UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
Orlando Division

SHANNON ARBUTHNOT, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ACUITY – CHS, LLC f/k/a COMPREHENSIVE HEALTH SERVICES LLC
8600 Astronaut Blvd.
Cape Canaveral, Florida 32920

Defendant.

Case No. _____

JURY DEMAND

CONSUMER CLASS ACTION COMPLAINT

Plaintiff SHANNON ABUTHNOT ("Plaintiff") brings this Class Action Complaint against ACUITY – CHS, LLC f/k/a COMPREHENSIVE HEALTH SERVICES LLC ("Defendant" or "CHS"), in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendant, a subsidiary of Acuity International, a provider of professional services, specialized consulting, engineering, medical, and environmental solutions, and large-scale program management services for the U.S. government and commercial clients in the national defense, healthcare, international diplomacy, and homeland security markets.

2. CHS failed to reasonably secure, monitor, and maintain Personally Identifiable

Information ("PII") provided by Plaintiff and Class Members, including, without limitation, names and Social Security numbers stored on its private network. As a result, Plaintiff and other Class Member suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. Moreover, after learning of the Data Breach, Defendant waited over sixteen (16) months (from September 30, 2020 to February 15, 2022) to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

5. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to take reasonable steps to protect the PII of Plaintiff and Class Members and warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized

disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

6. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, present, concrete injuries. These injuries include: (i) actual misuse of the stolen PII; (ii) the current and imminent risk of fraud and identity theft (iii) lost or diminished value of PII ; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vii) the invasion of privacy; (viii) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Members' PII; and (ix) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

7. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

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

II. PARTIES

Plaintiff Shannon Arbuthnot

9. Plaintiff Shannon Arbuthnot is, and at all times relevant has been, a resident and citizen of Arizona, where she intends to remain. Plaintiff received a "Notice of Data Security Incident" letter dated February 15, 2022, on or about that date.

10. The letter notified Plaintiff that on some unidentified date, CHS detected suspicious activity on its computer network.

11. After an investigation, CHS determined that Plaintiff's information was compromised in the Data Breach by the unauthorized access. The files subject to unauthorized access contained Plaintiff's names and Social Security number.

12. The letter further advised Plaintiff that she should spend time mitigating her losses by taking steps to help safeguard her information, including signing up for 24-months of credit and identity monitoring through Equifax. Upon information and belief, the credit and identity monitoring offered is only single bureau credit monitoring.

13. Defendant obtained and continues to maintain Plaintiff's and Class Members' PII and has a continuing legal duty and obligation to protect that sensitive information from unauthorized access and disclosure. Plaintiff would not have entrusted her PII to Defendant had she known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

Defendant Acutity – CHS, LLC

14. Defendant CHS is Delaware limited liability company with a principal place of business at 8600 Astronaut Blvd., Cape Canaveral, Florida 32920.

15. Defendant CHS is a wholly owned subsidiary of Acuity International, and provides

occupational health services including physical examinations as part of the pre-hiring process for various employers, including the federal government and its agencies like the Transportation Safety Administration (TSA).

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members (including Plaintiff Arbuthnot, a citizen of Arizona) are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

18. This Court has personal jurisdiction over CHS because it is headquartered in and maintains its principal place of business in this District. CHS is authorized to and regularly conducts business in Florida. In this District, CHS makes decisions regarding corporate governance and management of its business, including decisions regarding the security measures to protect its customers' PII. CHS intentionally avails itself of this jurisdiction by promoting, selling and marketing its services from Florida . Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because CHS's headquarters and principal place of business are located in this District, CHS resides in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made

by CHS's governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Data Breach.

IV. FACTUAL ALLEGATIONS

Background

19. Defendant provides occupational health services, including pre-employment physical examinations, to a wide variety of employers, prospective employers, and former employers, including TSA.

20. Plaintiff and Class Members were persons who provided, or who third-parties provided on their behalf, their PII to Defendant in conjunction with utilizing occupational health services.

21. Specifically, Plaintiff Arbuthnot provided her PII (including her name, address, cell phone number, email address, driver's license number, medical history, Social Security number, and birthdate) to Defendant as part of the pre-employment vetting process that Defendant conducted in connection with Plaintiff's application for employment with the TSA.

22. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

23. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. As such, CHS has a legal duty to keep consumer's PII safe and confidential.

24. The information held by Defendant in its computer systems and networks (including its invoicing files pre-dating 2019) included the unencrypted PII of Plaintiff and Class Members.

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

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, CHS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

27. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

The Data Breach

28. On September 30, 2020, CHS detected unusual activity within its digital environment following discovery of multiple fraudulent wire transfers.

29. Upon discovering this activity, CHS engaged a team of cybersecurity experts in an attempt to secure the digital environment and conduct a forensic investigation to determine the method of initial compromise and access, the scope of the incident, what systems were impacted and whether any PII was accessed or exfiltrated as a result of the incident.

30. Following review and analysis of the information impacted by the incident, and as a result of the investigation, CHS determined on November 3, 2021 that the PII of a number of individuals employed by one or more of its customers was accessed, compromised, and acquired by a malicious actor.

31. To date, CHS has not revealed most (if not all) of the findings of the investigation it commissioned. CHS has not revealed when the unauthorized actor first gained access to CHS's

networks, nor has it revealed the mechanism by which the unauthorized actor first gained access to CHS's networks. CHS has not revealed whether the unauthorized actor accessed any files other than pre-2019 invoicing files for certain CHS clients.

32. Even worse, CHS has failed to disclose the exact nature of the unauthorized access to Plaintiff's and Class Members' PII. Instead, CHS speaks in generalities and equivocations, claiming that it only knows that pre-2019 invoicing files containing PII "may have been accessed or acquired without authorization," and that Plaintiff's name and Social Security number "may have been accessed or acquired during the incident."

33. Upon information and belief, Defendant knows full well that it is likely, if not certain, that Plaintiff's and Class Members' PII was accessed and acquired by unauthorized, malicious actors during this Data Breach.

34. Defendant's "disclosure" – delivered a shocking sixteen and a half months after the Data Breach was first discovered -- amounts to no real disclosure at all.

35. Defendant's offering of 24-months of credit and identity monitoring belies Defendant's equivocal statements that Plaintiff's and Class Members' PII "may have been accessed and acquired," and instead establishes that Plaintiff's and Class Members' sensitive PII was in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

36. According to disclosures made to States' Attorney Generals, the unauthorized actor gained access to CHS's networks on April 9, 2020, and continued to have access until October 22, 2020, well after the September 30, 2020 date that the intrusion was first discovered by CHS. This means that the unauthorized actor had unfettered and undetected access to Defendant's networks (and the ability to spread laterally throughout Defendant's networks) for nearly ***six months*** prior

to CHS becoming aware of the unauthorized access to its computer systems and network, and for nearly a month ***after*** the Data Breach was discovered.

37. The failure to discover the unauthorized intrusion into its computer networks and systems demonstrates a complete failure by Defendant to monitor its own computer systems, and a complete failure to implement proper information security practices, procedures, and protocols.

38. The investigation commissioned by CHS did not conclude until November 3, 2021, and notice was not sent to victims of the data breach until over three months after that. Thus, the victims of this Data Breach, including Plaintiff and Class Members, were not sent notice of this Data Breach until approximately sixteen and a half (16.5) months after CHS first knew about this Data Breach, and not until three and a half (3.5 months) after the investigation was concluded.

39. Defendant's "disclosure" or notice letter claims that there is no evidence that the PII accessed and acquired by malicious actors was misused However, upon information and belief, CHS has no methods, policies, or procedures in place that would afford person like Plaintiff and Class Members any mechanism or opportunity to report misuse of the data back to CHS. The investigation commissioned by CHS did not survey CHS's clients whose data was breached for evidence of misuse, nor were the persons (like Plaintiff) whose data was accessed and acquired by the malicious actors ever contacted by CHS to inquire about any misuse of their data.

40. The attacker accessed and acquired files (including without limitation pre-2019 invoicing files) containing unencrypted PII of Plaintiff and Class Members, including names, and Social Security numbers.

41. On or around February 15, 2022, Defendant disclosed the Data Breach to multiple States' Attorney Generals, including the Maine Attorney General.

42. CHS first notified its impacted consumers of the incident on or around February 15,

2022, sending written notifications to individuals whose personal information was compromised in the Data Breach.

43. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

44. Plaintiff further believes her PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain 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.

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

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

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

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

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

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

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

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[1]

47. To prevent and detect cyber-attacks attacks 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

[1] *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 visited Nov. 11, 2021).

- 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].[2]

48. To prevent this Data Breach, Defendant could and should have implemented and employed the following basic data security protections: 1) implementing robust and up-to-date endpoint detection and response tools, and installing this software on all servers and endpoints on the network enterprise; 2) employing an adequate and up-to-date threat detection and monitoring surveillance vendor; 3) implementing capabilities for extended detection and response to attempted network intrusions; and 4) conducting network penetration testing.

49. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

50. The occurrence of the Data Breach, and Defendant's changes to its data security procedures, processes, and protocols after the Data Breach, indicates that Defendant failed to adequately implement one or more of the above measures to prevent this cyberattack, resulting in the Data Breach and the exposure of the Plaintiff's and Class Members' PII.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

51. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

52. Defendant retains and stores this information, and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII,

[2] *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 visited Nov. 11, 2021).

Defendant would be unable to perform its occupational health services.

53. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

54. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

55. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

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

57. Defendant knew and understood unprotected or exposed PII in the custody of business entities such as Defendant is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access, as occupational health service companies maintain highly sensitive PII, including Social Security numbers and health information.

Value of Personally Identifiable Information

58. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[3] The FTC describes "identifying information" as "any name or number that may be used, alone or

[3] 17 C.F.R. § 248.201 (2013).

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."[4]

59. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. 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.[5] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[6] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[7]

60. Social Security numbers, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[8]

---

[4] *Id*.
[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 19, 2022).
[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan 19, 2022).
[7] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 19, 2022).
[8] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 19, 2022).

61. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[9]

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, addresses, and financial information.

64. 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 and Social Security numbers are worth more than 10x on the black market."[10]

65. Among other forms of fraud, identity thieves may use Social Security numbers to

[9] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 19, 2022).

[10] 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 visited Nov. 11, 2021).

obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

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

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

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

69. In the breach notification letter, Defendant made an offer of 24 months of single bureau credit and identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

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

71. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant Violated the FTC Act

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

73. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Plaintiff Shannon Arbuthnot's Experience

74. Based upon the Notice of Data Breach letter that she received, Plaintiff's PII, including her name and Social Security Numbers was acquired, stored, and maintained by Defendant.

75. After the Data Breach, Plaintiff Arbuthnot has suffered from the actual misuse of the data stolen in this Data Breach. Unauthorized persons requested a promotional check for Dish Network that appeared on her credit in February 2022. Also, in November 2021 and again on January 29, 2022, there were unauthorized requests for information from OneMain Financial (a company with whom Plaintiff Arbuthnot has never done business) that also showed up on her

credit report. Ms. Arbuthnot was notified by Equifax of these issues on her credit report. These unauthorized activities are all easily accomplished utilizing Ms. Arbuthnot's name and Social Security number, the precise information stolen in this Data Breach, and a fairly traceable to this Data Breach.

76. Also, she has seen a marked increase in spam emails, texts, and phone calls that she believes are related to this Data Breach, due to the timing of the increase. At least one of the spam phone calls came from a number that, when searched on the internet, returned a Google search result as being related to "CHS." The spam texts and emails are often of a pornographic nature, and misgender Ms. Arbuthnot as a man

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

78. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack.

79. The fraud and identity monitoring services offered by Defendant are only for 24-months, 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 timely issues when the service number for enrollment does not work properly. Although Plaintiff Arbuthnot was able to successfully sign up for the Equifax service offered by Defendant, this service only lasts for 24-months, and has not prevented any attempted fraud activities, but merely has reported them after they occurred.

80. Plaintiff and Class Members have been further damaged by the compromise of their PII.

81. Plaintiff Arbuthnot's PII was compromised in the Data Breach, and was likely stolen and in the hands of cybercriminals who illegally accessed CHS network for the specific purpose of targeting the PII.

82. Plaintiff Arbuthnot typically takes measures to protect her PII, and is very careful about sharing her PII. Arbuthnot has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

83. Plaintiff Arbuthnot stores any documents containing her PII in a safe and secure location, and she diligently chooses unique usernames and passwords for her online accounts.

