JUNE WALTROP
c/o Murphy, Falcon & Murphy
1 South Street
30th Floor
Baltimore, Maryland 21202

WILLIAM WALTROP
c/o Murphy, Falcon & Murphy
1 South Street
30th Floor
Baltimore, Maryland 21202

Plaintiffs

v.

MARYLAND HEALTH ENTERPRISES, INC., d/b/a LORIEN HEALTH SERVICES
1205 York Road
Lutherville, MD 21093

SERVE ON:

Resident Agent
LINDA M. LICATA
1205 York Road
Penthouse Suite
Lutherville, MD 21093

Defendant

IN THE

CIRCUIT COURT

FOR

BALTIMORE COUNTY

CASE NO. C-03-CV-21-001062

* * * * * * * * * * * * *

CLASS ACTION COMPLAINT, DEMAND FOR JURY TRIAL, AND REQUEST FOR INJUNCTIVE RELIEF

Plaintiffs William Waltrop and June Waltrop, individually and on behalf of all others similarly situated (collectively, "Plaintiffs"), by and through their undersigned counsel, hereby file this Class Action Complaint against Defendant Maryland Health Enterprises, Inc., d/b/a Lorien Health Services, and in support, state as follows:

JURISDICTION & VENUE

1. Jurisdiction is proper in the Circuit Court for Baltimore County pursuant to Md. Code Ann., Cts. & Jud. Proc. § 6-102, because Defendant is organized under the laws of the State of Maryland and/or maintains its principal place of business in Maryland.

2. Venue, as conferred under Md. Code Ann., Cts. & Jud. Proc. §§ 6-201 and 6-202, is proper in Baltimore County because Defendant either resides in and/or carries on regular business in Baltimore County, Maryland.

3. The amount of this claim exceeds $30,000.00.

4. This case is not removable to federal court because Plaintiffs, all putative class members (the "Class Members"), and Defendant are citizens of Maryland at the time of this Complaint. In addition, neither Plaintiffs nor any member of the Class asserts any federal question.

PARTIES

5. Plaintiff William Waltrop is a citizen of Maryland who resides in Baltimore County, Maryland. Mr. Waltrop's Personal Information (as defined below) was compromised in the Lorien Data Breach ("Data Breach" or "Breach"). After the Breach, Mr. Waltrop received a letter in the mail from Lorien stating that his Personal Information was compromised. As a result of the breach, Mr. Waltrop spent time and effort monitoring his accounts and searching for fraudulent activity related to his identity.

6. Plaintiff June Waltrop is a citizen of Maryland who resides in Baltimore County, Maryland. Mrs. Waltrop's Personal Information (as defined below) was compromised in the Data Breach. Mrs. Waltrop is married to Plaintiff William Waltrop. They have maintained the same bank and credit card accounts since they married in 1974 and have always filed their taxes jointly. As a result of the breach, Mrs. Waltrop spent time and effort monitoring her accounts and searching for fraudulent activity related to her identity.

7. Defendant Maryland Health Enterprises, Inc. d/b/a Lorien Health Services ("Lorien") is a corporation incorporated under the laws of the state of Maryland with its principal place of business located at 1205 York Road, Lutherville, MD 21093. Lorien is a citizen of Maryland. Lorien leaked, disbursed, and/or furnished Plaintiffs' and Class Members' valuable Personal Information (as defined below) to unknown cyber criminals, who in turn made it available for purchase by other unknown cyber criminals, thus causing Plaintiff and Class Members present, immediate, imminent, and continuing increased risk of harm.

FACTUAL ALLEGATIONS COMMON TO ALL COUNTS

8. This is a class action lawsuit brought by Plaintiffs, individually and on behalf of all others similarly situated who are citizens of the state of Maryland, resulting from Defendant Lorien's failure to safeguard and secure the medical information and other personally identifiable information of Plaintiffs and Class Members, including names, addresses, Social Security numbers, dates of birth, and health diagnosis and treatment information (collectively, the "Personal Information"). Personal Information can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

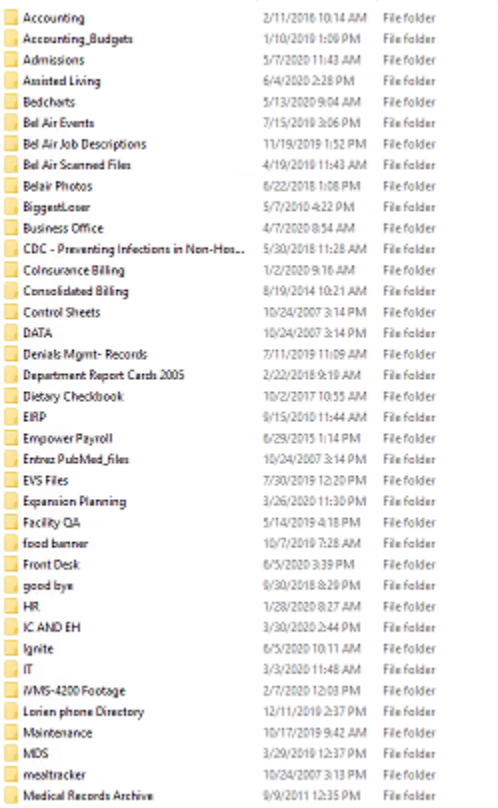
9. On June 6, 2020, cyber hackers operating Netwalker ransomware hacked Lorien's network and effectively held its files hostage by encrypting them and demanding a ransom. One

week later, on June 13, 2020, the criminal hackers published 147MB worth of stolen data to the Dark Web, labeling it as "Part 1," indicating that they have more files to publish in the future.[1] The hackers encrypted Part 1 of the stolen data with a password.[2] However, they published the password, making the data accessible to all other persons on the Dark Web. [3]

10. The Netwalker operators uploaded a screenshot of the files they posted to the Dark Web on Twitter, thereby confirming that they accessed, stole, and published the Personal Information:[4]

INTENTIONALLY LEFT BLANK

[1] Ionut Ilascu, *Lorien Health Services Discloses Ransomeware Attack Affecting Nearly 50,000*, Bleeping Computer (July 20, 2020), https://www.bleepingcomputer.com/news/security/lorien-health-services-discloses-ransomware-attack-affecting-nearly-50-000/; *see also* Adam Banister, *Maryland Elderly Healthcare Provider Hit By Data Breach Impacting 47,000 Individuals* (July 21, 2020), https://portswigger.net/daily-swig/maryland-elderly-healthcare-provider-hit-by-data-breach-impacting-47-000-individuals.
[2] *Id*.
[3] *Id*.
[4] *Id*.



