IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF IOWA

LOGAN ALDRIDGE, *individually and on behalf of all others similarly situated*,	Case No. 23-CV-357
Plaintiff,	**CLASS ACTION COMPLAINT**
v.	**JURY TRIAL DEMANDED**
PURFOODS LLC D/B/A MOM'S MEALS,	
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff Logan Aldridge brings this class action lawsuit, individually and on behalf of all others similarly situated (the "Class Members"), against PurFoods LLC d/b/a/ Mom's Meals ("PurFoods" or "Defendant") alleging as follows based upon information and good faith belief and due investigation of counsel except as to the allegations specifically pertaining to Plaintiff, which are based on personal knowledge:

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against PurFoods for its abject failure to properly secure and to safeguard its network thereby allowing a data breach to occur resulting in a tremendous amount of sensitive and personally identifiable information ("PII") including, but not limited to, customer names, financial account and payment card information, medical record numbers, health information, treatment information, diagnosis codes, meal categories and costs, health insurance information and patient ID numbers (collectively, the "Private Information") to be accessed and compromised by third-party hackers (the "Data Breach").

2. To put it bluntly, PurFoods, which does business as Mom's Meals, a meal delivery service, has ***not*** been forthcoming nor expedient in notifying the 1,237,681 persons whose Private Information was compromised as a result of its negligence.

3. Specifically, PurFoods did not begin to notify affected individuals until August 25, 2023—over seven months after its network was accessed and over six months after it became aware of "suspicious account behavior" that occurred between January 16, 2023 and February 22, 2023.

4. According to its breach notification letter, PurFoods, beginning in February of this year, commenced an investigation with the help of third-party specialists.[1]

5. That investigation revelated that PurFoods experienced a cyberattack between January 16, 2023 and February 22, 2023, that included the encryption of certain files in its network.

6. According to PurFoods, the investigation did not conclude until July 10, 2023, and then—and only then—was it able to determine that the Private Information at issue included personal and protected health information ("PHI") related to certain individuals.

7. PurFoods also said that tools commonly used to steal data were found on its network, strongly suggesting that the highly sensitive Private Information was likely taken from PurFoods' network and sold on the dark web (and elsewhere).[2]

8. PurFoods' failures affected—and continue to affect—1,237,681 individuals, many of which received Mom's Meals packages, including Medicare, Medicaid and self-paying members

---

[1] The Notice of Data Event, available at https://apps.web.maine.gov/online/aeviewer/ME/40/c7ad1c53-6e20-41d8-8fb6-f1ccd0e3e0cc.shtml; *see also* Defendant's Maine Data Breach Notice, attached as **Exhibit A** hereto, and Defendant's Notice to Plaintiff, attached as **Exhibit B** hereto.

[2] *Id.* ("We can't rule out the possibility that data was taken from one of our file servers," the company said.).

without an eligible health plan or who do not qualify for government assistance. The Data Breach also impacted the company's current and former employees, as well as independent contractors.

9. Compounding its negligence in failing to secure its network and to protect the Private Information, PurFoods appears to be actively concealing or—at least—attempting to suppress information related to the Data Breach.[3] According to TechCrunch, "PurFoods published a separate data breach notice on its website, which at the time of publication includes 'noindex' code telling search engines to ignore the webpage, effectively preventing affected individuals from finding the breach notice in search results."[4]

10. As detailed herein, PurFoods owed a non-delegable duty to Plaintiff and Class Members to implement and to maintain reasonable and adequate security measures to secure, to protect and to safeguard their Private Information against unauthorized access and disclosure.

11. PurFoods breached that duty by, among other things, failing to implement and to maintain reasonable security procedures and practices to protect their customers' Private Information from unauthorized access and disclosure.

12. Even in its rather milquetoast and self-serving Notice, PurFoods tacitly acknowledges the insufficiency of its network security policies, procedures and practices; "[PurFoods has] taken a number of steps to further strengthen our network security. We are also reviewing our existing policies and procedures to identify additional measures and safeguards."[5]

---

[3] *See* Carly Page, *Mom's Meals says data breach affects 1.2 million customers*, TechCrunch (Aug. 29, 2023) (available at https://techcrunch.com/2023/08/29/moms-meals-says-data-breach-affects-1-2-million-customers/ (last visited Sept. 9, 2023) ("PurFoods said it began notifying affected individuals on August 25 — seven months after it was first compromised and more than a month after it concluded its investigation into the breach. It's not clear why the company waited so long to tell affected customers, and PurFoods did not respond to TechCrunch's questions.").

[4] *Id.*

[5] *See* Ex. B, Notice at 1.

13. As a result of PurFoods's inadequate security and breach of their duties and obligations, Plaintiff's and Class Members' Private Information was accessed by third-party ransomware attackers who have the intent to take that data and to sell it on the dark web, among other things.

14. Plaintiff and Class Members therefore face an imminent and ongoing risk of identity theft, which is heightened here by the loss of social security numbers—the gold standard for identity thieves.

15. Plaintiff seeks to remedy these harms individually and on behalf of all others similarly situated (those whose Private Information was accessed during the Data Breach), and thus asserts claims for negligence, negligence *per se*, breach of implied contract and unjust enrichment, breach of confidence, bailment and breach of implied covenant of good faith and fair dealing, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief and all other relief authorized by law.

