UNITED STATES DISTRICT COURT
DISTRICT OF MONTANA
BUTTE DIVISION

JOHN DOE, JEAN ANN SMITH, and JANICE STEWART *individually and on behalf of all others similarly situated*, Plaintiff, v. SNOWFLAKE, INC., Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs John Doe, Jean Ann Smith, and Janice Stewart ("Plaintiffs"), individually and on behalf of the Class of similarly situated persons (defined below), allege the following against Defendant Snowflake, Inc. ("Snowflake" or "Defendant"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by counsel as to all other matters:

SUMMARY OF THE CASE

1. This action arises from Defendant's failure to secure the personal identifiable information ("PII")[1] of Plaintiffs and the members of the proposed

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,"

Class, where Plaintiffs and Class Members are current and former employees, customers, and others who provided their PII to Snowflake's clients, who in turn used Snowflake's cloud-based data hosting platform to share and maintain PII.

2. Snowflake is a cloud storage service with nearly 20% of the data hosting market share and is used by 9,437 customers, including globally ranked, industry leading companies such as Adobe, AT&T, Kraft Heinz, Mastercard, HP, Nielsen, Novartis, PepsiCo, Siemens, Advance Auto Parts, Ticketmaster, Santander Bank, Anheuser-Busch, Allstate Insurance, Mitsubishi, Neiman Marcus, Progressive, State Farm and NBC Universal among many others.[2]

3. According to Mandiant, starting in or about mid-April 2024, an unauthorized party began to use access Snowflake customer credentials, acquired using infostealer malware, to access the Snowflake platform and to target and acquire the unencrypted PII stored thereon (the "Data Breach").[3] The threat actor continued to access the Snowflake platform until approximately May 22, 2024, when

including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Seraiu Gatlan, *Advance Auto Parts stolen data for sale after Snowflake attack*, BLEEPING COMPUTER (June 5, 2024), https://www.bleepingcomputer.com/news/security/advance-auto-parts-stolen-data-for-sale-after-snowflake-attack/; Symmetry, *What We Know So Far about the Snowflake "Breach"*, https://www.symmetry-systems.com/blog/what-we-know-so-far-about-the-snowflake-breach/

[3] https://www.securityweek.com/snowflake-attacks-mandiant-links-data-breaches-to-infostealer-infections/

Snowflake was alerted to additional compromised customer accounts by Mandiant.[4]

4. Notably, many of the compromised access credentials had been acquired as early as 2020 and Snowflake could have prevented this Data Breach by requiring all accounts to regularly update their passwords to current standards, monitor infostealer marketplaces for compromised credentials and prevent access to the platform by these accounts until the compromised passwords had been updated accordingly. Moreover, Snowflake should have but did not require its clients to implement multi-factor authentication as a condition of accessing the platform. Had this basic security feature been required by Snowflake, none of the compromised account credentials could have been used to successfully access the platform. Snowflake could also have better monitored its systems to detect unusual activity or activity associated with unauthorized access, including by implementing IP filters and limiting access to its network environment to only necessary users.

5. Unfortunately for Plaintiffs and Class Members, Defendant failed to implement basic and expected data security practices appropriate to the vast amounts of PII stored on its platform and, as a consequence, records containing the PII of millions of individuals (with 560 million customers' records from Ticketmaster alone),[5] from over 165 organizations that used the Snowflake platform, were

[4] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

[5] https://techcrunch.com/2024/05/31/live-nation-confirms-ticketmaster-was-hacked-says-personal-information-stolen-in-data-breach/

accessed and acquired by the threat actors during the Data Breach.[6]

6. While the records exfiltrated in the Data Breach vary according to the organization using the Snowflake platform, the unlawfully accessed PII includes, Social Security numbers, names, dates of birth, email addresses, physical addresses, telephone numbers, driver's license information, payroll information, financial account information, and other confidential personal data.[7]

7. Soon after they exfiltrated the PII from Snowflake's platform, the threat actors attempted to extort payments from Snowflake's clients and began publishing samples of the stolen consumer PII on dark web marketplaces for sale to identity thieves and fraudsters. According to Mandiant, additional extortion attempts were reported by Snowflake's clients as recently as June 13, 2024.[8] Additional consumer PII continues to be published to dark web marketplaces in large batches, including a batch of 1 million Ticketmaster customer records released on June 21, 2024.[9]

8. As a result of the Data Breach, Plaintiffs and millions of Class Members were injured and the confidentiality of their PII was destroyed and commoditized by data thieves. Plaintiffs and Class Members were entitled to, and did, expect a

[6] *See* Mandiant initial Report, available at https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
[7] https://www.malwarebytes.com/blog/news/2024/06/advance-auto-parts-customer-data-posted-for-sale; https://www.securityweek.com/santander-employee-data-breach-linked-to-snowflake-attack/; *see also supra*, n. 2.
[8] https://www.cybersecuritydive.com/news/snowflake-customer-attacks-what-we-know/719056/
[9] https://www.malwarebytes.com/blog/news/2024/06/first-million-breached-ticketmaster-records-released-for-free

sophisticated data hosting company to take reasonable steps to prevent unauthorized access to their PII. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard PII from unauthorized access and by failing to take necessary steps to prevent unauthorized disclosure of that information. Defendant's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its actions and omissions.

9. Further exacerbating Plaintiffs' injuries, Defendant has offered insufficient assurances that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its security practices, sufficiently blacklisted all compromised credentials and limited access to its network environment or dedicated sufficient resources and staff to avoid a similar breach of its network in the future.

10. Plaintiffs and Class Members would not have entrusted their confidential PII to companies that utilized Snowflake's platform had they known that Snowflake would fail to implement proper password standards, fail to require its clients to regularly change passwords, fail to monitor dark web marketplaces for compromised access credentials, and fail to monitor their network for suspicious activity or limit access to necessary users.

11. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future 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' 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.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Through this Complaint, Plaintiffs seek to remedy the harms resulting from the Data Breach on behalf of themselves and all similarly situated individuals whose PII was accessed.

14. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

15. 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 about 180,000 people, many of whom, including Plaintiffs, have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

16. The Court has general personal jurisdiction over Snowflake because its headquarters and principal place of business is located in Bozeman, Montana.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because Snowflake's principal place of business is located in this District and the acts or omissions giving rise to Plaintiffs' claims emanated in this District.

PARTIES

18. Plaintiff John Doe is, and at all relevant times has been, a resident and citizen of Michigan, where he intends to remain.

19. Plaintiff Jean Ann Smith Doe is, and at all relevant times has been, a resident and citizen of Florida, where she intends to remain.

20. Plaintiff Janice Stewart is, and at all relevant times has been, a resident and citizen of Florida, where she intends to remain.

21. Defendant Snowflake is a Delaware corporation with its headquarters and principal place of business located at 106 E. Babcock Street, Suite 3A, Bozeman, Montana 59715.

FACTUAL ALLEGATIONS

A. The Data Breach

22. From about mid-April 2024, a cybercriminal group known as "ShinyHunters" began a prolonged series of hacks into Snowflake's network and ultimately accessed, obtained, and exfiltrated hundreds of millions of detailed consumer records containing the PII of Plaintiffs and Class Members, including their Social Security numbers, names, dates of birth, email addresses, physical addresses, telephone numbers, driver's license information, payroll information, financial account information, and other confidential PII.

23. The attackers managed to gain access to the Snowflake platform on which Defendant's clients stored PII by using stolen access credentials from as early as 2020 and which had long been made available on dark web marketplaces.[10] Defendant knew that its clients stored unencrypted PII on its platform and knew that such data was a motivating target for cyberattackers who monetize the information or use it themselves to commit fraud and identity theft.

24. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's platform was a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

25. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and

[10] https://www.wired.com/story/epam-snowflake-ticketmaster-breach-shinyhunters/

Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[11]

26. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that"*[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies*. They breach networks, use specialized tools to maximize damage, *leak corporate information on dark web portals*, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[12]

27. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that *"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data* if they refuse to pay and publicly naming and shaming victims as secondary forms of

[11] FBI, *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations* (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002

[12] ZDNet, *Ransomware mentioned in 1,000+ SEC filings over the past year* (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/

extortion."[13]

28. Companies should treat these attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[14] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[15] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[16]

29. Despite this knowledge, and the knowledge that access credential theft is an increasingly common attack vector, Defendant failed to implement basic security features that would detect and prevent such an attack. Indeed, cybersecurity experts have been increasingly vocal about the increase in infostealer attacks and the need to protect against them.[17]

---

[13] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf

[14] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[15] *Id*.

[16] *Id*.

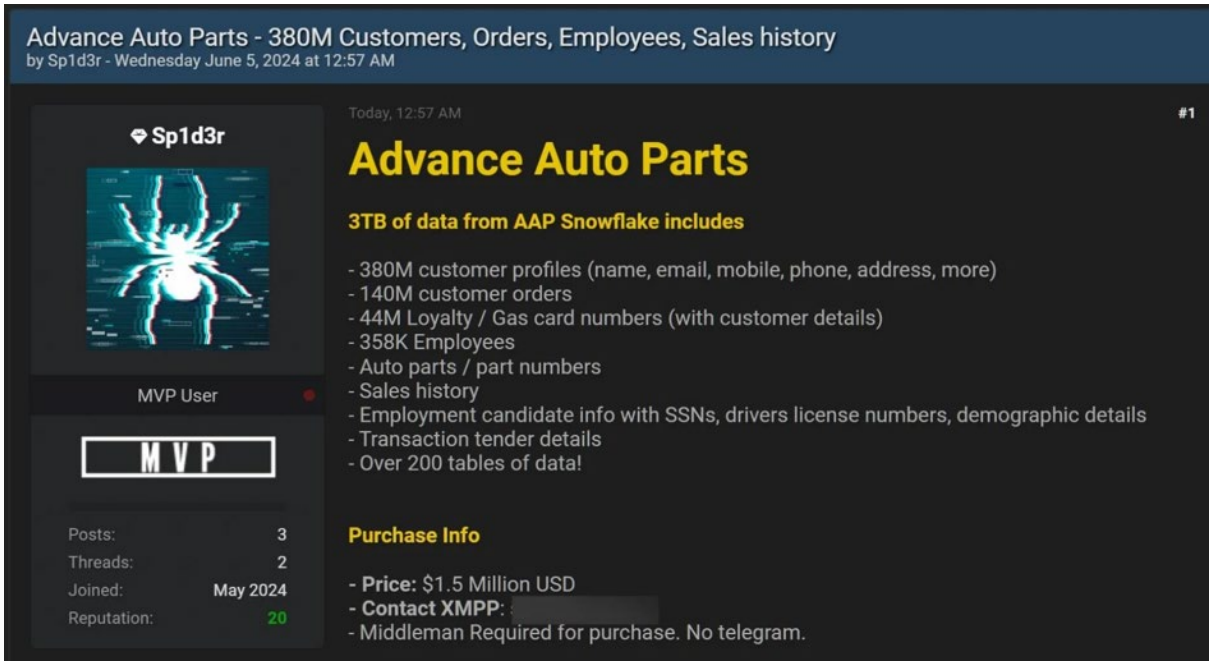
[17] https://blog.sekoia.io/overview-of-the-russian-speaking-infostealer-ecosystem-the-logs/#h-logs-marketplaces

30. Ultimately Defendant could have prevented this attack, which relied on the use of passwords compromised, in some case, four years prior by, *inter alia*: 1) requiring all accounts to regularly update their passwords to current industry standards; 2) monitoring infostealer marketplaces for compromised credentials and prevent access to the platform by these accounts; 3) requiring its clients to implement multi-factor authentication as a condition of accessing the platform; 4) requiring its client to encrypt data on its platform; 5) monitoring its network to detect unusual activity or activity associated with unauthorized access, including by implementing IP filters; and 6) limiting access to its network environment to only necessary users.

31. Given that Defendant was storing the unencrypted PII of hundreds of millions of individuals, Defendant could and should have implemented all of the above measures to prevent and detect the Data Breach.

32. Unfortunately for Plaintiffs' and Class Members' their PII has been posted for sale on the dark web by a known cybercriminal who uses the handle "Sp1d3r."[18]

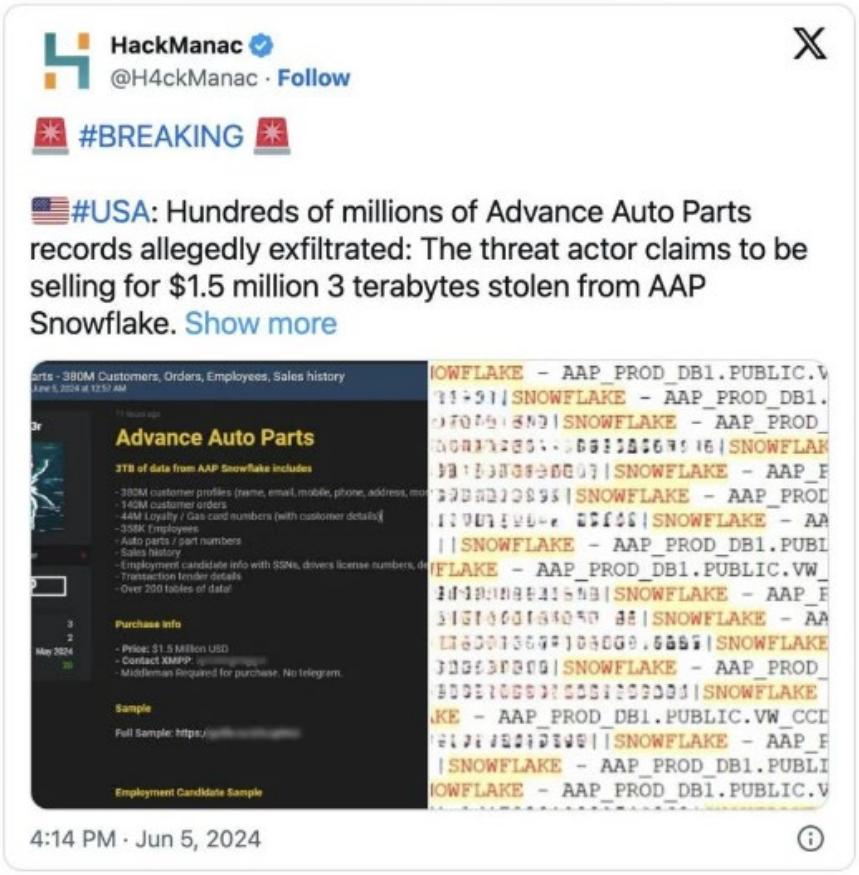
[18] *Id*.



[19]

33. The leaked material contains multiple references to "SNOWFLAKE," showing that the PII affiliated with Snowflake's customers (such as Advance Auto Parts) was stolen from Snowflake's platform.[20]

[19] *Id.*
[20] *Id.*



[21]

34. On June 21, 2024, Sp1d3r posted another batch of one million Ticketmaster customer records, this time offering the credit card details of these customers for free to anyone willing to download the dataset.

[21] *Id.*

35. As evidenced by the Data Breach and subsequent posting of Class Member data on the dark web, the PII contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

B. The Value of PII

36. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

37. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[22]

[22] *Shining a Light on the Dark Web with Identity Monitoring, IdentityForce*, Dec. 28, 2020, https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 18, 2024).

38. One example comes from when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[23]

39. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $2009.[24] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark

[23] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, https://www.armor.com/resources/blog/stolen-pii- ramifications- identity-theft-fraud-dark-web/ (last visited June 18, 2024).
[24] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal- data-sold-on-the-dark-web- how-much-it-costs/ (last visited June 18, 2024).

web.[25] Criminals can also purchase access to entire company data breaches.[26]

40. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

41. Because a person's identity is akin to a puzzle with multiple data points, 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 identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

42. 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 and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

[25] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is- selling-for-on-the-dark-web/ (last visited June 18, 2024).
[26] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous- browsing/in-the- dark/ (last visited June 18, 2024).

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

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

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

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

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

47. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package to collect that missing information.

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

49. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

50. The market for PII has continued unabated to the present, and in 2023 the number of reported data breaches in the United States increased by 78% over 2022, reaching 3205 data breaches.[28]

51. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[29] In fact, the

[28] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, INFOSECURITY MAGAZINE (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/ (last visited June 18, 2024); *see also* Identity Theft Resource Center, *2023 Data Breach Report*, https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited June 18, 2024).

[29] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[30] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[31]

52. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the dark web, where it is now available and holds significant value for the threat actors

C. Defendant Failed to Comply with Regulatory Requirements and Standards.

53. Federal and state regulators have established security standards and issued recommendations to prevent data breaches and the resulting harm to consumers and employees. There are a number of state and federal laws, requirements, and industry standards governing the protection of PII.

54. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain PII about a

[30] https://datacoup.com/; *see also* https://digi.me/what-is-digime/.

[31] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

resident of that state to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access.

55. 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

56. In October 2016, the FTC updated its publication, Protecting Private Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer 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 into 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.

57. 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. Defendant was at all times fully aware of its obligations to protect the PII on its networks yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

61. Defendant's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

D. Defendant Failed to Comply with Industry Practices.

62. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[32] All organizations collecting and handling PII, such as Defendant, are strongly encouraged to follow these controls.

63. Several best practices have been identified that a minimum should be implemented by data management companies like Defendant, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[33]

[32] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited June 18, 2024).
[33] *See* Center for Internet Security, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited June 18, 2024).

64. Defendant failed to follow these and other industry standards to adequately protect the PII of Plaintiffs and Class Members.

E. The Data Breach Caused Injury to Plaintiffs and Class Members and Will Result in Additional Harm Such as Fraud.

65. The ramifications of Defendant's failure to secure Plaintiffs' and Class Members' data are severe.

66. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[34] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[35]

67. Identity thieves can use PII, such as that of Plaintiffs and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

68. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend

[34] 17 C.F.R. § 248.201 (2013).
[35] *Id*.

numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[36]

69. The 2017 Identity Theft Resource Center survey[37] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

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

- 48.3% of respondents reported sleep disturbances;

[36] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited June 18, 2024).
[37] *Id*.

- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[38]

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[39]

72. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[38] *Id*.

[39] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

F. Plaintiffs and Class Members Suffered Damages.

73. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have already been harmed by the fraudulent misuse of their PII, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

74. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused via the sale of Plaintiffs' and Class Members' information on the Internet's black market;

c. the improper disclosure of their PII;

d. loss of privacy;

e. 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;

f. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

g. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

h. nominal damages.

75. Defendant continues to hold Plaintiffs' and Class Members' PII and Plaintiffs and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

G. Plaintiff Does's Experience

76. Plaintiff John Doe was a customer of Advance Auto Parts for several years preceding the Data breach and he provided his PII to Advance Auto and, in turn, to Snowflake when purchasing from Advance Auto.

77. Plaintiff Doe is very careful about sharing his sensitive PII. Plaintiff Doe stores any documents containing his PII in a safe and secure location.

78. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Doe's PII in its system. On June 24, 2024, Plaintiff Doe was alerted that his PII was published to the dark web, including his email address, name, phone number, and physical address and that Advance Auto was the source.

79. After receiving notice that his PII was published on the dark web, Plaintiff Doe received two phishing emails that used the email address he provided to Advance Auto and that he understands are intended to acquire additional information from him.

80. Plaintiff Doe made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant on mitigation activities in response to the Data Breach––valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

81. As a result of the Data Breach, Plaintiff Doe has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

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

85. Plaintiff Doe 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.

H. Plaintiff Smith's Experience

86. Plaintiff Jean Ann Smith was a customer of Ticketmaster, and she provided her PII to Ticketmaster and, in turn, to Snowflake when purchasing from Ticketmaster.

87. Plaintiff Smith is very careful about sharing her sensitive PII. Plaintiff Smith stores any documents containing her PII in a safe and secure location.

88. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Smith's PII in its system. On June 21, 2024, Plaintiff

Smith was alerted by Ticketmaster that her PII, including her name and payment card details were compromised in the Data Breach.

89. Soon after the Data Breach, Plaintiff Smith was notified of suspicious activity on her financial accounts and spent time closing two credit cards and debit card to prevent further misuse of her information.

90. Plaintiff Smith made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant on mitigation activities in response to the Data Breach--valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

91. As a result of the Data Breach, Plaintiff Smith has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized

third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

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

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

I. Plaintiff Stewart's Experience

96. Plaintiff Janice Stewart was a customer of Ticketmaster, and she provided her PII to Ticketmaster and, in turn, to Snowflake when purchasing from Ticketmaster.

97. Plaintiff Stewart is very careful about sharing her sensitive PII. Plaintiff Stewart stores any documents containing her PII in a safe and secure

location.

98. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Stewart's PII in its system. On June 21, 2024, Plaintiff Stewart was alerted by Ticketmaster that her PII, including her name and payment card details were compromised in the Data Breach.

99. Soon after the Data Breach, Plaintiff Stewart was notified that her PII had been published on the dark web.

100. Plaintiff Stewart made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant on mitigation activities in response to the Data Breach--valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

101. As a result of the Data Breach, Plaintiff Stewart has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

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

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

CLASS ALLEGATIONS

106. Plaintiffs bring this class action individually on behalf of themselves

and all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiffs seek certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Class:

> All persons residing in the United States whose PII was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

107. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which Defendant has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

108. Plaintiffs reserve the right to modify or amend the foregoing Class definitions before the Court determines whether certification is appropriate.

109. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, it has been reported that hundreds of millions of individuals' information was exposed in the Data Breach.

110. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII from unauthorized access and disclosure;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiffs' and Class Members' PII violated the FTC Act and/or state laws, and/or Defendant's other duties discussed herein;

d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiffs' and Class Members' PII;

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

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

h. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

i. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII;

j. Whether Defendant breached duties to protect Plaintiffs' and Class Members' PII;

k. Whether Defendant's actions and inactions alleged herein were negligent;

l. Whether Defendant was unjustly enriched by their conduct as alleged herein;

m. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages or other relief, and the measure of such damages and relief;

n. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

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

111. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

112. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

113. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs are an adequate representative of the Class and have no interests adverse to, or conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

114. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class Members are relatively small compared to the burden and expense that would be required to

individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

115. Injunctive and Declaratory Relief: Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

116. Likewise, particular issues are appropriate for certification under Rule 24(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this mater and the parties' interests therein. Such issues include, but are not limited to: (a) whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in preventing unauthorized access to its platform; (b) whether Defendant failed to adequately monitor and audit its data security systems; and (c) whether Defendant failed to take reasonable steps to safeguard the PII of Plaintiffs and Class Members.

117. All members of the proposed Class are readily ascertainable. Defendant has access to the names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach.

CAUSES OF ACTION

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

118. Plaintiffs re-allege and incorporate by reference all preceding paragraphs, as if fully set forth herein.

119. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

120. Defendant knew or reasonably should have known that the failure to exercise due care in the storing of the PII of Plaintiffs and the Class involved an unreasonable risk of harm, even if the harm occurred through the criminal acts of a third party.

121. Defendant 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. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Class in Defendant's possession was

adequately secured and protected.

122. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Class.

123. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

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

125. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for ensuring proper access credentials and encrypting PII stored on Defendant's systems.

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

127. Defendant was in an exclusive position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

128. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendant's possession might have

been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

129. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Class.

130. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class during the time the PII was within Defendant's possession or control.

131. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

132. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Class in the face of increased risk of theft.

133. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of

Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

134. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

135. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class 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 Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

136. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

137. Plaintiffs re-allege and incorporate by reference all preceding paragraphs, as if fully set forth herein.

138. Defendant had duties arising under the FTC Act to protect Plaintiffs' and Class Members' PII.

139. Pursuant to the Federal Trade Commission 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 Class Members' PII.

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

141. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

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

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

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

145. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Class)

146. Plaintiffs re-allege and incorporate by reference all preceding paragraphs, as if fully set forth herein.

147. On information and belief, Defendant entered into written contracts with its clients, including Ticketmaster and Advance Auto, to provide data hosting platform services.

148. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiffs and the Class and to timely and adequately notify them of the Data Breach.

149. On information and belief, these contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, the clients' patients and employees—Plaintiffs and Class Members—would be harmed.

150. Defendant breached the contracts entered into with its clients by,

among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

151. Plaintiffs and the Class were harmed by Defendant's breaches of contract, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

152. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

153. Plaintiffs re-allege and incorporate by reference all preceding paragraphs, as if fully set forth herein.

154. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiffs' retained data and commercialized and used Plaintiffs' and Class Members' PII for business purposes.

155. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for

the benefit of Plaintiffs and Class Members.

156. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

157. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

158. Defendant acquired the PII through inequitable means as it failed to disclose the inadequate data security practices previously alleged. If Plaintiffs and Class Members had known that Defendant would not fund adequate data security practices, procedures, and protocols to sufficiently monitor, supervise, and secure their PII, they would not have entrusted their Private Information to Defendant or obtained services from Defendant's clients.

159. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own benefit. Plaintiffs and Class

Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

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

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

162. As a direct and proximate result of Defendant's conduct, Plaintiffs and other Class Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required Plaintiffs' efforts to prevent from succeeding.

163. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant and all other relief allowed by law.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in Plaintiffs' favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMAND

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

Dated: June 27, 2024.

(signature on following page)

Respectfully submitted,

/s/ John Heenan

HEENAN & COOK, PLLC
1631 Zimmerman Trail
Billings, Montana 59102
TEL: (406) 839-9091

Gary M. Klinger (application for admission *pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Norman E. Siegel (pro hac vice forthcoming)
J. Austin Moore (pro hac vice forthcoming)
Jordan A. Kane (pro hac vice forthcoming)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100 (tel.)
siegel@stuevesiegel.com
moore@stuevesiegel.com
kane@stuevesiegel.com

Counsel for Plaintiffs and the Proposed Class