11. The Personal Information that the Netwalker operatives published to the Dark Web includes folders titled, as relevant: Admissions; Bed Charts; Bel Air Photos; Coinsurance Billing; Empower Payroll; HR; Lorien Phone Directory; and Medical Records Archive.

12. On July 9, 2020, Lorien identified 43,970 victims of the Data Breach after it employed a team of cybersecurity experts to investigate the breach. *See* Data Breach Notification, attached as **Ex. 1**.

13. On the Dark Web, a single medical record may sell for $1,000.[5] Misappropriated medical records can be used by criminals to illegally obtain prescriptions, file false medical claims,

[5] Paul Nadrag, *Industry Voices- Forget Credit Card Numbers. Medical Records Are the Hottest Items on the Dark Web, Fierce Healthcare* (January 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web#:~:text=Stolen%20records%20sell%20for%20as,at%20%24250%20(PDF)%20each.

open credit cards, and apply for fraudulent loans.[6] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage."[7] Almost half of medical identity theft victims lose their health care coverage as a result of the incident, while nearly one-third see their insurance premiums rise, and only forty percent are able to resolve their identity theft at all.[8]

14. Plaintiffs' and Class Members' Personal information were compromised, which led to issues including Personal Information being in possession of strangers, published to the Dark Web, and fraudulent transactions on Plaintiffs' credit and debit cards.

15. Plaintiffs and Class Members now face an increased risk of identity theft and fraud, if not actual identity theft and resulting loses, and need to take immediate action to protect themselves from such identity theft. Plaintiffs and Class Members are immediately and imminently in danger of sustaining further direct or indirect injuries as a result of Lorien's failure to protect their Personal Information. The Personal Information obtained by the Netwalker group contains all of the information wrongdoers need to misuse Plaintiffs' and Class Members' identities to their detriment.

16. As a result of the Breach, Plaintiffs and Class members spent and/or will have to spend significant time and money to protect themselves, including but not limited to the time and cost of responding to the Data Breach, acquiring identity theft protection and monitoring, instituting credit freezes, attempting to rehabilitate their Personal Information, conducting a damage assessment, and other costs of mitigation.

---

[6] *Id*.
[7] Elinor Mills, *Study: Medical Identity Theft is Costly for* Victims, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[8] *Id.*

17. With access to an individual's Personal Information, criminals can empty a victim's bank account, obtain a driver's license or official identification card in the victim's name, use the victim's Social Security number to obtain a job or government benefits, request and open loans, file a fraudulent tax return, or commit medical identity theft, *see supra* para. 13. Furthermore, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, and other negative effects.

18. Moreover, cyberattacks against the health care industry have increased over recent years due to the high cost of stolen medical records. Dozens of cyberattacks against health care organizations have occurred in 2018, 2019, and 2020, directed at health care organizations' data systems directly or those of the health care organizations' vendors and business associates.[9] This increase in health care data breaches placed Lorien on notice that a cyberattack against its system was likely. Accordingly, Lorien should have taken adequate precautions to safeguard its system from an attack to ensure that its systems were sufficient to prevent a breach of its patients' and employees' Personal Information.

19. Specifically, Lorien knew or should have known about the risk of a Netwalker ransomware attack. NetWalker ransomware attacks were deemed a "serious threat to the healthcare sector" in May 2020, just one month before Netwalker operators breached Lorien's network.[10] Accordingly, Lorien should have taken adequate precautions to safeguard its network from an

[9] Healthcare IT News Staff, *The Biggest Healthcare Data Breaches of 2018 (So Far)*, Healthcare IT News (October 25, 2018), http://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far; Jessica Davis, *Cyber Threats Behind the Biggest Healthcare Data Breaches of 2019*, Health IT Security (January 3, 2020), https://healthitsecurity.com/news/cyber-threats-behind-the-biggest-healthcare-data-breaches-of-2019; Jessica Davis, *Update: The 10 Biggest Healthcare Data Breaches of 2020, So Far*, Health IT Security (July 8, 2020), https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far.

[10] Jessica Davis, *Netwalker Ransomeware Expands Operations, Targeting Healthcare*, Health IT Security (May 22, 2020), https://healthitsecurity.com/news/netwalker-ransomware-expands-operations-targeting-healthcare ("The healthcare sector has been a prime target for NetWalker through the pandemic."

attack and to ensure its data systems were sufficient to prevent a breach of its patients' and employees' Personal Information.

Lorien Data Protection Policies

20. Lorien currently operates nine assisted rehabilitation and living centers and one dialysis center across Maryland. Lorien advertises its mission as "to exceed the expectations of the people we touch by providing, patient-centered care utilizing the latest in healthcare technology..."[11]

21. At all times relevant to this litigation, Lorien maintained privacy policies committing to protect the confidentiality of information that Lorien collected from its patients in the course of doing business, including personal and health-related information.

22. Specifically, Lorien's Privacy Policy was "created to demonstrate and inform you of [Lorien's] firm commitment to privacy."[12] The policy further states that "any information you provide such as name, email address, or telephone number to Lorien Health Services, is *kept confidential and secure* and only used for the purposes for which you provide" (emphasis added).[13]

23. Lorien has repeatedly acknowledged the importance of safeguarding the personally identifying information and private health information of its patients and employees. In fact, Lorien adopted a nine-page Notice of Privacy Practices policy on June 1, 2020, which outlines thirteen permitted disclosures of personal information ("Privacy Practices") ***See*** **Ex. 2** attached hereto and incorporated herein by reference.