PARTIES

16. Plaintiff Logan Aldridge is an adult who, at all relevant times, was and is a resident of the State of Texas, residing in Hart County, Kentucky, with the intent to remain there indefinitely. Plaintiff and Class members are, or were, clients and/or employees of PurFoods and entrusted it with their Private Information.

17. PurFoods is a domestic limited liability company organized and existing under Iowa law with its principal place of business located at 3210 SE Corporate Woods Drive in Ankeny, Iowa 50021.

JURISDICTION & VENUE

18. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class,

as defined below, is a citizen of a different state than PurFoods, there are more than 100 members of the Class and the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs.

19. This Court has personal jurisdiction over PurFoods because it: (i) is a domestic limited liability company organized and existing in the State of Iowa; (ii) maintains its principal place of business in Iowa and (iii) is engaged in substantial business activity in Iowa.

20. Venue is proper in this judicial district under 28 U.S.C. § 1391(b) because PurFoods's principal place of business is in Polk County, Iowa and a substantial part of the events or omissions giving rise to the claims occurred in, were directed to and/or emanated from this District.

FACTUAL BACKGROUND

A. PurFoods Fails to Employ Reasonable & Necessary Network Security Resulting in a Data Breach which Comprised the Private Information of Over 1.2 Million Individuals.

21. Purfoods describes itself as a health-focused food-delivery business, with its primary program called Mom's Meals, which purportedly works with more than 500 health providers including governments and managed-care organizations to deliver meals to people covered under Medicare and Medicaid as well as people who want to buy ready-to-eat entrees.[6]

22. By its Notice letter, PurFoods announced that it experienced a cyberattack sometime between January 16, 2023 and February 22, 2023, that resulted in the encryption of certain files in its network.

23. According to PurFoods, it commenced an investigation into the Data Breach on February 23, 2023 but the investigation did not conclude until July 10, 2023, nearly five months

[6] *See* https://www.theregister.com/2023/08/28/purfoods_meal_data_theft/ (last visited Sept 9, 2023).

later. And, then—and only then—was PurFoods able to determine that the files at issue included personal and protected health information related to certain individuals.

24. Defendant's failures affected—and continue to affect—1,237,681 individuals, many of which received Mom's Meals packages, including Medicare, Medicaid and self-paying members without an eligible health plan or who do not qualify for government assistance. The Data Breach also impacted PurFoods' current and former employees, as well as independent contractors.

B. PurFoods Did Not Timely nor Adequately Provide Affected Individuals Notice in Breach of its Promise to do so.

25. PurFoods has ***not*** been forthcoming nor expedient in notifying the 1,237,681 persons whose information was compromised as a result of its negligence. Specifically, PurFoods did not begin to notify affected individuals until August 25, 2023 regarding the Data Breach that occurred in January and February 2023.

26. PurFoods maintains a "Privacy Policy (Personal Information)" that "only applies to information collected by PurFoods online."

27. PurFoods proclaims that it "takes your privacy seriously" and that "[e]arning and maintaining your trust is important to us."[7]

28. PurFoods's website includes a policy on their cybersecurity capabilities, entitled **"**HOW PURFOODS HANDLES SECURITY," which states that "[t]he security of your Personal Information is important to us. When you enter sensitive information (such as credit card number) on our registration or order forms, we encrypt that information using secure socket layer

[7] https://www.purfoods.com/privacy-policy/ (last visited Sept. 9, 2023).

technology (SSL). We follow generally accepted industry standards to protect the Personal Information submitted to us, both during transmission and once we receive it."[8]

29. PurFoods also maintains "Mom's Meals Notice of Privacy Practices," which states that "THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."[9]

30. As part of the Notice, PurFoods states that "[w]e are committed to protecting the confidentiality of your health information and are required by law to do so."

31. In a section entitled "OUR RESPONSIBILITIES," PurFoods states that it is "required by law to maintain the privacy and security of your protected health information."

32. PurFoods also promises that it "will notify you know (sic) promptly if a breach occurs that may have compromised the privacy or security of your information."

33. This Data Breach occurred between the middle of January and the middle of February of 2023, but PurFoods did not find about any ongoing data breach until February 23, 2023 and did not begin to notify the over 1.2 million affected individuals until August 25, 2023, ***which is hardly prompt by any measure***.

34. Despite the fact that PurFoods allegedly conducted a five-month investigation, it has not revealed most of the findings of the investigation it commissioned.

35. PurFoods has not revealed when the unauthorized actor first gained access to its systems nor has it revealed the mechanism by which the unauthorized actor first gained access,

---

[8] *Id.*

[9] https://www.purfoods.com/webres/File/Website%20Privacy%20Policy.pdf (last visited Sept. 9, 2023).

PurFoods has not revealed whether the unauthorized actor was able to access PurFoods' broader computer systems and network. Even worse, PurFoods has failed to disclose the exact nature of the unauthorized access to Plaintiff's and Class Members' Private Information.

36. Instead, PurFoods speaks in generalities and equivocations stating that the impacted information "*may involve* some of your personal information […] includ[ing] name, diagnosis code, health insurance information, meal category and/or cost, patient ID number, and treatment information."[10]

37. This "disclosure" amounts to no real disclosure at all as it fails to inform Plaintiff and Class Members what information belonging to them was actually affected leaving Plaintiff and Class Members to believe that ***all*** of this incredibly sensitive Private Information was compromised in this Data Breach.

38. The result of PurFoods' "thorough investigation" is not provided in the Notice to Plaintiff and Class Members and the notice does not explain whether the accessed data has been or will be misused by the hackers.

39. However, upon information and belief, PurFoods has no methods, policies or procedures in place that would afford their customers (Plaintiff and Class Members) any mechanism or opportunity to report misuse of the data back to PurFoods and the investigation commissioned by PurFoods did ***not*** survey its clients whose data was breached for evidence of misuse.

40. To date, PurFoods has done next to nothing to adequately protect Plaintiff and Class Members or to compensate them for their injuries sustained in this Data Breach.

[10] *See* Ex A., Notice at 1.

41. PurFoods' data breach notice letter downplays the theft of Plaintiff's and Class Members Private Information, when the facts—which are almost exclusively in Defendant's possession—demonstrate that the Private Information was targeted, accessed and exfiltrated in a criminal cyberattack.

42. Moreover, the fraud and identity monitoring services offered by PurFoods are only for one year, are not three-bureau monitoring, and place the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing issues when the service number for enrollment does not work.

43. Moreover, PurFoods instructs Plaintiff and Class Members to mitigate their damages by self-monitoring their accounts and credit reports to ensure that they remain uncompromised as a result of PurFoods' failure to properly secure their Private Information.

C. PurFoods was Certainly Aware of the Risk of Cyber Attacks & Thus the Data Breach was Eminently Foreseeable.

44. Data security breaches have dominated the headlines for the last two decades.

45. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[11] Yahoo,[12] Marriott International,[13] Chipotle, Chili's, Arby's[14] and many, many others.[15]

46. PurFoods should certainly have been aware—and indeed was aware—that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

47. PurFoods was clearly aware of the risks it was taking and the harm that could result from inadequate data security and it voluntarily assumed a duty to protect such Private Information by collecting it in the first place.

48. Given that PurFoods collected the Private Information of over 1.2 million individuals, it should have been more vigilant about its network security policies, procedures and practices which would have prevented the unauthorized access to and disclosure of Plaintiff's and Class Members' Private Information.

---

[11] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited Sept. 11, 2023).

[12] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSO Online (Oct. 4, 2017), https://www.csoonline.com/article/560623/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited Sept. 11, 2023).

[13] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, The SSL Store: Hashedout (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Sept. 11, 2023).

[14] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/privacy/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/ (last visited Sept. 11, 2023).

[15] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO Online (Dec. 20, 2018), https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html (last visited Sept. 11, 2023).

49. At all relevant times, PurFoods knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result.

50. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[16]

51. PurFoods' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and retail industries.

D. PurFoods Failed to Properly Protect Plaintiff's & Class Members' Private Information.

52. PurFoods could have prevented this Data Breach by properly securing and encrypting its network systems containing the Private Information of Plaintiff and Class Members. Alternatively, PurFoods could have destroyed the data, especially for individuals with whom it has not had a relationship for a period of time.

53. PurFoods' negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like PurFoods to protect and to secure sensitive data they possess.

54. Despite the prevalence of public announcements of data breach and data security compromises, PurFoods failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

[16] *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 accessed Sept. 11, 2023).

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

56. 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, employer or taxpayer identification number."[17]

57. To prevent and to detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, PurFoods 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)…

- **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.

[17] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FTC, https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed Sept. 11, 2023).

- **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…[18]

58. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, PurFoods could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

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;

[18] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Sept. 11, 2023).

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].[19]

59. Given that PurFoods was storing the Private Information of Plaintiff and Class Members, it could and should have implemented all the above measures to prevent and to detect cyberattacks. The occurrence of the Data Breach indicates that PurFoods failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

E. PurFoods' Negligent Acts & Breaches.

60. PurFoods designed, controlled and maintained the process of gathering the Private Information from Plaintiff and Class Members.

61. PurFoods therefore assumed and otherwise owed duties and obligations to Plaintiff and Class Members to take reasonable measures to protect the Private Information, including the duty of oversight, training, instruction, testing of the data security policies and network systems.

[19] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Sept. 11, 2023).

62. PurFoods breached these obligations to Plaintiff and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies that would adequately safeguard Plaintiff's and Class Members' Private Information.

63. Upon information and belief, PurFoods' unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a) Failing to design and maintain an adequate data security system to reduce the risk of data breaches and to protect Plaintiff's and Class Members Private Information;

b) Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c) Failing to test and assess the adequacy of its data security system;

d) Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e) Failing to develop and to implement uniform procedures and data security protections;

f) Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g) Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

h) Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed herein;

i) Failing to implement or update antivirus and malware protection software in need of security updating;

j) Failing to require encryption or adequate encryption on its data systems and

k) Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' Private Information

provided to PurFoods, which in turn allowed cyberthieves to access its IT systems.

