E-FILED
Wednesday, 31 August, 2022 11:02:46 AM
Clerk, U.S. District Court, ILCD

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF ILLINOIS

LESLIE GREEN, individually and on behalf of all others similarly situated, Plaintiff, v. AFNI, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Leslie Green ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through counsel, file this Class Action Complaint against Afni, Inc. ("Afni" or "Defendant") and allege the following based on personal knowledge of facts pertaining to her and on information and belief based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. Afni provides customer service assistance to its clients, including debt collection services and customer interaction services.

2. Plaintiff and the Class Members (as further defined below) have had their personal identifiable information exposed as a result of Afni's inadequately secured computer network. Defendant betrayed the trust of Plaintiff and the other Class Members by failing to properly safeguard and protect their personal identifiable information and thereby enabling cyber criminals to steal such valuable and sensitive information.

3. This class action seeks to redress Afni's unlawful, willful and wanton failure to protect the personal identifiable information of approximately 261,449 individuals that was exposed in a major data breach of Defendant's network (the "Data Breach" or "Breach"), in violation of its legal obligations.[1]

4. The Data Breach was discovered on June 7, 2021, when Afni discovered suspicious activity on its systems.[2] Afni investigated the attack with the assistance of third-party computer specialists. The investigation confirmed that certain Afni systems containing confidential and personal information had been accessed without authorization.[3]

5. According to Afni, the personal identifiable information exposed in the Breach included: names, addresses, Social Security numbers, and birth dates (the "PII").[4]

6. Due to Defendant's negligence, cyber criminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of hundreds of thousands of individuals.

7. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/22f470bc-511d-4067-911d-bbf0b230e9c6.shtml.

[2] *See* Afni's breach notification letter, attached as Exhibit 1.

[3] *Id.*

[4] *Id.*

harm, damaged credit, deprivation of the value of their of PII, loss of privacy, and/or additional damages as described below.

8. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

Plaintiff

9. Plaintiff Leslie Green is domiciled in and a citizen of Michigan.

10. On or around July 29, 2022, Plaintiff received a breach notification letter from Afni informing her that her personal information, including name, address, Social Security Number, and date of birth had been exposed to cybercriminals during the Data Breach.

Defendant

11. Defendant Afni is an Illinois corporation with its principal place of business located at 1310 Martin Luther King Jr. Dr., Bloomington, Illinois 61701.

12. Afni provides customer service assistance to its clients, including debt collection services and customer interaction services.

III. JURISDICTION AND VENUE

13. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

14. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and many Class Members reside in this District. Venue is likewise proper as to Defendant in this District because Defendant employs a significant number of Class Members in this District, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. The Data Breach

15. Based on information supplied by Defendant, the Data Breach was discovered on June 7, 2021, when Afni discovered suspicious activity on its systems.[5] Afni investigated the attack with the assistance of third-party computer specialists. The investigation confirmed that certain Afni systems containing confidential and personal information had been accessed without authorization.[6]

16. According to Afni, the exposed PII included names, addresses, Social Security numbers, and birth dates.[7]

17. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized disclosure. Defendant's actions represent a flagrant disregard of the rights of the Class Members, both as to privacy and property.

B. Plaintiff's Experience

18. On or around July 29, 2022, Plaintiff received a breach notification letter from Afni informing her that her personal information, including name, address, Social Security Number,

[5] *See* Afni's breach notification letter, attached as Exhibit 1.

[6] *Id.*

[7] *Id.*

and date of birth had been exposed to cybercriminals during the Data Breach. The letter Plaintiff received is attached as Exhibit 1 hereto.

19. Plaintiff and Class Members' PII was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

20. Because of the Data Breach, Plaintiff's PII is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

21. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, monitoring her accounts and personal information, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff received from Afni specifically directed her to take these actions.[8]

22. As a direct and proximate result of the Data Breach, Plaintiff will likely need to purchase a lifetime subscription for identity theft protection and credit monitoring.

23. Plaintiff has been careful to protect and monitor her identity.

24. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's PII that was entrusted to Defendant for the sole purpose of obtaining medical services with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the

[8] *See* Exhibit 1, attached hereto.

bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

C. Cyber Criminals Have Used and Will Continue to Use Plaintiff's PII to Defraud Them

25. PII 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.

26. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[9] For example, with the PII stolen in the Data Breach, including Social Security numbers, 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.[10] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

[9] "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").

[10] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

27. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[11]
>
> [Emphasis added.]

28. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[12]

29. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like Afni is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[13] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[14]

30. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[15]

---

[11] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[12] *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/assets/270/262904.htmlu.

[13] 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.

[14] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[15] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

31. Hackers may not use the information right away, but this does not mean it will not be 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.[16]

32. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[17]

33. The ramifications of Defendant's failure to keep its Class Members' PII secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

34. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

35. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [18] 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

---

[16] *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/assets/270/262904.htmlu.

[17] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[18] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[19]

36. 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.[20]

37. Defendant's offer of limited identity monitoring to Plaintiff and the Class is woefully inadequate and will not fully protect Plaintiff from the damages and harm caused by its failures. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. Once the offered coverage has expired, 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 Afni's gross negligence. 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 PII)—it does not prevent identity theft.[21] Nor can an identity monitoring service remove personal information from the dark web.[22] "The 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."[23]

---

[19] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"), available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[20] "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.

[21] *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.

[22] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[23] *Id.*

38. As a direct and proximate result of the Data Breach, Plaintiff and the Class have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. 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. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

39. Plaintiff and the Class 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 PII;
c. Improper disclosure of their PII;
d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and 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 PII 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' personal information for which there is a well-established and quantifiable national and international market;

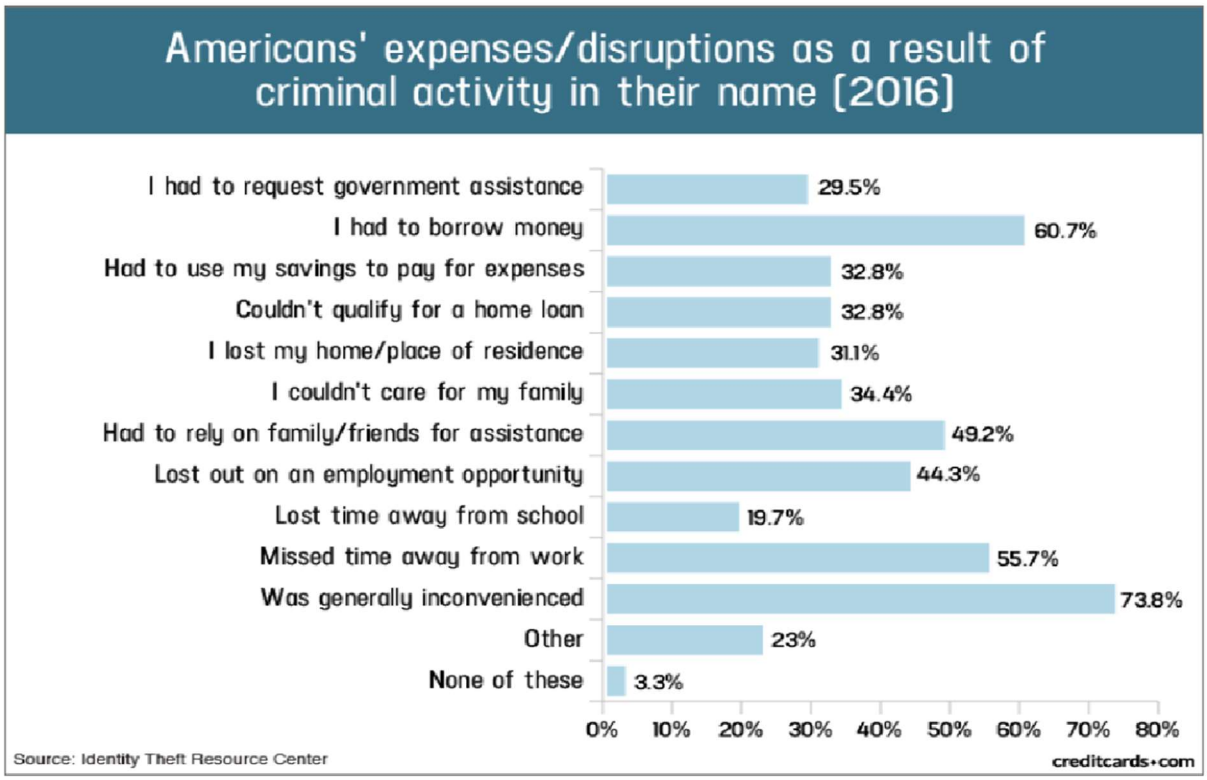
i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

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

40. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[24]:

[24] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



41. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's PII.

42. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to Afni is removed from Afni's unencrypted files.

43. Defendant acknowledged, in its letter to Plaintiff and other Class Members, that the Data Breach would cause "inconvenience" to effected individuals by providing numerous "steps" for Class Members to take in an attempt to mitigate the harm caused by the Data Breach.[25]

[25] *See* Exhibit 1, attached hereto.

44. The letter further acknowledge that financial harm would likely occur, stating: "We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information…. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statement and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution."[26]

45. At Afni's suggestion, Plaintiff is desperately trying to mitigate the damage that Afni has caused her. Given the kind of PII Afni made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have her PII, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[27]

46. None of this should have happened.

D. Defendant was Aware of the Risk of Cyber Attacks

47. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

[26] *Id.*

[27] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

of the biggest cybersecurity breaches: Target,[28] Yahoo,[29] Marriott International,[30] Chipotle, Chili's, Arby's,[31] and others.[32]

48. Afni should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

49. Indeed, Afni's Privacy Policy states the following:

> Afni, Inc. is committed to protecting any personal information that you may provide to us.
>
> ***
>
> We do not share, sell, or lease personal information about you to any third-parties for their marketing use. We will release information about you if you direct us to do so, if we are required by law to do so, or in other legally limited circumstances.[33]

50. Afni's assurances make it evident that Afni recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained. Yet, it appears that Afni did not meaningfully or comprehensively use the reasonable measures, including the measures it claims to utilize.

---

[28] 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/.

[29] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[30] 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/.

[31] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[32] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[33] *See* https://afni.com/privacy-policy#:~:text=We%20do%20not%20share%2C%20sell,in%20other%20legally%20limited%20circumstances.

51. Afni was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

E. Afni Could Have Prevented the Data Breach

52. Data breaches are preventable.[34] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[35] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[36]

53. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[37]

54. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[38] The guidelines

[34] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[35] *Id.* at 17.

[36] *Id.* at 28.

[37] *Id.*

[38] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

establish that businesses should protect the confidential 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 for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

55. Upon information and belief, Afni failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Afni also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

56. 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."[39]

57. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

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

[39] *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.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

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

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

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

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

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

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

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

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

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

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[40]

58. Further, to prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

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

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

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

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

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

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

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

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[41]

59. In addition, to prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant 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;
- **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

[41] *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.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[42]

60. Given that Defendant was storing the Confidential Information of more than 260,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect malicious cyberattacks.

61. Specifically, among other failures, Afni had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[43] Indeed, the United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[44]

62. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information. Further, the Data Breach could have likely been prevented had Defendant utilized appropriate malware prevention and detection technologies.

F. Defendant's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

63. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

---

[42] *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/.

[43] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[44] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

64. Defendant stated that it discovered the Data Breach in June 2021. And yet, Afni did not notify affected individuals until July 2022—*more than a year after it learned of the Data Breach*. Even then, Afni failed to inform Plaintiff and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiff and Class Members unsure as to the scope of information that was compromised.

65. During these intervals, the cybercriminals were exploiting the information while Afni was secretly still investigating the Data Breach.

66. If Afni had investigated the Data Breach more diligently and reported it sooner, Plaintiff and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

V. CLASS ACTION ALLEGATIONS

67. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

68. Plaintiff brings this action against Afni on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> All persons Afni, Inc. identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

69. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

70. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

71. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

72. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals affected in the Data Breach was 521,046 individuals.

73. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Afni's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Afni.

74. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

75. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Afni's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues

of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

76. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Afni breached its duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Afni failed to provide adequate cyber security;

f. Whether Afni knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

g. Whether Afni's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Afni was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;

i. Whether Afni was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;

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

k. Whether Afni continues to breach duties to Plaintiff and the Class;

l. Whether Plaintiff and the Class suffered injury as a proximate result of Afni's negligent actions or failures to act;

m. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

n. Whether Afni's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiff and the Class)

77. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

78. Defendant Afni solicited, gathered, and stored the PII of Plaintiff and the Class.

79. Defendant had full knowledge of the sensitivity of the PII it maintained and of the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their PII that was in Afni's possession. As such, a special relationship existed between Afni and Plaintiff and the Class.

80. Defendant was well aware of the fact that cyber criminals routinely target corporations, particularly those servicing the health industry, through cyberattacks in an attempt to steal the collected PII.

81. Defendant owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

82. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

83. Defendant had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks, including by encrypting documents containing PII, by not permitting documents containing unencrypted PII to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive PII. Additional duties that Afni owed Plaintiff and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;
b. To protect the PII in its possession using reasonable and adequate security procedures and systems;
c. To adequately and properly audit and test its systems;

d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

e. To train its employees not to store PII for longer than absolutely necessary;

f. To implement processes to quickly detect a data breach, security incident, or intrusion; and

g. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

84. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Afni. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

85. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit and test its computer systems to avoid cyberattacks;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII, including maintaining it in an encrypted format;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's PII;

f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

g. Failing to abide by reasonable retention and destruction policies for PII it collects and stores; and

h. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their PII.

86. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

87. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

88. The damages Plaintiff and the Class have suffered (as alleged above) were and are reasonably foreseeable.

89. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

90. Plaintiff and the Class have suffered injury, including as described in Section IV.B, *supra*, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of all Plaintiff and the Class)

91. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

92. Through the use of Plaintiff's and Class Members' PII, Defendant received monetary benefits.

93. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and Class Members.

94. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

95. However, acceptance of the benefit under the facts and circumstances described herein make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of 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 security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

96. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement the appropriate data management and security measures.

97. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

98. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to allow Defendant to have or maintain their PII.

99. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class members suffered and continue to suffer actual

damages, including (i) the amount of the savings and costs Defendant reasonably should have expended on data security measures to secure Plaintiff's PII, (ii) time and expenses mitigating harms, (iii) diminished value of the PII, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

100. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

101. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of all Plaintiff and the Class)

102. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

103. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII in order for Afni to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' PII and to timely notify them in the event of a data breach.

104. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

105. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

106. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

107. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members.

FOURTH CAUSE OF ACTION
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("CFA")
815 ILCS 505/2, *ET. SEQ.*
(On Behalf of all Plaintiff and the Class)

108. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

109. Plaintiff and the Class Members are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, Class Members, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

110. Defendant is engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

111. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff and Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting material facts to Plaintiff and Class Members regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and Class Members; (3) failing to disclose or omitting material facts to Plaintiff and Class Members about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and Class Members; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Class Members' PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

112. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and Class Members and defeat their reasonable expectations about the security of their PII.

113. Moreover, Defendant represented that they would maintain the data they collected in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration. Defendant intended that Plaintiff and Class Members rely on their deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

114. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to Class Members. Plaintiff and Class Members have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

115. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and Class Members of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

116. As a result of Defendant's wrongful conduct, Plaintiff and Class Members were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

117. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and Class Members have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant that Plaintiff and Class Members would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

118. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and Class Members seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

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

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

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

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

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

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

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: August 31, 2022

Respectfully submitted,

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Attorneys for Plaintiff

**Pro hac vice* applications forthcoming

E-FILED
Wednesday, 31 August, 2022 11:02:47 AM
Clerk, U.S. District Court, ILCD

EXHIBIT 1

DEPT 555
PO BOX 4115
CONCORD CA 94524

July 26, 2022

ADDRESS SERVICE REQUESTED

LESLIE GREEN
[redacted]

afni.
Office Address:
PO Box 3517
Attention: SDP
Bloomington, IL 61702
Monday - Friday 8:00am - 5:00pm Central

NOTICE DATE: July 29, 2022

Ref. No. [redacted]

NOTICE OF SECURITY INCIDENT

Dear LESLIE GREEN,

Afni, Inc. ("Afni") is writing to inform you of an event that may impact the security of some of your information. Although we have received no indication of any actual or attempted identity theft or fraud of your personal information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On June 7, 2021, Afni discovered anomalous activity within its computer network. Afni immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or before June 7, 2021, an unauthorized actor gained access to certain Afni systems and that the unauthorized actor may have viewed or taken data from within those systems. Therefore, we conducted a thorough and in-depth review of the information within those systems to identify individuals with personal information that was potentially accessible. On June 2nd, 2022, Afni finalized this review to confirm the nature and scope of impacted data and the individuals to whom that data related. Although we are unaware of any actual or attempted identity theft or fraud of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, address, and social security number may have been accessible.

What We Are Doing? The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we investigated and responded to the event, assessed the security of our systems, and notified potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause.

What You Can Do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statement and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed Steps You Can Take To Protect Personal Information.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-833-840-0917, Monday through Friday from 8:00 am through 5:00 pm Central Time, excluding major U.S. holidays. Again, we take the privacy and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Mike Schwermin
Chief Information Officer

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

LESLIE GREEN, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Gary M. Klinger (866) 252-0878
Milberg Coleman Bryson Phillips Grossman PLLC,
227 W. Monroe St., Ste. 2100, Chicago, IL 60606

DEFENDANTS

AFNI, INC.

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

unknown

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Class Action Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Hon. James E. Shadid DOCKET NUMBER 1:22-cv-1287-JES-JEH

DATE
Aug 31, 2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ Gary M. Klinger

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

E-FILED
Wednesday, 31 August, 2022 11:02:47 AM
Clerk, U.S. District Court, ILCD

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Central District of Illinois

LESLIE GREEN, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

AFNI, INC.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* AFNI, INC.
c/o Registered Agent
C T CORPORATION SYSTEM
208 SO LASALLE ST, SUITE 814
CHICAGO , IL 60604

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 West Monroe Street, Suite 2100
Chicago, IL 60606

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

ClassAction.org