[11] About Lorien, https://www.lorienhealth.com/about-lorien (last visited March 29, 2021).
[12] Privacy Policy, https://www.lorienhealth.com/privacy-policy (last visited March 29, 2021).
[13] *Id*.

24. Upon information and belief, Lorien's privacy policy and Privacy Practices were posted to its website since at least June 1, 2020, and were made available to Lorien patients, employees, and the public.

The Data Breach

25. On June 6, 2020, Lorien discovered that its network was breached and its files had been encrypted. Lorien purportedly hired a "team of cybersecurity experts to assist with its response and to determine whether any personal information may have been accessed during the incident."[14]

26. Lorien's investigation of the breach concluded on June 10, 2020. Lorien determined that the breach may have affected the Personal Information of 43,970 Maryland residents.[15]

27. On June 13, 2020, before Lorien informed Plaintiffs and Class Members of the breach, Netwalker operatives announced on Twitter that it hacked Lorien and published some the data that it accessed to the Dark Web.[16]

28. Despite its purported commitments to "take the privacy and security of [Plaintiffs' and Class Members'] very seriously," Lorien failed to notify Plaintiffs and Class Members that some of the information that had been breached was published on the Dark Web by cyber criminals. Lorien merely stated that it "learned that data on our network had been encrypted."[17] In doing so, Lorien intentionally failed to convey the seriousness of the breach and that Plaintiff and Class Members' information was already in the possession of an unauthorized third-party.

---

[14] Security Breach Notification, https://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2020/itu-330754%20(1).pdf (last visited March 29, 2021).
[15] *Id*.
[16] Ilascu, *supra* note 1.
[17] Security Breach Notification, https://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2020/itu-330754%20(2).pdf (last visited March 29, 2021).

29. When Lorien notified Plaintiffs and Class Members that its network had been breached and its filed encrypted, it "strongly encouraged [Plaintiffs and Class Members] to enroll in the credit monitoring and identity protection services through ID Experts," a service Lorien felt necessary to provide the Data Breach victims with for 12 months at no cost.[18]

30. Lorien published a press release in regard to the Data Breach to its website but has since deleted the page.[19]

31. As a result of Lorien's failure to implement and follow basic security protocols, procedures, and standards Plaintiffs' and Class Members' Personal Information is now in the hands of thieves.

32. 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."[20]

33. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Lorien could and should have implemented, as recommended by the United States Government, the following measures:

A. 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;

B. 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;

[18] *Id*.
[19] https://www.lorienhealth.com/contact/security-incident, (last visited March 29, 2021).
[20] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Mar. 15, 2021).

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

D. Configure firewalls to block access to known malicious IP addresses;

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

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

G. 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;

H. 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;

I. 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;

J. 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;

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

L. Use application whitelisting, which only allows systems to execute

programs known and permitted by security policy;

M. Execute operating system environments or specific programs in a virtualized environment; and

N. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[21]

34. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Lorien could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

A. 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;

B. 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);

C. 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;

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

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

E. 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;

F. 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; and

G. Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[22]

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

A. Secure internet-facing assets

i. Apply latest security updates;

ii. Use threat and vulnerability management;

iii. Perform regular audit; remove privileged credentials;

[22] *See* Security Tip (ST19-001) Protecting Against Ransomware (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Mar. 15, 2021).

B. Thoroughly investigate and remediate alerts

i. Prioritize and treat commodity malware infections as potential full compromise;

C. Include IT Pros in security discussions

i. Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

D. Build credential hygiene

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

E. Apply principle of least-privilege

i. Monitor for adversarial activities;

ii. Hunt for brute force attempts;

iii. Monitor for cleanup of Event Logs;

iv. Analyze logon events;

F. Harden infrastructure

i. Use Windows Defender Firewall;

ii. Enable tamper protection;

iii. Enable cloud-delivered protection; and

iv. Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[23]

36. Given that Lorien was storing the Personal Information of at least 43,970 individuals, Lorien could and should have implemented all of the above measures to prevent and detect ransomware attacks.

[23] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Mar. 15, 2021).

37. The occurrence of the Data Breach indicates that Lorien failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Personal Information of approximately 43,970 individuals, including Plaintiff and Class Members.

38. Lorien also failed to comply statutory and industry standards, including standards mandated by the Federal Trade Commission.

39. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

40. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[25] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[26]

41. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security;

[24] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 8, 2021).
[25] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 8, 2021).
[26] *Id*.

monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[27]

42. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personally identifying information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[28]

43. By allowing an unknown third party to access Lorien's network, Lorien failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Personal Information. Lorien's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

44. After the Data Breach, Mr. Waltrop received a letter in the mail from Lorien stating that his Personal Information was compromised. Mr. Waltrop jointly maintains bank and credit card accounts with his wife and has always filed his taxes jointly with her. As a result of the Breach, the Waltrops spent time and effort monitoring their accounts and searching for fraudulent activity related to their identity. Shortly after the Breach, in or around November 2020, Mrs. Waltrop received two calls from someone identifying as a Chase Bank representative. On one of the calls, the caller accurately identified the balance on the card, the date the card was open, and what the

[27] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 8, 2021).
[28] Federal Trade Commission, Privacy and Security Enforcement Press Releases, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited April 8, 2021).

last payment was for. Thereafter, the Waltrops spent time contacting their bank to shut off that credit card, requested new credit cards, and contacted Equifax to freeze their credit. Additionally, Mrs. Waltrop received a notification from Wells Fargo that someone charged her debit card for Uber rides in California and another notification for a different Chase Bank credit card stating that someone attempted to charge $8,000 or $10,000 in Florida. Most recently, in March 2021, Mrs. Waltrop received a call from an Amazon delivery driver stating that the food she ordered would be delivered within an hour. The caller had her name and stated that the food was ordered with her credit card. The Waltrops do not have an Amazon account.

45. It is evident that the Waltrops will need significant identity theft protection for years to come as a result of Lorien's careless handling of their Personal Information, which, because of its highly sensitive nature, puts the Waltrops at a substantial and imminent risk of future harm.

CLASS ACTION ALLEGATIONS

46. Plaintiffs repeat and re-allege each and every allegation contained in the preceding and following paragraphs of this Complaint as if fully set forth herein.

47. This civil action is properly maintainable as a class action pursuant to Md. R. 2-231 and includes one class of victims:

> All Maryland citizens at the time of the filing of this action whose Personal Information was compromised as a result of the data breach publicly announced by Lorien on or about July 16, 2020.

48. Excluded from the definition of the Class is Lorien, any entity in which Lorien has a controlling interest, any current officers, members, or directors of Lorien, and Lorien's legal representatives, heirs, successors, and assigns. Also excluded are any judicial officers assigned to this case, their court staff, and their immediate families.

Maintainability of a Class Action

49. Plaintiffs are informed and believe, based on Lorien's own admissions that there are approximately 43,970 Class Members. Those individuals' names and addresses are available from Lorien's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. Accordingly, the members of the Class are so numerous that joinder of all members is impracticable.

50. There are common questions of law and fact in this action that are not only common to the Class, but predominate over any questions affecting individual class members. The predominating common questions include, but are not limited to:

A. Whether Lorien knew or should have known that its network was vulnerable to attack;

B. Whether Lorien unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Personal Information;

C. Whether Lorien failed to take adequate and reasonable measures to ensure its network and files were protected before the Data Breach;

D. Whether Lorien failed to take available steps to prevent and stop the Data Breach from happening, especially since it was on actual notice that Netwalker ransomware attacks were targeting healthcare facilities;

E. Whether Lorien owed a duty to Plaintiffs and Class Members to protect their Personal Information;

F. Whether Lorien breached its duty to protect the Personal Information of Plaintiffs and Class members by failing to provide adequate data security;

G. Whether Lorien's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its network, resulting in unauthorized access;

H. Whether Lorien's conduct amounted to violations of the Maryland Personal Information Protect Act, and/or the Maryland Consumer Protection Act;

I. Whether Lorien's conduct renders it liable for negligence and/or negligent misrepresentation;

J. Whether, as a result of Lorien's conduct, Plaintiffs and Class members face a significant threat of harm and/or have already suffered harm, and if so, the appropriate measure of damages to which they are entitled; and

K. Whether as result of Lorien's conduct, Plaintiff and Class Members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature and extent of such relief.

51. Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same alleged unlawful conduct and damaged in the same way.

52. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs' interests do not conflict with the interests of Class Members whom they seek to represent. The interests of the Plaintiffs and of all other members of the Class are identical, and the Plaintiffs are cognizant of their duties and responsibilities to the Class. Plaintiffs intend to prosecute this action vigorously. Plaintiffs' counsel are experienced in data breach and privacy class actions and other complex litigation, and have previously litigated numerous class actions with success both within this Court's jurisdiction and elsewhere. Therefore, Plaintiffs' counsel will adequately represent the interests of the Class.

53. This action is properly maintained as a class action under Md. R. 2-231(b)(1)(A) in that separate actions by individual members of the Class could create a risk of inconsistent or varying adjudications with respect to individual members of the Class that could establish incompatible standards of conduct for members of the Class as well as the Defendant.

54. This action is properly maintainable as a class action pursuant to Md. R. 2-231(b)(1)(B) in that separate actions by individual members of the Class would create a risk of adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of other members not party to the adjudications, or would substantially impair or impede their ability to protect themselves.

55. This action is also properly maintainable under Md. R. 2-231(b)(3), in that questions of law or fact common to members of the Class predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy between the Class and Defendant.

56. This action is also properly maintainable under Md. R. 2-231(d), in that particular issues common to the Class, as described in part in paragraph 50, are most appropriately and efficiently resolved via class action.

The Desirability of a Class Action

57. The commonality of issues of law and fact in this case are clear. Many Class Members may be unaware of their right to prosecute a claim against Lorien. This class action can be managed without undue difficulty because Plaintiffs will vigorously pursue the interests of the Class by virtue of the fact that the Plaintiffs have suffered the same injuries arising out of the same events as other Class Members.

58. To the extent that some Class Members have an interest in individually controlling the prosecution of a separate action, they may exclude themselves from the Class upon their receipt of notice under Md. R. 2-231(e).

59. The difficulties likely to be encountered in the management of a class action in this litigation are insignificant, especially when weighed against the virtual impossibility of affording adequate relief to the members of the Class through dozens of separate actions.

COUNT I
MARYLAND PERSONAL INFORMATION PROTECTION ACT
Md. Code Ann., Com. Law, §§ 14-3501, *et seq.*

60. Plaintiffs repeat and reallege the allegations contained in paragraphs 1 through 59 of this Complaint as if fully set forth herein.

61. Under the Maryland Personal Information Protection Act ("MPIPA"), Md. Code Ann., Com. Law, § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations."

62. Lorien is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Code Ann., Com. Law, § 14-3501(b)(1).

63. Plaintiffs and Class Members are "individuals" and "customers" as defined in Md. Code Ann., Com. Law, §§ 14-3502(a) and 14-3503.

64. Plaintiffs and Class Members' Personal Information includes "[h]ealth information" and "[p]ersonal information" as covered under Md. Code Ann., Com. Law, §§ 14-3501(d)-(e).

65. Lorien did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Code Ann., Com. Law, § 14-3503.

66. The Data Breach was a "breach of the security of a system" as defined by Md. Code Ann., Com. Law, § 14-3504(1).

67. Under Md. Code Ann., Com. Law, § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

68. Under Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the owner or licensee of the computerized data shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical but not later than 45 days after the business discovers or is notified of the breach of a security system."

69. Under Md. Code Ann., Com. Law §14-3504(c)(3) the notification the "business that is required to notify an owner or licensee of personal information of a breach of security of a system under paragraph (1) of this subsection shall share with the owner or licensee information relative to the breach."

70. Because Lorien discovered the security breach and had notice of the security breach, Lorien had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2).

71. Lorien failed to notify Plaintiffs and Class Members that a Netwalker operative group breached its network, was in possession of their Personal Information, and published a portion of their Personal Information to the Dark Web. By failing to disclose all of the information that was available to Lorien when it notified Plaintiffs and Class Members of the Data Breach, Lorien violated Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2).

72. As a direct and proximate result of Lorien's violations of Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiffs and Class Members have suffered and will continue to suffer damages.

73. Pursuant to Md. Code Ann., Com. Law, § 14-3508, Lorien's violations of Md. Code Ann., Com. Law, §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act (codified at Md. Code Ann., Com. Law, § 13-301 *et seq*.) ("CPA") and are subject to the enforcement and penalty provisions contained within the CPA.

74. Plaintiffs and Class Members seek relief under Md. Code Ann., Com. Law, § 14-3508, including actual damages and attorneys' fees.

WHEREFORE, Plaintiffs, on behalf of themselves and others similarly situated, respectfully request that the Court enter judgment in their favor and against Lorien, and that they be awarded damages together with equitable relief as follows:

A. That the Court enter a judgment against Defendant finding that it is liable to Plaintiffs and Class Members;

B. That the Court award compensatory damages, including at least nominal damages, in an amount that exceeds $75,000, plus interest and costs, to Class Members in an amount to be determined at trial;

C. That the Court reimburse Plaintiffs all costs paid by Plaintiffs or on behalf of Plaintiffs;

D. That the Court award the costs and expenses of this case, including attorneys' fees;

E. That the Court award pre-judgment and post-judgment interest;

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

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

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

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

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and

integrity of the personal identifying information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

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

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

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

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

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

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

upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, 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 respective 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 personal identifying information 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

xvii. 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; and

G. That the Court award all other further and general relief as the Court deems just and necessary.

COUNT II
MARYLAND CONSUMER PROTECTION ACT
Md. Code Ann., Com. Law, §§13-301, *et seq.*

75. Plaintiffs repeat and reallege each and every allegation contained in paragraphs 1 through 59 of this Complaint as if fully set forth herein.

76. Lorien is a person as defined in Md. Code Ann., Com. Law, § 13-101(h).

77. Lorien's conduct as alleged herein is related to "sales," "offers for sale," or "bailment" as defined in Md. Code Ann., Com. Law, §§ 13-101(i) and 13-303.

78. Plaintiffs and Class Members are "consumers" as defined in Md. Code Ann., Com. Law, § 13-101(c).

79. Lorien advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Code Ann., Com. Law, § 13-101(d).

80. Lorien advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

81. Neither Plaintiffs nor any member of the Class asserts a claim regarding professional services, including the quality of care rendered by a health care provider. Lorien

engaged in unfair and deceptive trade practices with respect to its commercial and/or entrepreneurial services.

82. Lorien engaged in unfair and deceptive trade practices in violation of Md. Code Ann., Com. Law, § 13-301, including:

A. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

B. Representing that consumer goods or services have a characteristic that they do not have;

C. Representing that consumer goods or services are of a particular standard quality or grade that they are not;

D. Failing to state a material fact where the failure deceives or tends to deceive;

E. Advertising or offering consumer goods or services without intent to sell, lease, or rent than as advertised or offered; and

F. Engaging in deception, fraud, false pretense, false premise, representation, or knowing concealment, suppression, or commission of any material fact with the intent that a consumer relies on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale, lease or rental.

83. Lorien engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services in violation of Md. Code Ann., Com. Law, § 13-303, including:

A. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach;

B. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the MPIPA, Md. Code Ann., Com. Law, § 14-3503, which was a direct and proximate cause of the Data Breach;

C. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Personal Information, including by implementing and maintaining reasonable security measures;

D. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the MPIPA, Md. Code Ann., Com. Law, § 14-3503;

E. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Personal Information; and

F. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the MPIPA, Md. Code Ann., Com. Law, § 14-3503.

84. Lorien's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Lorien's security and ability to protect the

confidentiality of consumers' Personal Information. Lorien's misrepresentations and omissions would have been important to consumers when choosing a health care provider.

85. Lorien intended to mislead Plaintiffs and Class Members as to the true nature and/or condition of Lorien's security, commercial, and entrepreneurial practices, and intentionally induced them to rely on its misrepresentations and omissions.

86. Had Lorien disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Lorien would have been forced to adopt reasonable data security measures and comply with applicable laws. Instead, Lorien was trusted with sensitive and valuable Personal Information regarding thousands of patients and employees, including Plaintiffs and Class Members. Lorien accepted the responsibility of safeguarding data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class Members reasonably relied on Lorien's misrepresentations and omissions, the truth of which they could not have discovered.

87. As a direct and proximate result of Lorien's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts and medical information for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

88. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

89. Unless Defendant is restrained from engaging in the aforementioned unfair and deceptive trade practices, Plaintiffs and Class Members will continue to suffer substantial and irreparable injury.

90. The benefits to Plaintiffs and Class Members in obtaining injunctive relief are equal to or outweigh the potential harm which Defendant would incur if this Court grants the requested injunctive relief.

91. The public interest is best served by granting the injunction.

WHEREFORE, Plaintiffs, on behalf of themselves and others similarly situated, respectfully request that the Court enter judgment in their favor and against Lorien, and that they be awarded damages together with equitable relief as follows:

A. That the Court enter a judgment against Defendant finding that it is liable to Plaintiffs and Class Members;

B. That the Court award compensatory damages, in an amount that exceeds $75,000, plus interest and costs, to Class Members in an amount to be determined at trial;

C. That the Court reimburse Plaintiffs all costs paid by Plaintiffs or on behalf of Plaintiffs;

D. That the Court award the costs and expenses of this case, including attorneys' fees;

E. That the Court award pre-judgment and post-judgment interest;

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

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

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

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

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

v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

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

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

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

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

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

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

xii. requiring Defendant to routinely and continually conduct internal training and education, 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 respective 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 personal identifying information 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

xvii. 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; and

G. That the Court award all other further and general relief as the Court deems just and necessary.

COUNT III
NEGLIGENCE

92. Plaintiffs repeat and reallege each and every allegation contained paragraphs 1 through 59 of this Complaint as if fully set forth herein.

93. Lorien required Plaintiffs and Class Members to submit Personal Information in order to, among other things, receive health care services and/or gainful employment.

94. Lorien knew or should have known of the risks inherent in collecting, maintaining, and storing the Personal Information of Plaintiffs and Class Members and the heightened risk of doing so without adequate security systems and protocols.

95. Lorien owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Lorien's security systems to ensure that Plaintiffs and Class Members' Personal Information in Lorien's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts regarding intrusions to its networks; (d) timely providing accurate notice to Plaintiffs and Class Members of any data breaches and the steps that can be taken by Plaintiffs and Class Members to protect themselves from identity theft and medical fraud; and (e) maintaining data security measures consistent with statutory and industry standards.

96. Lorien had a duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were foreseeable and probable victims of inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Lorien also knew that it was more likely than

not Plaintiffs and other Class Members would be harmed, and in fact, suffered harm as identified above.

97. Lorien also had a duty to safeguard the Personal Information of Plaintiffs and Class Members and to accurately notify them of a breach. That duty is also imposed by applicable Maryland laws and statutes that require Lorien to reasonably safeguard sensitive Personal Information, as detailed herein.

98. An accurate notification was required, appropriate, and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to prevent, mitigate, or ameliorate the damages caused by Lorien's misconduct.

99. Lorien violated the MPIPA and CPA by failing to use reasonable measures to protect Personal Information and not complying with industry standards. Lorien's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stores and the foreseeable consequences of a data breach at a major health system.

100. Plaintiff and Class members are among the class of persons the MPIPA and CPA were designed to protect, and the injuries suffered by Plaintiffs and Class members are the type of injury the MPIPA and CPA were intended to prevent.

101. Lorien violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect Plaintiffs' and Class Members' Personal Information.

102. Plaintiffs and Class Members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiffs and Class members are the type of injury Section 5 of the FTC Act was intended to prevent.

103. Lorien breached the duties it owed to Plaintiffs and Class Members described above by, among things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiffs and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) timely discover and disclose that Plaintiffs and Class Members' Personal Information in Lorien's possession had been or was reasonably believed to have been, stolen or compromised.

104. But for Lorien's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, and without any wrongdoing on the part of Plaintiffs or Class Members, Plaintiffs' and Class Members' Personal Information would not have been compromised.

105. As a direct and proximate result of Lorien's negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory and nominal damages, in an amount to be proved at trial. Plaintiffs' and Class Members' injuries include but are not limited to:

A. Theft of their Personal Information;

B. Publication of their Personal Information to the Dark Web;

C. Costs associated with medical identity theft;

D. Loss or delay of tax refunds as a result of fraudulently filed tax returns;

E. Costs associated with the detection and prevention of identity theft and unauthorized use of their accounts;

F. Costs associated with purchasing identity theft protection services and other monitoring services;

G. Unauthorized charges and loss of use and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

H. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and imposing withdrawal and purchase limits on compromised accounts;

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

J. Damages to and diminution in value of their Personal Information; and

K. Continued risk of exposure to hackers and thieves of their Personal Information, which remains in Lorien's possession and is subject to further breaches so long as Lorien fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members.

106. Unless Defendant is restrained from engaging in the aforementioned negligent security practices, Plaintiffs and Class Members will suffer substantial and irreparable injury.

107. The benefits to Plaintiffs and Class Members in obtaining injunctive relief are equal to or outweigh the potential harm which Defendant would incur if this Court grants the requested injunctive relief.

108. The public interest is best served by granting the injunction.

WHEREFORE, Plaintiffs, on behalf of themselves and others similarly situated, respectfully request that the Court enter judgment in their favor and against Lorien, and that they be awarded damages together with equitable relief as follows:

A. That the Court enter a judgment against Defendant finding that it is liable to Plaintiffs and Class Members;

B. That the Court award compensatory damages, including at least nominal damages, in an amount that exceeds $75,000, plus interest and costs, to Class Members in an amount to be determined at trial;

C. That the Court reimburse Plaintiffs all costs paid by Plaintiffs or on behalf of Plaintiffs;

D. That the Court award the costs and expenses of this case, including attorneys' fees;

E. That the Court award pre-judgment and post-judgment interest;

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

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

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

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

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

v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

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

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

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

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's

network is compromised, hackers cannot gain access to other portions of Defendant's systems;

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

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

xii. requiring Defendant to routinely and continually conduct internal training and education, 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 respective 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 personal identifying information 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

xvii. 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; and

G. That the Court award all other further and general relief as the Court deems just and necessary.

COUNT IV
NEGLIGENT MISREPRESENTATION

109. Plaintiffs repeat and reallege each and every allegation contained in paragraphs 1 through 59 of this Complaint as if fully set forth herein.

110. Lorien negligently represented to Plaintiffs and Class Members that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which were false at the time they were made.

111. Lorien also negligently misrepresented to Plaintiffs and Class Members that it did and would comply with the requirements of relevant laws pertaining to the privacy and security of Plaintiffs' and Class Members' Personal Information.

112. Plaintiffs and Class Members justifiably relied on Lorien's statements that Lorien would maintain adequate data and privacy security practices and procedures to safeguard Plaintiffs' and Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft and that it did and would comply with the requirements of applicable laws pertaining to the privacy and security of Plaintiffs' and Class Members' Personal Information.

113. Had Plaintiffs and Class Members, as reasonable persons, known of Lorien's inadequate data privacy and security practices, or that Lorien was failing to comply with the requirements of applicable laws pertaining to the privacy and security of Plaintiffs' and Class Members' Personal Information, they would not have purchased or received health-related services from Lorien and would not have entrusted Lorien with their Personal Information.

114. As a direct and proximate result of Lorien's conduct, Plaintiffs and Class Members have suffered damages as discussed herein.

115. Unless Defendant is restrained from engaging in the aforementioned negligent misrepresentation, Plaintiffs and Class Members will suffer substantial and irreparable injury.

116. The benefits to Plaintiffs and Class Members in obtaining injunctive relief are equal to or outweigh the potential harm which Defendant would incur if this Court grants the requested injunctive relief.

117. The public interest is best served by granting the injunction.

WHEREFORE, Plaintiffs, on behalf of themselves and others similarly situated, respectfully request that the Court enter judgment in their favor and against Lorien, and that they be awarded damages together with equitable relief as follows:

A. That the Court enter a judgment against Defendant finding that it is liable to Plaintiffs and Class Members;

B. That the Court award compensatory damages in an amount that exceeds $75,000, plus interest and costs, to Class Members in an amount to be determined at trial;

C. That the Court reimburse Plaintiffs all costs paid by Plaintiffs or on behalf of Plaintiffs;

D. That the Court award the costs and expenses of this case, including attorneys' fees;

E. That the Court award pre-judgment and post-judgment interest;

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

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

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

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

can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

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

v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

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

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

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

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

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

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

xii. requiring Defendant to routinely and continually conduct internal training and education, 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 respective 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 personal identifying information 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

xvii. 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; and

G. That the Court award all other further and general relief as the court deems just and necessary.

COUNT V
INVASION OF PRIVACY

118. Plaintiffs repeat and reallege each and every allegation contained in paragraphs 1 through 59 of this Complaint as if fully set forth herein.

119. Plaintiff and Class Members had a legitimate expectation of privacy to their Personal Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

120. Lorien owed a duty to Plaintiff and Class Members to keep their Personal Information confidential.

121. Lorien failed to protect and released to unknown and unauthorized third parties the Personal Information of Plaintiffs and Class Members.

122. Lorien allowed unauthorized and unknown third parties to access, examine, and publish to the Dark Web Plaintiffs' and Class Members' Personal Information as a result of its failure to protect the Personal Information.

123. Plaintiffs' and Class Members' Personal Information was not of valid concern to the public.

124. The publication of Plaintiffs' and Class Members' Personal Information was highly offensive to any reasonable person and constitutes unreasonable publicity given to Plaintiffs' and Class Members' private life.

125. The unauthorized release to, custody of, and examination, of Plaintiff and Class Members' Personal Information by unauthorized third parties is highly offensive to the reasonable person.

126. Lorien's conduct constituted an intentional instruction into the privacy of Plaintiffs and Class Members.

127. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Personal Information to Lorien as part of their assisted living and/or rehabilitation treatment with Lorien, but privately with an intention that the Personal Information would be kept confidential and would be protected from

128. The Data Breach at the hands of Lorien constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

129. Lorien acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

130. Because Lorien acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

131. As a proximate result of the above acts and omissions of Lorien, the Personal Information of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

WHEREFORE, Plaintiffs, on behalf of themselves and others similarly situated, respectfully request that the Court enter judgment in their favor and against Lorien, and that they be awarded damages together with equitable relief as follows:

A. That the Court enter a judgment against Defendant finding that it is liable to Plaintiffs and Class Members;

B. That the Court award compensatory damages, including at least nominal damages, in an amount that exceeds $75,000, plus interest and costs, to Class Members in an amount to be determined at trial;

C. That the Court reimburse Plaintiffs all costs paid by Plaintiffs or on behalf of Plaintiffs;

D. That the Court award the costs and expenses of this case, including attorneys' fees;

E. That the Court award pre-judgment and post-judgment interest;

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

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

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

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

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

v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to

promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

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

xii. requiring Defendant to routinely and continually conduct internal training and education, 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 respective 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 personal identifying information 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

xvii. 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; and

G. That the Court award all other further and general relief as the court deems just and necessary.

COUNT VI
BREACH OF CONFIDENCE

132. Plaintiffs repeat and reallege each and every allegation contained in paragraphs 1 through 59 of this Complaint as if fully set forth herein.

133. At all times during Plaintiffs and Class Members interactions with Lorien, Lorien was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' Personal Information that Plaintiffs and Class Members provided to Lorien.

134. Lorien gained the confidence of Plaintiffs and Class Members and purported to act or advise with their interest in mind when it collected, stored, and maintained Plaintiffs' and Class Members' Personal Information.

135. Lorien established a confidential relationship with Plaintiffs and Class Members.

136. As alleged herein and above, Lorien's relationship with Plaintiffs and Class Members was governed by the terms and expectations that Plaintiffs' and Class Members' Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

137. Plaintiff and Class Members provided their Personal Information to Lorien with the explicit and implicit understandings that Lorien would protect and not permit the Personal Information to be disseminated to any unauthorized third parties.

138. Plaintiff and Class Members also provided their Personal Information to Lorien with the explicit and implicit understandings that Lorien would take precautions to protect their Personal Information from unauthorized disclosure. Lorien voluntarily received in confidence Plaintiff's

and Class Members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

139. Due to Lorien's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' Personal Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

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

141. But for Lorien's disclosure of Plaintiffs' and Class Members' Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been compromised, stolen, viewed, accessed, published to the Dark Web and used by unauthorized third parties. Lorien's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Personal Information as well as the resulting damages.

142. The injury and harm Plaintiffs and Class members have suffered was the reasonably foreseeable result of Lorien's unauthorized disclosure of Plaintiffs' and Class Members' Personal Information. Lorien knew or should have known its methods of accepting and securing Plaintiffs' and Class Members' Personal Information was inadequate as it relates to, at the very least, securing its network and other equipment containing Plaintiffs' and Class Members' Personal Information.

143. As a direct and proximate result of Lorien's breach of its confidence with Plaintiffs Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the theft and publication of their Personal Information to the Dark Web; (ii) costs associated with medical identity theft; (iii) loss or delay of tax refunds as a result of fraudulently filed tax returns; (iv) costs associated with the detection and prevention of identity theft and

unauthorized use of their accounts; (v) costs associated with purchasing identity theft protection services and other monitoring services; (vi) unauthorized charges and loss of use and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit; (vii) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and imposing withdrawal and purchase limits on compromised accounts; (viii) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals; (ix) damages to and diminution in value of their Personal Information; and (x) continued risk of exposure to hackers and thieves of their Personal Information, which remains in Lorien's possession and is subject to further breaches so long as Lorien fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members.