84. To her knowledge, Plaintiff Arbuthnot has never received any data breach notices from any other company.

85. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She has spent at least 8 hours monitoring her accounts and credit scores, she searches every suspicious phone number that calls her on Google, she searches for herself on the internet to see if there is any evidence of suspicious activity, as well as researching how she has been impacted by the Data Breach. In addition, Plaintiff has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

86. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

87. 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 her privacy.

88. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security Number being placed in the hands of criminals.

89. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff would not have entrusted her PII to Defendant had she known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

90. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

91. Plaintiff brings this suit on behalf of herself and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

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

92. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

93. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time,

public news reports indicate that approximately 106,910 individuals had their PII compromised in this Data Breach. The identities of Class Members are ascertainable through CHS's records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether CHS unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

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

c. Whether CHS data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether CHS data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether CHS owed a duty to Plaintiff and Class Members to safeguard their PII;

f. Whether CHS breached its duty to Plaintiff and Class Members to safeguard their PII;

g. Whether computer hackers obtained Plaintiff's and Class Members' PII in the Data Breach;

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

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of CHS's misconduct;

j. Whether CHS's conduct was negligent;

k. Whether CHS's conduct was *per se* negligent, and;

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

95. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

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

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

98. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to

individual Class Members, which would establish incompatible standards of conduct for CHS. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

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

100. Likewise, particular issues under Federal 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 CHS owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether CHS's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether CHS's failure to institute adequate protective security measures amounted to negligence;

d. Whether CHS failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

101. Finally, all members of the proposed Class are readily ascertainable. CHS has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by CHS.

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

102. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 101.

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

104. CHS had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

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

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

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

108. CHS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within CHS's possession.

109. CHS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

110. CHS, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within CHS's possession might have been compromised and precisely the type of information compromised.

111. CHS's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

112. As a result of CHS's ongoing failure to notify Plaintiff and Class Members regarding the type of PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

113. CHS's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

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

115. Plaintiff seeks the award of actual damages on behalf of herself and the Class.

116. In failing to secure Plaintiff's and Class Members' PII and promptly notifying them of the Data Breach, CHS is guilty of oppression, fraud, or malice, in that CHS acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of herself and the Class.

117. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling CHS to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

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

118. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 101.

119. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

120. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

121. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing (or having third-parties provide on their behalf) their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

122. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

123. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

124. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

125. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

126. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

127. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, nominal damages, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

128. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 101.

129. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice

by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

130. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

131. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

132. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

133. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty 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 suffered by Plaintiff and Class Members.

134. As a direct and proximate result of Defendant CHS's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach

reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

PRAYER FOR RELIEF

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

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

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

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

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

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to

the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

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

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

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

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

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

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

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

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

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

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

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

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

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2

Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

April 4, 2022

Respectfully, submitted,

/s/ John A. Yanchunis

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis (FL Bar No. 324681)
Patrick A. Barthle (FL Bar No. 99286)
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-2434
jyanchunis@forthepeople.com
pbarthle@forthepeople.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878

Facsimile: (202) 686-2877
dlietz@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice applications forthcoming*

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
SHANNON ARBUTHNOT

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Morgan and Morgan Complex Litigation Group, 201 N. Franklin St., 7th Fl, Tampa, FL 33602, 813.223.5505

DEFENDANTS
ACUITY - CHS, LLC

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)*

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

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

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

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

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

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:
Negligence, Unjust Enrichment, and Negligence per se

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5000000

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

VIII. RELATED CASE(S) IF ANY *(See instructions):*

JUDGE _____ DOCKET NUMBER _____

DATE
Apr 4, 2022

SIGNATURE OF ATTORNEY OF RECORD
/s/ John A. Yanchunis

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

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

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

SHANNON ARBUTHNOT, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

ACUITY - CHS, LLC

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* ACUITY - CHS, LLC
c/o Registered Agent
UNITED AGENT GROUP INC.
801 US HIGHWAY 1
NORTH PALM BEACH, FL 33408

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: MORGAN & MORGAN COMPLEX LITIGATION GROUP
John A. Yanchunis
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
jyanchunis@forthepeople.com

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: