UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DAVID STEPHENS *and* KAITLYN STRAWN, *individually and on behalf of all others similarly situated*, Plaintiffs, v. CHICK-FIL-A, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs David Stephens and Kaitlyn Strawn (together, "Plaintiffs") bring this Class Action Complaint against Chick-fil-A, Inc. ("Chick-fil-A" or "Defendant") as individuals and on behalf of all others similarly situated (the "Class," as defined below; each member of the Class is a "Class Member") and allege, upon personal knowledge as to their own actions, upon their counsel's investigation, and upon information and belief as to all other matters, as follows:

JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy

exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one member of the class, including Plaintiff Stephens, is a citizen of a state different from Defendant.

2. This Court has personal jurisdiction over Defendant because its principal place of business is in this District; it regularly conducts business in Georgia; and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

3. Venue is proper under 18 U.S.C. § 1391 because Defendant's principal place of business is in this District.

NATURE OF THE ACTION

4. This class action arises out of a recent data breach involving Defendant Chick-fil-A, Inc., a leading fast-food chain in the United States.

5. According to Defendant, "[s]erving communities across the country with more than 2,400 restaurants, today customers can find Chick-fil-A inside airports, malls, college campuses, in the heart of Manhattan, and nestled among the thousands of busy streets connecting neighborhoods in 47 states and Washington D.C."[1]

6. Defendant is headquartered in Atlanta, Georgia, and it proudly

[1] https://www.chick-fil-a.com/about/who-we-are (last visited March 6, 2023).

promises "to leave Georgia better than we found it."[2] Defendant further claims to be "[d]eveloping a positive legacy in our own backyard."[3]

7. There is nothing positive about the recent failure to properly secure the sensitive, personal information of thousands of Chick-fil-A customers.

8. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including personal identifying information and financial account and payment data.

9. Current and former Chick-fil-A customers entrusted Defendant with sensitive, non-public personally identifiable information, without which Defendant could not perform its regular business activities with respect to Defendant's Chick-fil-A One program through Defendant's website and/or mobile App.

10. By obtaining, collecting, using, and deriving a benefit from the personally identifiable information of Plaintiffs and the Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

11. Upon information and belief, Defendant became aware of suspicious activity on its networks on or around January 4, 2023 (and likely earlier).

[2] *Id.*
[3] *Id.*

12. On January 4, 2023, Defendant posted on its official Twitter account the following statement:

https://twitter.com/ChickfilANews/status/1610743183272730624 (last visited March 5, 2023).

13. In an alert on its website on January 6, 2023, Defendant announced, "We are investigating suspicious activity on some customer accounts. We are committed to protecting customers' data and are working quickly to resolve the issue."[4] Upon information and belief, Defendant has since removed that alert from its website.

14. Defendant's customers took to social media immediately, expressing frustration with Defendant's inadequate response to the data breach.

15. For example, one customer voiced concerns over Defendant's inadequate customer service support:

[4] https://www.bleepingcomputer.com/news/security/chick-fil-a-investigates-reports-of-hacked-customer-accounts/ (last visited March 6, 2023).

16. It took Defendant two months to admit that someone successfully launched an "automated attack" against the company's website and app over the

course of more than two months, stealing customers' sensitive information.[5] On March 2, 2023, Defendant filed a security notice on the California Attorney General's website.[6]

17. In the Notice Letter, Defendant states that "[w]e recently identified suspicious login activity to certain Chick-fil-A One accounts."[7] Defendant further claims that "unauthorized parties launched an automated attack against our website and mobile application between December 18, 2022 and February 12, 2023 using account credentials (e.g., email addresses and passwords) obtained from a third-party source."[8] It states, "[b]ased on our investigation, we determined on February 12, 2023 that the unauthorized parties subsequently accessed information in your Chick-fil-A One account."[9]

18. In addition to email addresses and passwords, Defendant also claims that customers' sensitive personal information was exposed, including "name, email address, Chick-fil-A One membership number and mobile pay number, QR code, masked credit/debit card number, and the amount of Chick-fil-A credit (e.g.,

---

[5] https://www.bleepingcomputer.com/news/security/chick-fil-a-confirms-accounts-hacked-in-months-long-automated-attack/ (last visited March 6, 2023).
[6] The "Notice Letter," *available at* https://oag.ca.gov/system/files/2023-03-02%20-%20CFA%20-%20Individual%20Notification%20Template.pdf.
[7] *Id.*
[8] *Id.*
[9] *Id.*

e-gift card balance) on your account (if any). In addition, if saved to your account, the information may have included the month and day of your birthday, phone number, and address."[10] This sensitive information will be referred to herein as "PII."