F. PurFoods Did Not Comply with FTC Guidelines.

64. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

65. According to the FTC, the need for data security should be factored into all business decision making.

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal 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.[20]

67. The guidelines also recommend that businesses use an intrusion detection system to discover and 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.

68. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

[20] *See Protecting Personal Information: A Guide for Business*, FTC (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Sept. 11, 2023).

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

70. PurFoods failed to properly implement basic data security practices.

71. PurFoods' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

72. Upon information and good faith belief, PurFoods was always fully aware of its obligation to protect the Private Information of Plaintiff and Class Members. PurFoods was also aware of the significant repercussions that would result from its failure to do so.

G. PurFoods is a Business Associate Under HIPAA

73. PurFoods is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

74. PurFoods is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

75. HIPAA permits covered entities (such as the medical providers that provided Plaintiffs' and Class members' Private Information to Defendant) to disclose such information to business associates only if the covered entities obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule.[21]

76. In order to comply with the Privacy Rule, the satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.[22]

77. Thus, while it may not have made representations directly to Plaintiff regarding its data security and privacy obligations, practices and capabilities, PurFoods is—further to HIPAA and its business associate agreement ("BAA") requirements under the Privacy Rule—required to have a contract in place with each of its healthcare provider (covered entity) clients as a business associate under HIPAA, HITECH and any implementing regulations.[23]

---

[21] *See* New HHS Fact Sheet On Direct Liability of Business Associates under HIPAA, 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e) (last visited Sept. 11, 2023).

[22] *See* Business Associates, 45 CFR 164.502€, 164.504€, 164.532(d) & €, available at www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (last visited Sept. 11, 2023).

[23] *See* New HHS Fact Sheet On Direct Liability of Business Associates under HIPAA, 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e) (last visited Sept. 11, 2023).

78. Thus, upon information and good faith belief, PurFoods would have agreed to implement reasonable administrative, physical, technical and electronic safeguards to protect the confidentiality, integrity and availability of all Private Information provided to it by its clients.

79. Plaintiff and Class members are intended third-party beneficiaries of any BAA between PurFoods and its various healthcare clients who are covered entities under HIPAA.

80. While Plaintiff and Class members have not been provided any BAAs that PurFoods is required to have with its covered entity clients, BAAs must all include the following information, according to HHS:

- A description of the permitted and required PHI used by the business associate/subcontractor;
- A representation that the business associate/subcontractor will not use or further disclose PHI other than as permitted or required by the contract or as required by law;
- A requirement that the business associate/subcontractor use appropriate safeguards to prevent inappropriate PHI use or disclosure.[24]

81. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[25]

H. PurFoods Did Not Comply with Industry Standards.

82. HHS's Office for Civil Rights has stated:

---

[24] *See* 45 CFR 164.504(e).

[25] *Breach Notification Rule*, U.S. Dep't of Health & Human Services, *available at* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited Sept. 11, 2023).

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[26]

83. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (i) the proper encryption of Private Information; (ii) educating and training healthcare employees on how to protect Private Information and (iii) correcting the configuration of software and network devices.

84. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of the value of the Private Information which they maintain and because as an industry they have been slow to adapt and to respond to cybersecurity threats.[27] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized access to and disclosure of Private Information.

85. Despite the abundance and availability of information regarding cybersecurity best practices, PurFoods chose to ignore them. These best practices were known, or should have been known by PurFoods, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

I. Cyber Criminals Have Used & Will Continue to Use Plaintiff's Private Information.

---

[26] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

[27] *See, e.g., 10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.

86. Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

87. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[28] For example, with the Private Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[29] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

88. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[30]

89. This Data Breach was clearly a financially motivated attack as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like PurFoods is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

---

[28] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited Sept. 11, 2023).

[29] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 15, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/ (last visited Sept. 11, 2023).

[30] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737 (last visited Sept. 11, 2023).

90. The Private Information of consumers is of extremely high value to criminals, as evidenced by the prices offered through the dark web.

91. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[31]

92. According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[32] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[33]

93. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information…[is] worth more than 10x on the black market."[34]

---

[31] *See 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/.

[32] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: https://www.privacyaffairs.com/dark-web-price-index-2021/

[33] *In the Dark*, VPNOverview, 2019, available at https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[34] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Sept. 11, 2023).

94. 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.[35]

95. Moreover, hackers may not use the information right away, but this does not mean it will notbe used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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. [36]

96. One such example of criminals using Private Information for profit, to the detriment of Plaintiff and Class Members, is the development of "Fullz" packages, where cyber-criminals cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[37]

---

[35] There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers, and an entire economy exists related to the value of personal data. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market. *See* Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited Sept. 11, 2023).

[36] For example, approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[36] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names. *See The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches* ("*Potential Damages*"), Experian, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Sept. 11, 2023).

[37] "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

97. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and to identify it to Plaintiff's and Class Members' phone numbers, email addresses and other unregulated sources and identifiers.

98. In other words, even if certain information such as emails, phone numbers or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

99. It is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and Class Members stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

100. 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.[38]

---

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/ (last visited Sept. 11, 2023).

[38] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at*: https://www.gao.gov/assets/gao-07-737.pdf (last accessed Sept. 11, 2023).

101. As such, future monitoring of financial and personal records is reasonable and necessary well beyond the one of protection offered by PurFoods.

102. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[39]

103. PurFoods' offer of limited identity monitoring to Plaintiff and Class Members is woefully inadequate and will not fully protect them from the damages and harm caused by PurFoods' failures.

104. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. Once the offered coverage expires, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to PurFoods' gross negligence.

105. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's Private Information)—it does not prevent identity theft.[40]

106. Nor can an identity monitoring service remove personal information from the dark web; "[t]he people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."

---

[39] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[40] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited Sept. 11, 2023).

107. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

108. Even more serious is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following FTC checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

J. Plaintiff & Class Members Have Suffered Numerous Common Injuries & Damages.

109. As result of PurFoods' ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

110. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including:

111. Plaintiff and Class Members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private

Information being placed in the hands of criminals and having been already misused;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves have already used that information to defraud other victims of the Data Breach;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' Private Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information and

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

K. The Risk of Identity Theft to Plaintiff & Class Members Is Present & Ongoing.

112. The link between a data breach and the risk of identity theft is simple and well established. Simply put, criminals acquire and steal Private Information 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.

113. 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.[41]

114. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[42]

115. Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[43] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

116. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal information like the Private Information at issue here.[44]

---

[41] 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 are often the starting point for these additional targeted attacks on the victims.

[42] *What Is the Dark Web?,* Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last accessed Sept. 11, 2023).

[43] *Id.*

[44] *What is the Dark Web*? – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last accessed Sept. 11, 2023).

117. The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity.

118. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[45]

119. As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[46]

120. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[47]

121. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[48]

122. PurFoods did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen.

---

[45] *Id.*; What Is the Dark Web?, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/

[46] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web

[47] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Sept. 11, 2023).

[48] *Id.*

123. 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.

124. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Private Information.

125. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

126. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[49]

L. Loss of Time to Mitigate the Risk of Identity Theft & Fraud.

127. 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 Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and to spend time to address the

[49] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last accessed Sept. 11, 2023).

dangerous situation, learn about the breach and otherwise mitigate the risk of becoming a victim of identity theft of fraud.

128. 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.

129. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as PurFoods' Notice instructs them, regularly monitor their accounts for unusual activity and review and monitor free credit reports.

130. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity—which may take years to discover and detect—and filing police reports.

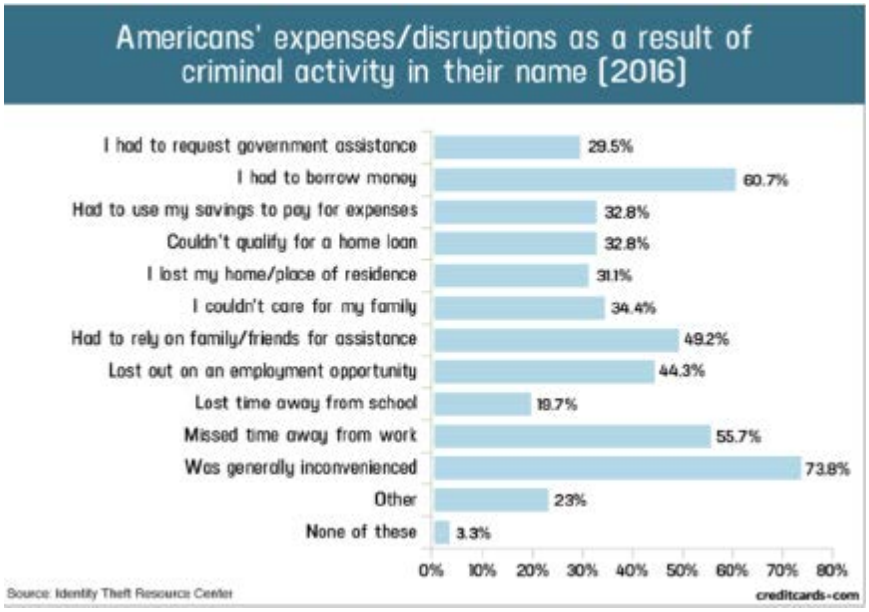
131. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office, who released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[50]

132. Plaintiff's mitigation efforts are also consistent with the steps that 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 consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their

[50] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[51]

133. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[52]



134. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") 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."[53]

135. Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting

[51] *See* FTC, IdentityTheft.com, https://www.identitytheft.gov/Steps (last accessed Sept. 11, 2023).

[52] Jason Steele, *Credit Card and ID Theft Statistics* (Oct. 24, 2017), available at https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed Sept. 11, 2023).

[53] *See supra* note 50, p. 2.

one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[54]

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

REPRESENTATIVE PLAINTIFF'S EXPERIENCE

137. Plaintiff Logan Aldridge has been a customer of PurFoods since approximately July 2022.

138. On or about August 25, 2023, Plaintiff Aldridge received the Notice informing him that his Private Information was compromised in the Data Breach.

139. Based upon the Notice of Data Breach letter that he received, Plaintiff's Private Information, including but not limited to his name, diagnosis code, health insurance information, meal category and/or cost, patient ID number, and treatment information, was acquired, stored and maintained by PurFoods, and was compromised in the Data Breach.

140. Since receiving the Notice, Plaintiff has been required to spend valuable time monitoring his various accounts and changing his account passwords in an effort to detect and to prevent any misuses of his Private Information—time which he would not have had to expend but for the Data Breach.

[54] *See* https://www.identitytheft.gov/Steps (last accessed Sept. 11, 2023).

141. As a result of the Data Breach, Plaintiff Aldridge will continue to be at heightened and certainly impending risk for fraud and identity theft and their attendant damages for years to come.

142. As a requisite to receiving goods and services, Plaintiff provided his Private Information to PurFoods and trusted that the information would be safeguarded according to state and federal law.

143. Upon receipt, Private Information was entered and stored on Defendant's network and systems.

144. Plaintiff is very careful about sharing his sensitive Private Information.

145. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information.

146. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents.

147. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

148. Had Plaintiff known that PurFoods failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

149. As a result of the Data Breach and the lack of detailed notification, Plaintiff is extremely anxious about the safety of his information.

150. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that he entrusted to Defendant, which was compromised in and as a result of the Data Breach.

151. He also lost his benefit of the bargain by paying for meal delivery services that failed to provide the data security that was promised.

152. Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

153. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

154. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

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

156. As a result of the Data Breach, Plaintiff heeded PurFoods' warning and spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred.

157. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at PurFoods' direction by way of the Data Breach notice where it advised Plaintiff to mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

158. Even with the best response, the harm caused to Plaintiff cannot be undone.

CLASS ALLEGATIONS

159. Plaintiff brings this class action individually, and on behalf of all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

160. Plaintiff seeks certification of the following class of persons defined as follows:

> **Nationwide Class**: All individuals in the United States whose Private Information was compromised in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach.

161. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.[55]

162. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at more than 1.2 million persons impacted by the Data Breach. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

163. **Commonality:** This action involves questions of law and fact common to the Class; such common questions include but are not limited to:

a. Whether Defendant failed to timely notify Plaintiff and Class Members of the Data Breach;

b. Whether Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

c. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' Private Information, and breached its duties thereby;

d. Whether Defendant was negligent in collecting and disclosing Plaintiff's and Class Members' Private Information to third-parties;

e. Whether Defendant entered into an implied contract with Plaintiff and Class Members;

[55] This proposed class definition is based on the information available to Plaintiff at this time, and she reserves the right to modify or to amend the class definition as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

f. Whether Defendant breached that contract by failing to adequately safeguard Plaintiff's and Class Members' Private Information;

g. Whether Defendant was unjustly enriched;

h. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct and

i. Whether Plaintiff and Class Members are entitled to declaratory judgment due to Defendant's wrongful conduct.

164. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class are all customers, employees or independent contractors of PurFoods, each having their Private Information exposed and/or accessed by an unauthorized third party.

165. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and Class Members are substantially identical as explained above.

166. **Superiority**: 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.

167. 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 a large company such as PurFoods. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose an avoidable burden on the courts.

168. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because PurFoods would necessarily gain an unconscionable advantage since it would be able to exploit and to 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 Plaintiff was 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.

169. Moreover, the litigation of the claims brought herein is manageable. PurFoods' uniform conduct, uniform methods of data collection, the consistent provisions of the relevant laws and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

170. 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 PurFoods owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether PurFoods breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether PurFoods failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between PurFoods on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether PurFoods breached the implied contract;

f. Whether PurFoods adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether PurFoods 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 PurFoods engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of PurFoods' wrongful conduct.

171. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class.

If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

172. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2). Unless a Class-wide injunction is issued, PurFoods may continue in their failure to properly secure the Private Information of Class Members, PurFoods may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and PurFoods may continue to act unlawfully as set forth in this Complaint.

173. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

IOWA LAW SHOULD APPLY TO ALL PLAINTIFF'S & CLASS MEMBERS' CLAIMS

174. The State of Iowa has a significant interest in regulating the conduct of businesses operating within its borders.

175. Iowa, which seeks to protect the rights and interests of Iowa and all residents and citizens of the United States against a company headquartered and doing business in Iowa, has a greater interest in the claims of Plaintiffs and Class Members than any other state and is most intimately concerned with the claims and outcome of this litigation.

176. The principal place of business and headquarters of PurFoods, located at 3210 SE Corporate Woods Drive in Ankeny, Iowa 50021, is the "nerve center" of its business activities—the place where its high-level officers direct, control and coordinate its activities, including major policy, financial and legal decisions.

177. PurFoods' actions and corporate decisions surrounding the allegations made in the Complaint were made from and in Iowa.

178. PurFoods' breaches of duty to Plaintiffs and Class Members emanated from Iowa.

179. Application of Iowa law to the asserted claims is neither arbitrary nor fundamentally unfair because choice of law principles which are applicable to this action mandate the application of Iowa law to the nationwide common law claims of all Class Members.

180. Additionally, given Iowa's significant interest in regulating the conduct of businesses operating within its borders, and that Iowa has the most significant relationship to Defendant, as it is headquartered in Iowa, there is no conflict in applying Iowa law to non-resident consumers such as Plaintiffs and Class Members.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff & the Nationwide Class)

181. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

182. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

183. PurFoods voluntarily assumed and therefore owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Private Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons.

184. In addition to voluntarily assuming a duty by collecting Plaintiff's and Class Members' Private Information, PurFoods' duty to use reasonable care arose from several sources including, but not limited to, those described herein.

185. PurFoods had a common law duty to prevent foreseeable harm to others.

186. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of PurFoods.

187. Defendant knew or should have known the risks of collecting and storing Plaintiff's and Class Members' Private Information and the importance of maintaining and using secure systems. Defendant knew or should have known of the many data breaches that have targeted companies that collected and stored Private Information in recent years.

188. Given the nature of Defendant's business, the sensitivity and value of the Private Information it maintains and the resources at its' disposal, PurFoods should have conducted more robust assessments of its network security, dedicated sufficient resources to detecting and addressing vulnerabilities in its systems in order to prevent the dissemination of Plaintiff's and Class Members' Private Information.

189. PurFoods makes statements on its website demonstrating its awareness of the risk of potential data breaches, that it will follow privacy laws and regulations and that it will use reasonable methods to protect the Private Information in its control.

190. By collecting and storing valuable Private Information that is routinely targeted by criminals for unauthorized access, PurFoods was obligated to act with reasonable care to protect against these foreseeable threats.

191. PurFoods breached the duties owed to Plaintiff and Class Members and thus was negligent.

192. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data

security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiff's and Class Members' Private Information.

193. Plaintiff and Class Members had no ability to protect their Private Information that was, or remains, in PurFoods's possession.

194. As a result of the Data Breach that compromised Plaintiff's and Class Members' Private Information, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of clients' information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its clients; and (h) failing to adequately train and supervise employees and/or third party vendors with access or credentials to systems and databases containing sensitive Private Information.

195. It was or should have been reasonably foreseeable to PurFoods that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software

and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

196. But for PurFoods' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Private Information would not have been compromised. The Private Information of Plaintiff and the Class was accessed and stolen as the proximate result of Defendant's failure to exercise reasonable care in safeguarding, securing, and protecting such Private Information.

197. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injuries, as set forth herein.

198. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive and/or nominal damages, in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff & the Nationwide Class)

199. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

200. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

201. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described herein also form part of the basis of PurFoods' duty in this regard.

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

203. PurFoods' conduct was particularly unreasonable given the nature and amount of Private Information it obtained, stored, and shared with third parties, and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

204. PurFoods' violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

206. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

207. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

208. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on

credit reports; (vii) the continued risk to their Private Information, which remains in PurFoods' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

209. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members 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.

210. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains 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 Private Information in its continued possession.

211. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members are entitled to recover actual, consequential and nominal damages.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff & the Nationwide Class)

212. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

213. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

214. When Plaintiff and Class Members provided their Private Information to PurFoods, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiff's and Class Members' Private Information, comply with its statutory and common law duties to protect Plaintiff's and Class Members' Private Information and to timely notify them in the event of a data breach.

215. PurFoods solicited and invited Plaintiff and Class Members to provide their Private Information as part of its business of selling and delivering pre-packaged meals. Plaintiff and Class Members accepted PurFoods' offers and provided their Private Information.

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

217. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that PurFoods' data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' Private Information and to timely notify them in the event of a data breach.

218. Plaintiff and Class Members paid money to PurFoods in exchange for goods and services, along with PurFoods' promise to protect their Private Information from unauthorized access and disclosure.

219. Plaintiff and Class Members reasonably believed and expected that PurFoods would use part of those funds to obtain adequate data security.

220. PurFoods did not do so.

221. Plaintiff and Class Members would not have provided their Private Information to PurFoods had they known that it would not safeguard their Private Information, as promised or provide timely notice of a data breach.

222. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with PurFoods.

223. PurFoods breached its implied contracts with Plaintiff and Class Members by failing to safeguard their Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

224. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their Private Information;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate,

mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

225. As a direct and proximate result of PurFoods' breach of contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive and/or nominal damages, in an amount to be proven at trial.

226. Plaintiff and Class Members are also entitled to injunctive relief requiring PurFoods to, *e.g.*, (i) strength its data security systems and monitoring procedures; (ii) submit to future annual

audits of those systems and monitoring procedures and (iii) immediately provide and continue to provide adequate credit monitoring to Plaintiff and all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff & the Nationwide Class)

227. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

228. Plaintiff brings this claim individually and on behalf of the Nationwide Class in the alternative to Count III above.

229. Upon information and belief, PurFoods funds its data security measures from its general revenue including monies received (in exchange for the provision of goods and services) from or on behalf of Plaintiff and Class Members.

230. As such, a portion of the payments made by or on behalf of Plaintiff 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.

231. Plaintiff and Class Members conferred a monetary benefit on Defendant.

232. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

233. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

234. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members Private

Information. Instead of providing a reasonable level of data security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective data security measures.

235. Under principles of equity and good conscience, PurFoods should not be permitted to retain the money belonging to Plaintiff and Class Members because PurFoods failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

236. Defendant failed to secure Plaintiff and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members conferred.

237. Defendant acquired Plaintiff's and Class Members' Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

238. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information.

239. Plaintiff and Class Members have no adequate remedy at law.

240. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered injuries, as set forth herein.

241. As a direct and proximate result of PurFoods' conduct, Plaintiff and Class Members 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 noneconomic losses.

242. PurFoods should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for PurFoods' goods and services.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff & the Nationwide Class)

243. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

244. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

245. At all times during Plaintiff's and Class Members' interactions with PurFoods, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information.

246. As alleged herein and above, PurFoods' relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Private Information would be collected, stored and protected in confidence, and would not be disclosed to unauthorized third parties.

247. Plaintiff and Class Members provided their Private Information to PurFoods with the explicit and implicit understandings that PurFoods would protect and not permit the Private Information to be disseminated to any unauthorized parties.

248. Plaintiff and Class Members also provided their Private Information to PurFoods with the explicit and implicit understandings that Defendant would take precautions to protect such Private Information from unauthorized disclosure.

249. Defendant voluntarily received in confidence Plaintiff's and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

250. Due to PurFoods' failure to prevent, detect or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security, Plaintiff's and Class Members'

Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence and without their express permission.

251. As a direct and proximate cause of PurFoods' actions and/or omissions, Plaintiff and Class Members have suffered damages.

252. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their protected Private Information would not have been compromised, stolen, viewed, accessed and used by unauthorized third parties.

253. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information, as well as the resulting damages.

254. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information.

COUNT VI
BAILMENT
(On Behalf of Plaintiff & the Nationwide Class)

255. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

256. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

257. Plaintiff and Class members delivered their Private Information to PurFoods to receive goods and services from Defendant.

258. The Private Information was furnished to PurFoods for the exclusive purpose of receiving the services PurFoods provides in the ordinary course of business, and Defendant took possession of the Private Information for the same reason.

259. Upon delivery, Plaintiff and Class Members intended and understood that PurFoods would adequately safeguard their Private Information, and PurFoods, in accepting possession, understood the expectations of Plaintiff and Class Members.

260. Accordingly, bailment was established for the mutual benefit of the parties at the time of delivery and acceptance of possession.

261. Pursuant to the bailment arrangement, PurFoods owed Plaintiff and Class members a duty of reasonable care in safeguarding and protecting their Private Information.

262. Defendant breached this duty by failing to take adequate steps to protect the Private Information entrusted to them and by failing to conform to best practices and industry standards to prevent unauthorized access to Plaintiff's and Class Members' Private Information.

263. As a result of Defendant's failure to fulfill its bailment arrangement, Plaintiff and Class members suffered and will continue to suffer injury, as set forth herein.

COUNT VII
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of Plaintiff & the Nationwide Class)

264. Plaintiff restates and realleges all preceding factual allegations as if fully set forth herein.

265. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

266. As a condition of obtaining goods and services from PurFoods, Plaintiff and Class Members provided their personal and financial information.

267. In so doing, Plaintiff and Class Members entered into implied contracts with PurFoods by which it agreed to safeguard and protect such information, to keep such information secure and confidential and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

268. PurFoods offered to provide goods and services to members of the Class in exchange for payment. PurFoods also required the members of the Class to provide PurFoods with their Private Information to receive those goods and services.

269. Plaintiff and Class Members fully performed their obligations under the implied contracts with PurFoods.

270. Had Plaintiff and Class Members known that PurFoods would not adequately protect their Private Information, Plaintiff and members of the Class would not have entrusted PurFoods with their Private Information.

271. PurFoods represented to Plaintiff and Class Members, implicitly and otherwise, that their Private Information would be secure.

272. Plaintiff and Class Members relied on such representations when they agreed to provide their Private Information to PurFoods.

273. Plaintiff and Class Members would not have entrusted their Private Information to PurFoods without such agreement with PurFoods.

274. The covenant of good faith and fair dealing is an element of every contract.

275. All such contracts impose on each party a duty of good faith and fair dealing.

276. The parties must act with honesty in fact in the conduct or transactions concerned.

277. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain.

278. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

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

280. PurFoods failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

281. PurFoods' duty to safeguard Plaintiff's and Class Member's Private Information is inherent in and consistent with the contracts entered into by PurFoods and Plaintiff and Class Members.

282. PurFoods would not have suffered harm by enacting industry standard measures to safeguard Plaintiff's and Class Member's Private Information.

283. PurFoods' failure to enact reasonable safeguards to protect the Private Information it collected resulted in harm to Plaintiff and Class Members and violated the covenant of good faith and fair dealing.

284. Plaintiff and Class Members have sustained damages because of PurFoods' breaches of their agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

285. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of implied contract of good faith and fair dealing, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Logan Aldridge, individually and on behalf of all others similarly situated, prays for judgment in his favor and against PurFoods and respectfully requests the following relief:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff reasonable attorneys' fees, costs and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: September 13, 2023

Respectfully submitted,

/s/ Timothy M. Hansen
Timothy M. Hansen, AT0010747
HANSEN REYNOLDS LLC
301 N. Broadway, #400
Milwaukee, WI 53202
Tel: (414) 273-8473
thansen@hansenreynolds.com

/s/ Nicholas J. Mauro
Nicholas J. Mauro, AT0005007
CARNEY & APPLEBY LAW FIRM
303 Locust St., #400
Des Moines, IA 50309
Tel: (515) 282-6803
mauro@carneyappleby.com

ClassAction.org