proper damages measure is; and

i. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

120. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

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

121. Plaintiffs and the members of the Class incorporate the above allegations as if fully set forth herein.

122. Plaintiffs and members of the Class entrusted their PII to CommScope. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing

Defendant's security systems to ensure the PII of Plaintiffs and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

123. CommScope was under a basic duty to act with reasonable care when it undertook to collect, create, maintain, and store Plaintiffs' and the Class's sensitive data on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

124. Defendant knew that the PII of Plaintiffs and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harm that could happen if the PII of Plaintiffs and the Class was wrongfully disclosed.

125. By being entrusted by Plaintiffs and the Class to safeguard their PII, Defendant had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class agreed to provide their PII with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiffs and the Class of any security concerns that might call for action by Plaintiffs and the Class.

126. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiffs' and the other Class member's PII.

127. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the personal data of Plaintiffs and the Class and all resulting damages.

128. The injury and harm suffered by Plaintiffs and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class members' PII. Defendant knew its systems and technologies for processing and securing the PII of Plaintiffs and the Class had numerous security vulnerabilities.

129. As a result of this misconduct by Defendant, the PII of Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

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

130. Plaintiffs and the members of the Class incorporate the above allegations as if fully set forth herein.

131. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

132. 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 Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's sensitive PII.

133. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

134. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

135. 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 members of the Class.

136. Defendant breached its respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

137. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

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

139. Had Plaintiffs and members of the Class known that Defendant did not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

140. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and members of 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; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

141. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as CommScope fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

COUNT III
Violation Of North Carolina Unfair Trade Practices Act
(On Behalf of Plaintiffs and the Class)

142. Plaintiffs and the members of the Class incorporate the above allegations as if fully set forth herein.

143. Defendant advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

144. Defendant engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.

145. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

146. Defendant intended to mislead Plaintiffs and Class members and induce them to rely on its omissions.

147. Had Defendant disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiffs and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

148. Defendant acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiffs' and Class members' rights.

149. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

150. Defendant's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

151. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

COUNT IV
Breach Of Implied Contract
(On Behalf of Plaintiffs and the Class)

152. Plaintiffs and the members of the Class incorporate the above allegations as if fully set forth herein.

153. Plaintiffs and Class Members were required to provide their PII Defendant as a condition of receiving employment from Defendant. Plaintiffs and Class Members provided their PII to Defendant in exchange for Defendant's employment.

154. Plaintiffs and Class Members reasonably understood that a portion of the funds from their employment would be by Defendant used to pay for adequate cybersecurity and protection of their PII.

155. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for employment.

156. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

157. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII.

158. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

159. After all, Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

160. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

161. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

162. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

163. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, receive and maintained.

164. In these and other ways, Defendant violated its duty of good faith and fair dealing.

165. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

166. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

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

167. Plaintiffs and the members of the Class incorporate the above allegations as if fully set forth herein.

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

169. Plaintiffs and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate its business.

170. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members. And Defendant benefited from receiving Plaintiffs' and Class Members' PII, as this was used to facilitate its business.

171. Plaintiffs and Class Members reasonably understood that a portion of the funds from their employment would be by Defendant used to pay for adequate cybersecurity and protection of their PII.

172. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

173. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

174. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' services because Defendant failed to adequately protect their PII.

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

176. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: February 23, 2024

Respectfully Submitted,

By: */s/ Raina C. Borrelli*

Raina C. Borrelli (*pro hac vice*)
Samuel J. Strauss (*pro hac vice* anticipated)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com

Joel R. Rhine, NC Bar No. 16028
Martin A. Ramey, NC Bar No. 33617
Ruth A. Sheehan, NC Bar No. 48069
Elise H. Wilson, NC Bar No. 60366
RHINE LAW FIRM, P.C.
1612 Military Cutoff Road, Suite 300,
Wilmington, NC 28403
Telephone: (910) 772-9960
Facsimile: (910) 772-9062
Phone: (910) 772-9960
jrr@rhinelawfirm.com
mjr@rhinelawfirm.com
ras@rhinelawfirm.com
ehw@rhinelawfirm.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I, Raina C. Borrelli, hereby certify that on February 23, 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record via the ECF system.

DATED this 23rd day of February, 2024.

TURKE & STRAUSS LLP

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423