19. It has been reported that the sustained attack on Defendant's systems allowed the threat actors to hack 71,473[11] Chick-fil-A accounts.[12] The automated attack against Defendant's website and mobile application between December 18, 2022, and February 12, 2023, will be referred to herein as the "Data Breach."

20. Defendant failed to adequately protect Plaintiffs' and the Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiffs' and the Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and the Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

---

[10] *Id.*

[11] Discovery will reveal the fuller extent of the data breach, and Plaintiffs reserve the right to amend or modify this Complaint to include additional facts obtained through discovery and further investigation.

[12] https://www.bleepingcomputer.com/news/security/chick-fil-a-confirms-accounts-hacked-in-months-long-automated-attack/ (last visited March 6, 2023).

21. Moreover, after learning of the Data Breach, Defendant waited *over two months* to notify Plaintiffs and the Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiffs and the Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

22. To make matters worse, Defendant's January 4, 2023, statement on Twitter explicitly assured customers that the fraudulent activity on their accounts was ***not*** the result of a compromise of Defendant's internal systems. This statement was either false or made by Defendant when it did not have sufficient facts to make such an assurance to concerned customers. Such a premature and factually inaccurate statement is negligent.

23. Because of Defendant's January 4, 2023, statement, Plaintiffs and the Class Members lost valuable time to take measures to protect and safeguard their data.

24. Not until almost two months later did Defendant contradict its initial public statement and admit to the Data Breach.

25. This confusing and botched series of announcements made by Defendant essentially rendered Defendant's March notice meaningless.

26. In breaching its duties to properly safeguard Plaintiffs' and the Class Members' PII and give timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

27. Plaintiffs brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and the Class Members; (ii) warn Plaintiffs and the Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

28. Defendant disregarded the rights of Plaintiffs and the Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure the PII of Plaintiffs and the Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and the Class Members was compromised through disclosure to an unknown and unauthorized third party.

Plaintiffs and the Class Members have a continuing interest in ensuring their information is and remains safe, and they seek injunctive and other equitable relief.

29. Plaintiffs and the Class Members have suffered injuries as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their 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.

30. Plaintiffs and the Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff David Stephens

31. Plaintiff David Stephens is and has been, at all relevant times, a resident and citizen of Missouri, currently residing in Wood Heights, Missouri.

32. In approximately 2018 or 2019, Mr. Stephens signed up for Defendant's Chick-fil-A One membership.

33. As part of the sign-up process, Mr. Stephens provided PII to Defendant, including but not limited to name, email, password, financial information, including credit card information and other billing information.

34. Mr. Stephens is a victim of the Data Breach.

35. On February 4, 2023, Mr. Stephens' Chick-fil-A One account was unlawfully accessed by an unauthorized third party and his account was charged $50.

36. Mr. Stephens called Defendant on or around February 4 or 5, shortly after noticing the unauthorized charge. When he called, Mr. Stephens was provided an automated message with a menu of options telling him to press a specific button if he had suspicious activity on his account. After pressing the button, a live customer service agent read off a canned script and assured Mr. Stephens that there was no data breach. Mr. Stephens was told by Defendant's customer service

representative that Chick-fil-A had several people with suspicious activity and that it would add his name to a list of other Chick-fil-A customers and process a refund.

37. Defendant refunded Mr. Stephens' Chick-fil-A One account on February 16, 2023, in the amount of $50.

38. As shown by Mr. Stephens' phone call and Defendant's prepared response, Defendant continued in its failure to own up to the Data Breach despite having knowledge of numerous customer complaints about the Data Breach.

39. Mr. Stephens provided his PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his PII. If Mr. Stephens had known Defendant would not adequately protect his PII, he would not have entrusted Defendant with his PII or allowed Defendant to maintain this sensitive PII.

Plaintiff Kaitlyn Strawn

40. Plaintiff Kaitlyn Strawn is and has been, at all relevant times, a resident and citizen of Georgia, currently residing in Dallas, Georgia.

41. In approximately 2021, Ms. Strawn signed up for Defendant's Chick-fil-A One membership.

42. As part of the sign-up process, Ms. Strawn provided PII to Defendant, including but not limited to name, email, password, financial

information, including credit card information and other billing information.

43. Ms. Strawn is a victim of the Data Breach.

44. On February 2, 2023, Ms. Strawn' Chick-fil-A One account was unlawfully accessed by an unauthorized third party and her account was charged two times for $50 each, or $100 total.

45. Shortly after noticing the suspicious activity in her account, Ms. Strawn called her bank, which refunded her $100.

46. Thereafter, Ms. Strawn e-mailed Defendant about the suspicious activity in her account.

47. Defendant responded with a canned response on February 14, 2023, which stated:

> We appreciate your patience as we continue to resolve suspicious account activity impacting some Chick-fil-A One members.
>
> To further protect your account, Chick-fil-A has proactively taken the following security measures:
>
> - If we detected an email change for your account, we have reverted your email address back to an email address that was previously associated with your Chick-fil-A One account.
>
> - Reset your password.
>
> - We've sent a password reset email to the email address on file. To log in to your account, please update your password

to one that is new and unique to your Chick-fil-A One account. Click **here** to see step-by-step directions to confirm the change online or through the Chick-fil-A(R) App.

- Temporarily froze funds previously loaded on your Chick-fil-A One Card to protect your account from unauthorized financial activity. We are actively working to restore your access to the Chick-fil-A One Card funds as quickly as possible and will update you as soon as the Chick-fil-A One Card functionality is restored.

- During this short time period, you will not be able to pay for your order using your Chick-fil-A One Card or load additional funds to that card. You can still order ahead via the Chick-fil-A App and use other methods of payment or complete your payment at the restaurant.

We understand and take seriously the trust you place in us to ensure your personal information is secure, and we apologize for any inconvenience you may have experienced. You can review the **Suspicious Activity FAQs** for more information. If you have any additional questions or concerns, please reach out to our team here and select Technical and Account Support. We are committed to resolving this issue and will provide another update as soon as possible.

48. Defendant still refused to admit the Data Breach.

49. Finally, on February 14, 2023, Defendant sent another email to Ms. Strawn, which stated:

Thank you for your patience as we worked to address your inquiry related to suspicious activity on your account. In addition to the previous communications you have received, we have restored your Chick-fil-A(R) One account balance where necessary, which may have included a refund to your original form of payment. Please note that the time in which it will take

> for the refund to post to your account is dependent upon your financial institution.
>
> As a small token of our appreciation for your patience during this time, we've added 2,000 points that can be used to redeem rewards of your choice and three rewards to your account. To view these rewards, select "Rewards" from the main screen in the Chick-fil-A App and then "My rewards". You can choose to redeem these by adding them to a mobile order or scanning at the Restaurant. Please be sure to use these rewards before they expire on June 30, 2023.
>
> We understand and take seriously the trust you place in us to ensure your personal information is secure, and we apologize for any inconvenience you may have experienced.
>
> If you still have concerns regarding your account, simply reply to this email and it will be escalated to our team for prompt investigation.

50. As shown in these emails, Defendant continued in its failure to admit the Data Breach, despite having knowledge of numerous customer complaints about the Data Breach.

51. Ms. Strawn provided her PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her PII. If Ms. Strawn had known that Defendant would not adequately protect her PII, she would not have entrusted Defendant with her PII or allowed Defendant to maintain this sensitive PII.

Defendant Chick-fil-A, Inc.

52. Defendant Chick-fil-A is a Georgia corporation with its principal place of business located at 5200 Buffington Road, Atlanta, Georgia 30349-2998.

DEFENDANT'S BUSINESS

53. Defendant is a Georgia-based company that sells fast food, particularly chicken, to customers nationwide.

54. Plaintiffs and the Class Members are current and former customers of Defendant.

55. Defendant sells fast food to consumers in brick-and-mortar locations nationwide. Additionally, Defendant created Chick-fil-A One, a rewards program allowing customers to earn points with every order. Customers can use points to redeem rewards, such as free menu items, and customers also have the option to give rewards to friends and family.

56. To join the Chick-fil-A One membership program, customers must create an account through Defendant's website or mobile App (available on both the Android and iPhone platforms).

57. To create a Chick-fil-A One account, customers must provide a first name, a last name, and an email and address and choose a password.

58. To purchase food using a Chick-fil-A One account, members must

provide payment information such as credit card information. The month and day of the customer's birthday, their phone number, and their address can also be included on the Chick-fil-A one account.

59. The information held by Defendant in its computer systems included the unencrypted PII of Plaintiffs and the Class Members.

60. Upon information and belief, in the course of collecting PII from customers, including Plaintiffs, Defendant promised to provide adequate security for customer data and to prevent unauthorized access, use, and disclosure, through its applicable privacy policy and other disclosures.

61. Plaintiffs and the Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

62. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and the Class Members relied on Defendant's sophistication to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and the Class Members value the confidentiality of their PII and demand security to safeguard their PII.

63. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and the Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumers' PII safe and confidential.

64. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and the Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

65. Defendant derived a substantial economic benefit from collecting Plaintiffs' and the Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

66. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and the Class Members' PII from disclosure.

THE DATA BREACH

67. On March 2, 2023, Defendant posted the Notice Letter informing victims of the Data Breach that Chick-fil-A did, in fact, suffer a data breach.[13]

68. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, why it took over two months to

[13] *See* Notice Letter, https://oag.ca.gov/system/files/2023-03-02%20-%20CFA%20-%20Individual%20Notification%20Template.pdf.

inform impacted individuals after Defendant determined their information was involved, why Defendant issued a public statement on its official Twitter account assuring that it was not involved in a data breach, and why it continued to tell customers who complained about unauthorized charges on their accounts that there was no data breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and the Class Members, who retain a vested interest in ensuring their PII remains protected.

69. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and the Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and the Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

70. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and the Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

71. The attackers accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiffs and the Class Members, including

but not limited to their names, emails, passwords, and financial information, including credit card information and billing information. Plaintiffs' and the Class Members' PII was accessed and stolen in the Data Breach.

72. Plaintiffs further believe their PII, and that of the Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

DATA BREACHES ARE PREVENTABLE

73. As the Federal Bureau of Investigation explains, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[14]

74. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain

[14] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited March 6, 2023).

Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[15]

75. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . . .

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . . .

[15] *Id.* at 3-4.

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it . . . .

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . . .[16]

76. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

[16] *See* Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited March 5, 2023).

Secure internet-facing assets
- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely

Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege
- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications][17]

77. Given that Defendant was storing the sensitive PII of its current and

[17] *See* Human-operated ransomware attacks: A preventable disaster (Mar. 5, 2020), *available at* https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

former customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

78. The occurrence of the Data Breach indicates Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of at least 71,473 current and former customers, including that of Plaintiffs and the Class Members.

DEFENDANT ACQUIRES, COLLECTS, AND STORES PLAINTIFFS' PII

79. As a condition of joining Defendant's Chick-fil-A One program, Plaintiffs and the Class Members were required to give their sensitive and confidential PII to Defendant.

80. Defendant retains and stores this information and derives a substantial economic benefit from the PII it collects. But for the collection of Plaintiffs' and the Class Members' PII, Defendant would be unable to perform its business services.

81. By obtaining, collecting, and storing the PII of Plaintiffs and the Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from disclosure. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely,

to use this information for business purposes only, and to make only authorized disclosures of this information.

82. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and the Class Members.

83. Upon information and belief, Defendant made promises to Plaintiffs and the Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

DEFENDANT KNEW, OR SHOULD HAVE KNOWN, OF THE RISK SINCE COMPANIES IN POSSESSION OF PII ARE SUSCEPTIBLE TO CYBER ATTACKS

84. Data thieves regularly target companies like Defendant due to the highly sensitive information they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

85. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad

(268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known the PII it collected and maintained would be targeted by cybercriminals.

86. Additionally, as companies have become more dependent on computer systems to run their business,[18] *e.g.*, the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.

87. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and the Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and the Class Members as a result of a breach.

88. In 2021, 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[19]

---

[18] *See* https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited March 6, 2023).

[19] *See* Identity Theft Resource Center, 2021 Data Breach Annual Report at 6 (Jan. 24, 2022), *available at* https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited

89. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and the Class Members from being compromised.

90. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

91. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and the Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and the Class Members as a result of a breach.

92. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

March 5, 2023).

93. In the Notice Letter, Defendant states:

> **What We Are Doing.**
>
> Chick-fil-A takes the protection of personal information seriously. As soon as Chick-fil-A discovered the incident, we immediately took action to protect customers' accounts, which included requiring customers to reset passwords, removing any stored credit/debit card payment methods, and temporarily freezing funds previously loaded onto customers' Chick-fil-A One accounts. We also restored customers' Chick-fil-A One account balances, which may have included a refund to your original form of payment, where possible. As an additional way to say thank you for being a loyal Chick-fil-A customer, we have added rewards to your account. Chick-fil-A continues to enhance its security, monitoring, and fraud controls as appropriate to minimize the risk of any similar incident in the future.

This is wholly inadequate to compensate Plaintiffs and the Class Members, as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and the Class Members' PII. Moreover, Plaintiffs and the Class Members are forced to pay out of pocket for necessary identity monitoring services.

94. The injuries to Plaintiffs and the Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and the Class Members.

95. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and the Class Members are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

96. As a company in possession of its current and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and the Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and the Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

VALUE OF PERSONALLY IDENTIFYING INFORMATION

97. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] 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," 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,

[20] 17 C.F.R. § 248.201.

employer or taxpayer identification number."[21]

98. The PII of individuals 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.[22] For example, online payment services login info can be sold at a price ranging from $20 to $200.[23] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[24]

99. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

100. 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

[21] *Id.*

[22] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited March 6, 2023).

[23] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited March 6, 2023).

[24] *In the Dark*, VPNOverview.com (2019), *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited March 6, 2023).

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.[25]

101. Plaintiffs and the 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.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

102. The Federal Trade Commission 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.

103. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that

[25] GAO, *Report to Congressional Requesters*, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited March 6, 2023).

is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[26]

104. 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.[27]

105. 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.

106. 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

[26] FED. TRADE COMM'N, *Protecting Personal Information: A Guide for Business* (2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 6, 2023).
[27] *Id.*

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

107. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

108. Defendant failed to properly implement basic data security practices.

109. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

110. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the

immense damages that would result to Plaintiffs and the Class.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

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

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

113. Other best cybersecurity practices that are standard for companies 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.

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

115. These foregoing frameworks are existing and applicable industry standards for retail employers, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actors and causing the Data Breach.

COMMON INJURIES AND DAMAGES

116. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and the Class Members has materialized and is imminent, and Plaintiffs and the Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent

threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and the Class Members' PII.

THE DATA BREACH INCREASES PLAINTIFFS' AND THE CLASS MEMBERS' RISK OF IDENTITY THEFT

117. The unencrypted PII of Plaintiffs and the Class Members will end up for sale on the dark web, as that is the *modus operandi* of hackers.

118. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and the Class Members. Simply, unauthorized individuals can easily access the PII of Plaintiffs and the Class Members.

119. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity

theft related crimes discussed below.

120. Plaintiffs' and the Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

LOSS OF TIME TO MITIGATE THE RISK OF IDENTITY THEFT AND FRAUD

121. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

122. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and the Class Members must, as Defendant's Notice Letter instructs them, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

123. Plaintiffs and the Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching

the Data Breach's occurrence, reviewing their financial accounts for fraudulent activity, researching credit and identity theft monitoring insurance, and enrolling in credit and identity theft monitoring insurance.

124. Plaintiffs' and the Class Members' mitigation efforts are consistent with the U.S. Government Accountability Office's 2007 report regarding data breaches, in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

125. Plaintiffs' and the Class Members' mitigation efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone has stolen 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.[29]

126. A study by Identity Theft Resource Center shows the multitude of

[28] *See* GAO, *Report to Congressional Requesters*, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited March 6, 2023).

[29] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited March 6, 2023).

harms caused by fraudulent use of personal and financial information:[30]

[30] Jason Steele, *Credit Card and ID Theft Statistics* (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php, available on Internet Archive Wayback Machine at https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited March 6, 2023).

DIMINUTION OF VALUE OF PII

127. PII is a valuable property right.[31] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts, which include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

128. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[32] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[33] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[34]

129. As a result of the Data Breach, Plaintiffs' and the Class Members' PII,

---

[31] *See, e.g.*, John T. Soma et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets." (citations omitted)).

[32] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited March 6, 2023).

[33] https://datacoup.com/ (last March 6, 2023).

[34] Nielsen Computer & Mobile Panel, Frequently Asked Questions (2022), *available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited March 6, 2023).

which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or the Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the PII has been lost, thereby causing additional loss of value.

130. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and the Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and the Class Members as a result of a breach.

131. The fraudulent activity resulting from the Data Breach may not come to light for years.

132. Plaintiffs and the 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.

133. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to

potentially hundreds of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

134. The injuries to Plaintiffs and the Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and the Class Members.

FUTURE COST OF CREDIT AND IDENTITY THEFT MONITORING IS REASONABLE AND NECESSARY

135. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and reports of misuse of Class Member PII, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – *e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns; taking out loans or lines of credit, or filing false unemployment claims.

136. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

137. Consequently, Plaintiffs and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

138. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect the Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and the Class Members would not need to bear but for Defendant's failure to safeguard their PII.

CLASS ACTION ALLEGATIONS

139. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

140. Plaintiffs seek to represent a class defined as follows:

> **The Class.** All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party between December 18, 2022, and February 12, 2023, through the Data Breach.

141. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct

protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

142. Plaintiffs reserve the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate the definition of the Class should be narrowed, expanded, or otherwise modified.

143. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 71,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to California Attorney General's Office. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

144. Commonality and Predominance: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members are the following:

a. whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and the Class Members;

b. whether Defendant had a duty not to disclose the PII of

Plaintiffs and the Class Members to unauthorized third parties;

c. whether Defendant failed to adequately safeguard the PII of Plaintiffs and the Class Members;

d. whether and when Defendant actually learned of the Data Breach;

e. whether Defendant adequately, promptly, and accurately informed Plaintiffs and the Class Members that their PII had been compromised;

f. whether Defendant violated the law by failing to promptly notify Plaintiffs and the Class Members that their PII had been compromised;

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

h. whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

i. whether Plaintiffs and the Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

j. whether Plaintiffs and the Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

145. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

146. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect the Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

147. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members, and the infringement of the rights and the damages they have suffered are typical of the other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

148. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action

treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

149. The nature of this action and the nature of laws available to Plaintiffs and the Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class Members for the wrongs alleged because otherwise Defendant would necessarily gain an unconscionable advantage, since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will

establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

150. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of the Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

151. Adequate notice can be given to the Class Members directly using information maintained in Defendant's records.

152. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of the Class Members; Defendant may continue to refuse to provide proper notification to the Class Members regarding the Data Breach; and Defendant may continue to act unlawfully as set forth in this Complaint.

153. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

154. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the

resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Defendant failed to timely notify Plaintiffs and the Class Members of the Data Breach;

b. whether Defendant owed a legal duty to Plaintiffs and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. whether adherence to FTC data security recommendations, and measures recommended by data security experts, would have reasonably prevented the Data Breach.

CLAIMS FOR RELIEF

FIRST COUNT

Negligence
(On Behalf of Plaintiffs and the Class)

155. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 154 above as if fully set forth herein.

156. Plaintiffs bring this claim for negligence against Defendant on behalf

of the Class.

157. Defendant required Plaintiffs and the Class Members to submit non-public PII as a condition of joining and utilizing Defendant's Chick-fil-A One program.

158. Plaintiffs and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information.

159. Defendant had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiffs and the Class Members.

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

161. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and the Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

162. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

163. Defendant'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 is bound by industry standards to protect confidential PII.

164. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Class Members' PII. 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 the Class Members' PII;

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

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

d. allowing unauthorized access to the Class Members' PII; and

e. failing to detect in a timely manner that the Class Members' PII had been compromised.

165. It was foreseeable that Defendant's failure to use reasonable measures to protect the Class Members' PII would result in injury to the Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

166. It was therefore foreseeable that the failure to adequately safeguard the Class Members' PII would result in one or more types of injuries to the Class Members.

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

168. As a result of Defendant's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

169. Plaintiffs and the Class Members seek compensatory and consequential damages suffered as a result of the Data Breach.

170. Plaintiffs and the Class Members also seek injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

SECOND COUNT

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

171. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 154 above as if fully set forth herein.

172. Plaintiffs bring this claim for breach of implied contract against Defendant on behalf of the Class.

173. Plaintiffs and the Class Members were required to provide their PII to Defendant as a condition of joining and utilizing Defendant's Chick-fil-A One program.

174. Plaintiffs and the Class Members provided their sensitive PII to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure.

175. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and the Class Members that it would only disclose

PII under certain circumstances, none of which relate to the Data Breach.

176. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and the Class Members' PII would remain protected.

177. Implicit in the agreement between Plaintiffs and the Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and the Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and the Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

178. When Plaintiffs and the Class Members provided their PII to Defendant as a condition of joining and utilizing Defendant's Chick-fil-A One program, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

179. Defendant required the Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and the Class Members accepted Defendant's offers and provided their PII to Defendant.

180. In entering into such implied contracts, Plaintiffs and the Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

181. Plaintiffs and the Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and the Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

182. Plaintiffs and the Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

183. Defendant breached its implied contracts with the Class Members by failing to safeguard and protect their PII.

184. As a direct and proximate result of Defendant's breaches of the implied contracts, the Class Members sustained damages as alleged herein.

185. Plaintiffs and the Class Members seek compensatory and consequential damages suffered as a result of the Data Breach.

186. Plaintiffs and the Class Members also seek nominal damages for the

breach of implied contract.

187. Plaintiffs and the Class Members also seek injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT

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

188. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 154 above as if fully set forth herein.

189. Plaintiffs bring this claim for negligence *per se* against Defendant on behalf of the Class.

190. Pursuant to Section 5 of the FTC Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and the Class Members' PII.

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

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

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

194. The injury and harm suffered by Plaintiffs and the 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 the Class Members to experience the foreseeable harms associated with the exposure of their PII.

195. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Class Members have suffered injury and seek compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOURTH COUNT

Violation of Georgia's Uniform Deceptive Trade Practices Act
GA. CODE § 10-1-370 *et seq.*
(On Behalf of Plaintiffs and the Class)

196. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 154 above as if fully set forth herein.

197. Plaintiffs bring this claim against Defendant on behalf of the Class for

violation of Georgia's Uniform Deceptive Trade Practices Act, GA. CODE § 10-370 *et seq.*

198. Plaintiffs and the Class Members are "persons" within the meaning of Georgia Code section 10-1-371(5).

199. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of Georgia Code section 10-1-372(a), including:

a. representing that goods or services have characteristics that they do not have;

b. representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. advertising goods or services with intent not to sell them as advertised;

d. engaging in other conduct that creates a likelihood of confusion or misunderstanding.

200. Defendant's deceptive trade practices include, *inter alia*:

a. implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties

pertaining to the security and privacy of individuals including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach; and

d. omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Plaintiffs' PII.

201. Defendant's omissions were material because they were likely to and did deceive Plaintiffs and the Class Members about the adequacy of Defendant's data security.

202. As a direct and proximate result of Defendant's actions, Plaintiffs and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

203. Plaintiffs and the Class Members seek all relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs under Georgia Code section 10-1-373.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class Members, request judgment against Defendant and that the Court grant the following:

A. an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. equitable relief enjoining Defendant from engaging in the wrongful

conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and the Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and the Class Members;

C. injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and the Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and the Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and the Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks,

penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and the Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal

identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

D. an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. prejudgment interest on all amounts awarded; and

F. such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Date: March 6, 2023

Respectfully Submitted,

By: *Robert E. Jones, Esq.*
Robert E. Jones, Esq.
Georgia Bar No. 398206
THE JONES LAW FIRM, P.C.
1100 Peachtree Street
Suite 950
Atlanta, GA 30309
rob@robjoneslaw.com
Telephone: (404) 877-2345

Michael R. Reese (*pro hac vice* to be filed)
New York State Bar No. 2818672
mreese@reesellp.com
REESE LLP
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500
Facsimile: (212) 253-4272

George V. Granade
Georgia Bar No. 559603
Application for admission to District bar to be filed
ggranade@reesellp.com
REESE LLP
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Telephone: (310) 393-0070
Facsimile: (212) 253-4272

Charles D. Moore
New York State Bar No. 2818672
(*pro hac vice* to be filed)
cmoore@reesellp.com
REESE LLP

100 South 5th Street, Suite 1900
Minneapolis, Minnesota 55402
Telephone: (212) 643-0500

Kevin Laukaitis
Pennsylvania Bar No. 321670
(*pro hac vice* to be filed)
klaukaitis@laukaitislaw.com
LAUKAITIS LAW
737 Bainbridge Street, #155
Philadelphia, Pennsylvania 19147
Telephone: (215) 789-4462

Counsel for Plaintiffs David Stephens and Kaitlyn Strawn and the Proposed Class

ClassAction.org
