IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No: _____

SUSAN OWEN-BROOKS, on behalf of herself and all others similarly situated,

Plaintiff,

v.

DISH NETWORK CORPORATION, a Nevada Corporation,

Defendant.

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Susan Owen-Brooks, individually and on behalf of the Classes defined below of similarly situated persons ("Plaintiff"), alleges the following against DISH Network Corporation ("DISH" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against DISH for its failure to properly secure and safeguard Plaintiff's and other similarly situated DISH customers' and employees' personal information from hackers.

2. DISH, based in Englewood, Colorado, is a satellite television company that serves nearly 10 million customers from around the country. According to news reports, "this widespread

outage hit Dish.com, the Dish Anywhere app, Boost Mobile (a subsidiary owned by Dish Wireless), and other websites and networks owned and operated by Dish Network."[1]

3. In a Form 8-K filed with the Securities and Exchange Commission on or about February 28, 2023 the company announced "a network outage that affected internal servers and IT telephony" and that the company "became aware that certain data was extracted from the Corporation's IT systems as part of this incident[,]" which possibly "includes personal information."[2]

4. On or about March 14, 2023, DISH emailed customers notifying them of a hacking incident in which data including personal information was compromised.

5. This email confirmed that on February 23, DISH experienced a cybersecurity incident. In the email DISH stated that on February 27, DISH it "became aware that certain data was extracted from our IT systems as part of this incident" (the "Data Breach"). In response, the company says that it began an investigation which is ongoing.

6. According to news reports, the incident was actually a "ransomware attack on the Corporation's employees, customers, business, operations or financial results" carried out by a Russian ransomware gang by the name of "Black Basta."[3]

[1] https://www.bleepingcomputer.com/news/security/dish-network-confirms-ransomware-attack-behind-multi-day-outage/

[2] https://www.sec.gov/ix?doc=/Archives/edgar/data/0001001082/000155837023002254/dish-20230223x8k.htm

[3] https://www.bleepingcomputer.com/news/security/dish-network-confirms-ransomware-attack-behind-multi-day-outage/

7. On information and belief, DISH has not yet formally notified all impacted individuals (consumers or employees) and has not yet notified state Attorney Generals and other reporting authorities about the full impact of the Data Breach.

8. Upon information and belief, information compromised in the Data Breach included highly sensitive data that represents a gold mine for a ransomware gang like Black Basta. On information and belief, the Data Breach included customer and employee names, dates of birth, addresses, email addresses, Social Security numbers, driver's license or state identification card numbers, credit card or account information (collectively the "Private Information") and additional personally identifiable information ("PII") that DISH collected and maintained.

9. Armed with the Private Information accessed in the Data Breach, and a head start, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. Therefore, Plaintiff and Class Members will show that they have suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

11. Plaintiff brings this class action lawsuit to address DISH's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

12. The potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to DISH, and thus DISH was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

13. DISH and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had DISH properly monitored its networks, it would have discovered the Data Breach sooner.

14. Plaintiff's and Class Members' identities are now at risk because of DISH's negligent conduct since the Private Information that DISH collected and maintained is now likely in the hands of data thieves and unauthorized third-parties.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to DISH's data security systems, future annual audits, and adequate credit monitoring services funded by DISH.

PARTIES

17. Plaintiff Susan Owen-Brooks is, and at all times mentioned herein was, an individual citizen of the State of North Carolina residing in the City of Ahoskie in Hertford County. Plaintiff Owen-Brooks was informed by DISH that her information was compromised in the Data Breach.

18. Defendant DISH, a satellite television company, is a Nevada corporation with its principal place of business in Englewood, Colorado.

JURISDICTION AND VENUE

19. The 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. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant DISH. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over the Defendant because its principal place of business is in this District, and the computer systems implicated in this Data Breach are likely based in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. DISH has harmed some Class Members residing in this District.

DISH COLLECTS HIGHLY SENSTIVE CUSTOMER INFORMATION

22. DISH is a satellite television provider based in Englewood, Colorado. Founded in 1995, DISH quickly grew to be one of the biggest satellite television providers in the United States, serving nearly 10 million customers across the country. DISH employs more than 14,000 people in the United States and generates over $2 billion in annual revenue.

23. As a condition of receiving services and/or employment, DISH requires that its customers and employees entrust it with highly sensitive personal information. In the ordinary

course of receiving service from DISH, customers, for example, are required to provide sensitive personal and private information, such as:

- Names;
- Dates of birth;
- Addresses
- Email addresses
- Social Security numbers;
- Driver's license numbers and information;
- Financial account information; and
- Payment card information.

24. DISH uses this information, *inter alia*, to provide services and collect payment.

25. In its privacy policy, DISH promises its customers that it will not share this Personal Information with third parties except in specified, defined circumstances such as service providers and mailing list partners.[4]

26. In its privacy policy, DISH also assures customers, "We take information security seriously. We use commercially reasonable efforts to protect information we collect and maintain against loss; misuse; and unauthorized access, disclosure, alteration, or destruction."[5]

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, DISH assumed legal and equitable duties and knew or should have

[4] https://www.dish.com/privacy-policy (last visited May 8, 2023).

[5] *Id.*

known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

28. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

29. Plaintiff and Class Members relied on DISH to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

DISH'S DATA BREACH

30. Plaintiff was a customer of DISH. As a mandatory part of being a customer, DISH collected names, addresses, Social Security number, financial information, and driver's license information for Plaintiff.

31. On or about February 25, 2023, news reports circulated that for the previous 24 hours DISH had been experiencing a "widespread outage [that] affect[ed] Dish.com, Dish Anywhere app as well as several websites and networks owned by the corporation. Customers also suggest[ed] the company's call center phone numbers are unreachable."[6] Later reports indicated that the outages also effected Boost Mobile, which is a subsidiary of DISH.[7]

32. According to public announcements by DISH, including a Form 8-K filed with the SEC, the company experienced a cybersecurity incident on February 23, 2023. The unauthorized

[6] https://www.bleepingcomputer.com/news/security/dish-network-goes-offline-after-likely-cyberattack-employees-cut-off/

[7] https://www.bleepingcomputer.com/news/security/dish-network-confirms-ransomware-attack-behind-multi-day-outage/

individual or individuals, believed to have been the Black Basta ransomware gang according to news reports, accessed a cache of highly sensitive PII.[8]

33. Although DISH has not divulged to Plaintiff, the Class, or the public the exact information that was accessed, given the widespread nature of the breach and the fact that DISH collects all of this data, Plaintiff believes that it includes or may include: individuals' names, addresses, telephone numbers, email addresses, Social Security numbers, dates of birth, driver's license numbers, bank account data, and credit card numbers.

34. DISH has confirmed to customers that the Data Breach included personal information and says that "[t]he forensic investigation and assessment of the impact of this incident is ongoing." It promises customers that it will let "impacted customers know" what personal information was compromised.[9] However, as of March 22, 2023, DISH told its customers that it was still working to restore all of its "customer experiences … but it will take a little time before our systems are fully restored."[10]

35. DISH had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

36. As of the filing of this action, DISH has not provided specific notice to the vast majority of its effected customers and has provided no information regarding exactly what PII was

[8] https://www.bleepingcomputer.com/news/security/dish-network-confirms-ransomware-attack-behind-multi-day-outage/

[9] https://www.dish.com/statement

[10] *Id.*

stolen. Nevertheless, after learning about the security incident, Plaintiff discovered that over $200 had been improperly removed from her DISH account without her consent. She contacted DISH and a company representative confirmed to her that her PII was part of the Data Breach.

37. Plaintiff and Class Members provided their Private Information to DISH with the reasonable expectation and mutual understanding that DISH would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of security breaches.

38. DISH's data security obligations were particularly important given the substantial increase in cyberattacks and ransomware attacks in particular.

39. DISH knew or should have known that its electronic records would be targeted by cybercriminals.

DISH FAILED TO COMPLY WITH FTC GUIDELINES

40. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

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

detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

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

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. The FTC has also long warned companies about the possibility of ransomware attacks in particular, providing *inter alia* specific guidance to companies regarding how to avoid such attacks, and going so far as to provide a "Ransomware Quiz" for companies to use to identify ransomware.[11]

45. On information and belief, DISH failed to properly implement basic data security practices. DISH's failure to employ reasonable and appropriate measures to protect against

[11] https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/ransomware; https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz/ransomware; https://www.ftc.gov/business-guidance/blog/2020/12/ransomware-prevention-update-businesses

unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

46. DISH was at all times fully aware of its obligation to protect the PII of its customers.

DISH FAILED TO COMPLY WITH INDUSTRY STANDARDS

47. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

48. Like the FTC, law enforcement and industry leaders have long warned of the dangers regarding ransomware attacks. In 2021 alone, the FBI's Internet Crime Complaint Center received 3,729 complaints regarding ransomware attacks. "Those attacks accounted for financial losses of $49.2 million."[12] However, that number may be too small because according to the U.S. Treasury's Financial Crimes Enforcement Network analysis, in 2021 there were $1.2 billion in Bank Secrecy Act filings for ransomware-related incidents, up from just $416 million in similar filings in 2020.[13]

49. Among other things, security experts have noticed an increase in recent years of so called "Double Extortion:"

> In the past, ransomware was about attackers encrypting information found on a system and then demanding a ransom in exchange for a decryption key. With double extortion, attackers also exfiltrate the data to a separate location. There, it can be used for other purposes,

[12] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

[13] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

> including leaking the information to a public website if a payment is not received.[14]

50. According to news reports, Double Extortion is what happened to DISH.

51. Several best practices have been identified that a minimum should be implemented by businesses like DISH, 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. Various experts have provided numerous recommendations regarding how to prevent Double Extortion ransomware attacks. These include "preventive data encryption and preventive data deception" among other things.[15]

52. Upon information and belief, Defendant failed to follow some or all of these industry best practices, including a failure to implement multi-factor authentication.

53. Other best cybersecurity practices that are standard in the industry 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; and training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

54. Upon information and belief, Defendant failed to meet the minimum standards of any of the following frameworks, thereby opening the door to the cyber incident and causing the

---

[14] *Id.*

[15] http://people.se.cmich.edu/liao1q/papers/ransomwareportfolio.pdf

Data Breach: 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.

DISH'S SECURITY OBLIGATIONS

55. DISH breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. DISH's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees in the proper handling of emails containing PII;

e. Failing to fully comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTCA; and

f. Failing to adhere to industry standards for cybersecurity.

56. As the result of computer systems in need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the

cyberattack, DISH negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

57. Accordingly, as outlined below, Plaintiff's and Class Members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft. Plaintiff and the Class Members also lost the benefit of the bargain they made with DISH.

DATA BREACHES, FRAUD, AND IDENTITY THEFT

58. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.[16] Exposure of personal information that a consumer wishes to keep private, may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment. Consumers loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

59. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's

[16] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf. (last visited May 8, 2023).

identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

60. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

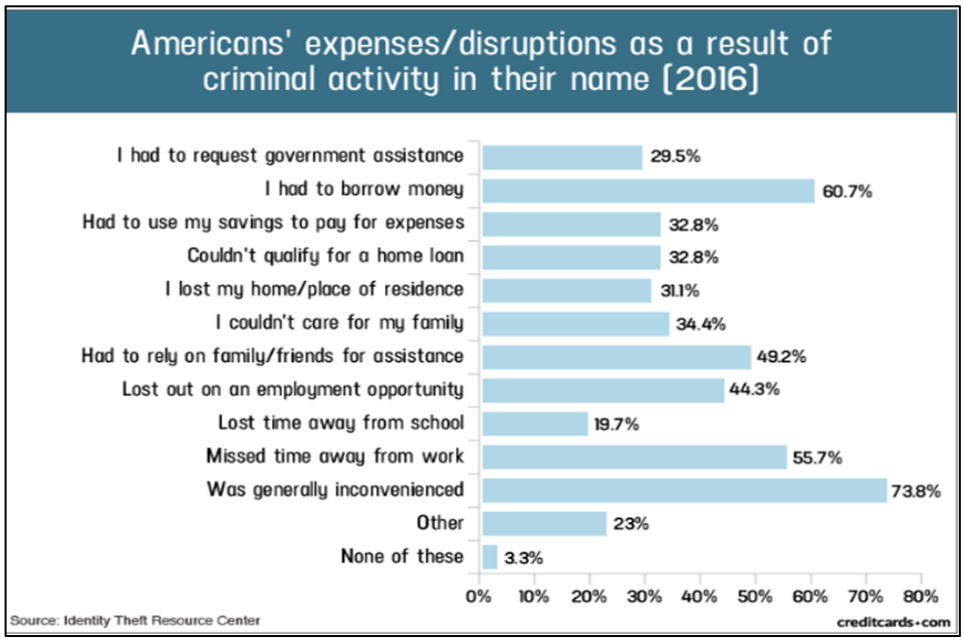
61. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

62. Identity thieves can also use Social Security numbers and driver's license numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's

[17] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited May 8, 2023).

name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

63. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[18]



64. Moreover, theft of Private Information is also gravely serious. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that Private Information has considerable market value.

65. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information

[18] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited May 8, 2023).

and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[19]

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

66. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

67. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

68. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

69. Plaintiff's Private Information, including sensitive PII, was compromised as a direct and proximate result of the Data Breach.

[19] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited May 8, 2023).

70. As a direct and proximate result of DISH's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

71. As a direct and proximate result of DISH's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

72. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

73. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

74. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

75. The information that DISH maintains regarding Plaintiff and Class Members, when combined with publicly available information, would allow nefarious actors to paint a complete financial and personal history of Plaintiff and Class Members.

76. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to DISH was intended to be used by DISH to fund adequate security of DISH's computer property and

protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

77. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

78. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims have suffered or will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

79. Indeed, as noted, Plaintiff's DISH account was zeroed out after the Data Breach when she previously had over $200 in that account. This is consistent with news reports stating that DISH's payment systems were compromised by the attack.

80. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of DISH, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

81. As a direct and proximate result of DISH's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and either have suffered harm or are at an imminent and increased risk of future harm.

CLASS ALLEGATIONS

82. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and on behalf of all other persons similarly situated (the "Class").

83. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

North Carolina Subclass

All residents of North Carolina who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

84. Excluded from each of the above Classes are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

85. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

86. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

87. Numerosity**.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of nearly 10 million customers of DISH whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through DISH's records, Class Members' records, self-identification, and other means.

88. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether DISH engaged in the conduct alleged herein;

b. Whether DISH's conduct violated the North Carolina Deceptive Trade Practices Act, invoked below;

c. When DISH first learned of the Data Breach and whether its response was adequate;

d. Whether DISH unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

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

f. Whether DISH's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether DISH's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether DISH owed a duty to Class Members to safeguard their Private Information;

i. Whether DISH breached its duty to Class Members to safeguard their Private Information;

j. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

k. Whether DISH had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether DISH breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether DISH knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of DISH's misconduct;

o. Whether DISH's conduct was negligent;

p. Whether DISH's conduct was *per se* negligent;

q. Whether DISH was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and are entitled to other monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

89. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

90. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

91. Predominance. DISH has engaged in a common course of conduct toward Plaintiff and Class Members, in that, on information and belief, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from DISH's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

92. 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 Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore 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, which would establish incompatible standards of conduct for DISH. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

93. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). DISH has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

94. Finally, all members of the proposed Class are readily ascertainable. DISH has access or will have access to Class Members' names and addresses affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NORTH CAROLINA SUBCLASS)

95. Plaintiff restates and realleges the allegations in paragraphs 1-94 as if fully set forth herein.

96. DISH knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

97. DISH's duty included a responsibility to implement processes by which they could detect and analyze a breach of its security systems in an expeditious period of time and to give prompt notice to those affected in the case of a cyberattack.

98. DISH knew, or should have known, of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. DISH was on notice because on information and belief it knew or should have known that utility entities are an attractive target for cyberattacks.

99. DISH owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. DISH's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting. and protecting Private Information in its possession;

b. To protect Private Information using reasonable and adequate security procedures and systems that are compliant with the industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the North Carolina Deceptive Trade Practices Act;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and the Class Members of a data breach and to disclose the types of information compromised.

100. DISH's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant was bound by industry standards to protect confidential Private Information.

101. Plaintiff and the Class Members were foreseeable and probable victims of any inadequate security practices and DISH owed them a duty of care not to subject them to an unreasonable risk of harm.

102. DISH, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within DISH's possession.

103. DISH, by its actions and/or omissions, breached its duty of care by failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

104. DISH, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

105. DISH breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards; and

d. Allowing unauthorized access to Class Members' Private Information.

106. DISH had a special relationship with Plaintiff and the Class Members. Plaintiff's and the Class Members' willingness to entrust DISH with their Private Information was predicated on the understanding that DISH would take adequate security precautions. Moreover, only DISH

had the ability to protect its systems (and the Private Information that it stored on them) from attack.

107. DISH's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

108. As a result of DISH's ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members are unable to take all the necessary precautions to mitigate damages by preventing future fraud.

109. DISH's breaches of duty caused a foreseeable risk of harm to Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

110. As a result of DISH's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

111. DISH also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and the Class Members' Private Information and promptly notify them about the Data Breach.

112. As a direct and proximate result of DISH's negligent conduct, Plaintiff and the Class Members have suffered damages and are at imminent risk of further harm.

113. The injury and harm that Plaintiff and the Class Members suffered was reasonably foreseeable.

114. The injury and harm that Plaintiff and the Class Members suffered was the direct and proximate result of DISH's negligent conduct.

115. Plaintiff and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

116. In addition to monetary relief, Plaintiff and the Class Members also are entitled to injunctive relief requiring DISH to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NORTH CAROLINA SUBCLASS)

117. Plaintiff restates and realleges the allegations in paragraphs 1-116 as if fully set forth herein.

118. Pursuant to Section 5 of the FTCA, DISH had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information, including PII, of Plaintiff and Class Members.

119. Upon information and belief, DISH breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

120. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

121. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures

to protect Private Information. The FTC publications described above, and the industry standard data and cybersecurity measures, also form part of the basis of DISH's duty in this regard.

122. DISH violated the FTCA by failing to use reasonable measures to protect Private Information of Plaintiff and Class Members and not complying with applicable industry standards, as described herein.

123. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to DISH's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Private Information.

124. DISH's violations of the FTCA constitutes negligence *per se*.

125. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to DISH's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

126. As a direct and proximate result of DISH's negligence *per se*, Plaintiff and the Class have suffered and continue to suffer injuries and damages arising from the unauthorized access of their Private Information (including PII) because of the Data Breach, including but not limited to, damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

127. DISH breached its duties to Plaintiff and the Class Members under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

128. As a direct and proximate result of DISH's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

129. In addition to monetary relief, Plaintiff and Class Members also are entitled to injunctive relief requiring DISH to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and the Class Members.

COUNT III
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NORTH CAROLINA SUBCLASS)

130. Plaintiff restates and realleges the allegations in paragraphs 1-129 as if fully set forth herein.

131. Plaintiff and Class Members entered into a valid and enforceable contract when they paid money to DISH in exchange for services, which included promises to secure, safeguard, protect, keep private, and not disclose Plaintiff's and Class Members' Private Information.

132. DISH's Privacy Policy memorialized the rights and obligations of DISH and its customers. This document was provided to Plaintiff and Class Members in a manner and during a time where it became part of the agreement for services.

133. In the Privacy Policy, DISH commits to using commercially reasonable efforts to protect the privacy and security of personal information against unauthorized access and it promises to only share customer information with third-parties in specified circumstances.

134. Plaintiff and Class Members fully performed their obligations under their contracts with DISH.

135. DISH did not secure, safeguard, protect, and/or keep private Plaintiff's and Class Members' PII and/or disclosed it to third parties, and therefore DISH breached its contract with Plaintiff and Class Members.

136. DISH allowed third parties to access, copy, and/or transfer Plaintiff's and Class Members' PII, without permission, and, therefore, DISH breached the Privacy Policy with Plaintiff and Class Members.

137. DISH's failure to satisfy its confidentiality and privacy obligations resulted in DISH providing services to Plaintiff and Class Members that were of a diminished value.

138. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein.

139. In addition to monetary relief, Plaintiff and Class Members are entitled to injunctive relief requiring DISH to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NORTH CAROLINA SUBCLASS)

140. Plaintiff restates and realleges the allegations in paragraphs 1-139 as if fully set forth herein.

141. This Count is pleaded in the alternative to Count III above.

142. Plaintiff and Class Members formed an implied contract with DISH for its services through their collective conduct, including by Plaintiff and Class Members paying for services and/or paying for labor or goods from DISH.

143. Through DISH's performance of, and/or sale of labor and goods and services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with DISH's policies, practices, and applicable law.

144. As consideration, Plaintiff and Class Members paid money to DISH for its services, labor and/or goods and turned over valuable PII to Defendant. Accordingly, Plaintiff and Class Members bargained with DISH to securely maintain and store their Private Information.

145. DISH violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information and by disclosing it for purposes not required or permitted under the contracts or agreements.

146. Plaintiff and Class Members have been damaged by DISH's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
VIOLATION OF NORTH CAROLINA DECEPTIVE TRADE PRACTICES ACT
(ON BEHALF OF PLAINTIFF OWEN-BROOKS
AND THE NORTH CAROLINA SUBCLASS)

147. Plaintiff Owen-Brooks restates and realleges the allegations in paragraphs 1-146 as if fully set forth herein.

148. As fully alleged above, DISH engaged in unfair and deceptive acts and practices in violation of the North Carolina Deceptive Trade Practices Act, N.C. Gen. Stat. §75-1.1.

149. North Carolina law declares unlawful all "unfair or deceptive acts or practices in or affecting commerce." N.C. Gen. Stat. § 75-1.1.

150. "Commerce" is defined broadly as any business activity other than "professional services rendered by a members of a learned profession." *Id.*

151. DISH's sale of satellite television services constitutes commerce under North Carolina law.

152. DISH engaged in unlawful, unfair, and deceptive acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by Plaintiff Owen-Brooks and the North Carolina Subclass in violation of N.C. Gen. Stat. § 75-1.1, including but not limited to the following:

a. DISH misrepresented material facts by representing that, in connection with its provision of services, it would maintain adequate data privacy and security practices and procedures to safeguard the Private Information from unauthorized disclosure, release, data breach, and theft;

b. DISH omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for the North Carolina Subclass's Private Information;

c. DISH engaged in unfair, unlawful, and deceptive acts and practices as part of its provision of commercial services by failing to maintain the privacy and security of the North Carolina Subclass's Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, including the FTCA, resulting in the Data Breach; and

d. DISH engaged in unlawful, unfair, and deceptive acts and practices with respect to its provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect the North Carolina

Subclass's Private Information from further unauthorized disclosure, release, data breach, and theft.

153. The above unlawful, unfair, and deceptive acts and practices on the part of DISH were immoral, unethical, oppressive, and unscrupulous. These acts and practices caused substantial injury or will cause substantial injury to individuals that they could not reasonably avoid. This substantial injury outweighs any benefits to consumers.

154. DISH knew, or should have known, that its computer systems and data security practices were inadequate to safeguard the North Carolina Subclass's Private Information and that risk of a data breach or theft was highly likely. DISH's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the North Carolina Subclass.

155. As a direct and proximate result of DISH's deceptive acts and practices, Plaintiff Owen-Brooks and members of the North Carolina Subclass suffered an ascertainable loss, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

156. Individuals injured by unfair or deceptive acts or practices are entitled to treble damages. N.C. Gen. Stat. § 75-16. Thus, Plaintiff Owen-Brooks and the North Carolina Subclass seek and request treble damages, attorney fees, expenses, and costs, and injunctive relief pursuant to N.C. Gen. Stat. §75-1.1, *et seq*.

COUNT VI
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NORTH CAROLINA SUBCLASS)

157. Plaintiff restates and realleges the allegations in paragraphs 1-156 as if fully set forth herein.

158. This Count is pleaded in the alternative to Counts III and IV above.

159. Plaintiff and Class Members conferred a benefit on DISH by paying for products and services that should have included data and cybersecurity protection to protect their Private Information. DISH did not provide such protection and Plaintiff and Class Members did not receive such protection.

160. DISH has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to DISH's conduct alleged herein, it would be unjust and inequitable under the circumstances for DISH to be permitted to retain the benefit of its wrongful conduct.

161. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from DISH, and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by DISH from its wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation may be created.

COUNT VII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS OR ALTERNATIVELY THE NORTH CAROLINA SUBCLASS)

162. Plaintiff restates and realleges the allegations in paragraphs 1-161 as if fully set forth herein.

163. 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 and state statutes described in this Complaint.

164. DISH owes a duty of care to Plaintiff and Class Members which required it to adequately secure Private Information.

165. DISH still possesses Private Information regarding Plaintiff and Class Members.

166. Plaintiff alleges that DISH's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continues to suffer injury as a result of the compromise of her and their Information and remain at imminent risk that further compromises of her and their Private Information will occur in the future.

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

a. DISH owes a legal duty to secure customers' Private Information and to timely notify individuals of a data breach under the common law and Section 5 of the FTCA;

b. DISH's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures

and practices appropriate to the nature of the information to protect individuals' Private Information; and

c. DISH continues to breach this legal duty by failing to employ reasonable measures to secure individuals' Private Information.

168. This Court also should issue corresponding prospective injunctive relief requiring DISH to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order DISH to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order DISH to comply with its explicit or implicit contractual obligations and duties of care, DISH must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on DISH's systems, on a periodic basis, and ordering DISH to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised hackers cannot gain access to other portions of DISH's systems;

v. conducting regular database scanning and securing checks;

vi. 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; and

vii. meaningfully educating its users about the threats they face resulting from the loss of their Private Information to third parties, as well as the steps DISH's customers must take to protect themselves.

169. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury and will lack an adequate legal remedy to prevent further injury in the event of, another data breach at DISH. The risk of another such breach is real, immediate, and substantial. If another breach at DISH occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

170. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to DISH if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other related damages. On the other hand, the cost of DISH's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and DISH has a preexisting legal obligation to employ such measures.

171. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

DISH, thus preventing the additional future injury to Plaintiff and Class Members whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes described above, seeks the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Classes requested herein;

b. Judgment in favor of Plaintiff and the Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Plaintiff and Classes as requested herein;

d. An order instructing DISH to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring DISH to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and the Classes awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law, and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: May 9, 2023.

Respectfully submitted,

By: */s/ Mark E. Saliman*
Mark E. Saliman
SALIMAN LAW, LLC
3900 E. Mexico Ave., Suite 300
Denver, CO 80210
Tel: (720) 907-7652
E: mark@salimanlaw.com

Mason A. Barney (*admission to be requested*)
Steven D. Cohen (*admission to be requested*)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: scohen@sirillp.com

Counsel for Plaintiff and the Proposed Class

ClassAction.org