144. As a direct and proximate result of Lorien's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

WHEREFORE, Plaintiffs, on behalf of themselves and others similarly situated, respectfully request that the Court enter judgment in their favor and against Lorien, and that they be awarded damages as follows:

A. That the Court enter a judgment against Defendant finding that it is liable to Plaintiffs and Class Members;

B. That the Court award compensatory damages in an amount that exceeds $75,000, plus interest and costs, to Class Members in an amount to be determined at trial;

C. That the Court reimburse Plaintiffs all costs paid by Plaintiffs or on behalf of Plaintiffs;

D. That the Court award the costs and expenses of this case, including attorneys' fees;

E. That the Court award pre-judgment and post-judgment interest; and

F. That the Court award all other further and general relief as the court deems just and necessary.

Respectfully submitted,

MURPHY, FALCON & MURPHY

Nikoletta S. Mendrinos (CPF # 1212120253)
Kaitlyn T. Holzer (CPF # 2012170242)
One South Street, 30th Floor
Baltimore, Maryland 21202
T: (410) 951-8744
F: (410) 539-6599
nikoletta.mendrinos@murphyfalcon.com
kaitlyn.holzer@murphyfalcon.com

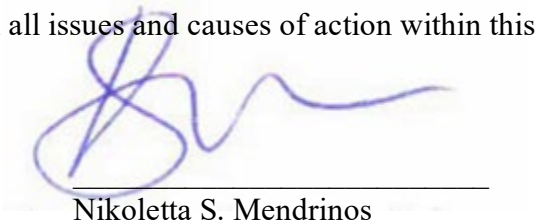
John Yanchunis, *Pro hac vice forthcoming*
Ryan Maxey, *Pro hac vice forthcoming*
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
T: (813) 275-5272

F: (813) 222-4736
JYanchunis@ForThe People.com
Rmaxey@ForThePeople.com

Counsel for Plaintiffs

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues and causes of action within this Complaint.



Nikoletta S. Mendrinos

LEWIS BRISBOIS
LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue Ste. 900
Portland, OR 97204
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

C-03-CV-21-001062

July 16, 2020

VIA E-MAIL
Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: Idtheft@oag.state.md.us

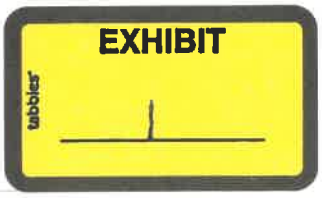
Re: Notice of Data Security Incident

Dear Attorney General Frosh:

We represent Lorien Health Services, ("Lorien") a Maryland-based company that provides assisted living and skilled nursing interventions for seniors across ten facilities, in connection with a data security incident which is described in greater detail below. This letter is being sent pursuant to Md. Code Ann. Comm. Law §§ 14-3501 – 3508 because the personal information of Maryland residents may have been affected by a recent data security incident. The incident may have involved unauthorized access to names, addresses, Social Security numbers, dates of birth, and health diagnosis and treatment information of residents and employees of Lorien.

On June 6, 2020, Lorien learned that data on its network had been encrypted. Upon discovering this incident, Lorien immediately engaged a team of cybersecurity experts to assist with its response and to determine whether any personal information may have been accessed during the incident. On June 10, 2020 the investigation determined that personal information may have been accessed during the incident. Lorien then worked to identify potentially affected persons. On July 9, 2020, Lorien identified forty three thousand, nine hundred and seventy (43,970) Maryland residents as among the potentially affected population. Lorien has reported this incident to law enforcement.

In addition to restoring its system, Lorien has implemented enhanced security measures to minimize the likelihood that an event like this might occur again in the future. Lorien notified the potentially affected Maryland residents via the attached sample letter on July 16, 2020. Out of an abundance of caution, Lorien is offering twelve (12) months of complimentary credit and identity monitoring services to the potentially affected residents through ID Experts.



Please contact me should you have any questions.

Sincerely,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter

C-03-CV-21-001062

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.
PLEASE REVIEW IT CAREFULLY.

This Notice of Privacy Practices was published on 6/1/2020, and replaces all previously published Notices.

We are required by law to maintain the privacy of your personal health information and to provide you with notice of our legal duties and privacy practices related to your personal health information. This Notice of Privacy Practices describes how we may use and disclose your personal health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your personal health information. "Personal health information" is information, including demographic information (such as your age or your address), that may identify you and that relates to your physical or mental health or conditions and related health care services (whether past, present or future) or payment for such services. We will not use or disclose your health information without your authorization, except as described in this Notice.

Understanding Your Health Record/Information

Each time you visit a hospital, physician, or other healthcare provider, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment.

This information, often referred to as your health or medical record, serves as a:

- basis for planning your care and treatment
- means of communication among the many health professionals who contribute to your care
- legal document describing the care you received
- means by which you or a third-party payer can verify that services billed were actually provided
- a tool in educating health professionals
- a source of data for medical research
- a source of information for public health officials charged with improving the health of the nation

- a source of data for facility planning and marketing
- a tool with which we can assess and continually work to improve the care we render and the outcomes we achieve

Understanding what is in your record and how your health information is used helps you to:

- ensure its accuracy
- better understand who, what, when, where, and why others may assess your health information
- make more informed decisions when authorizing disclosure to others

Uses and Disclosures of Personal Health Information

Your personal health information may be used and disclosed by and between individuals that are involved in your care and treatment for the purpose of providing health care services to you. Your personal health information may also be used and disclosed to pay your health care bills and to support our operations. Other uses and disclosures may be made if you are given an opportunity to object to the use or disclosure or with your express authorization.

Examples of the types of permitted uses and disclosures of your protected health care information are explained below. These examples are not meant to be exhaustive, but describe the types of uses and disclosures that may be made in the normal course of business.

A. Uses and Disclosures for Treatment, Payment and Practice Operations:

(1) Care and Treatment: We may use and disclose your personal health information for our own treatment purposes or the treatment purposes of another health care provider. Treatment activities include the provision, coordination, or management of your health care and any related services. *For example, we may disclose your personal health information to a doctor treating you for an injury or other illness.*

(2) Payment: Your personal health information may be used or disclosed to obtain payment for health care services we provide to you or for the payment purposes of another health care provider. *For example, we may disclose your personal health information to your health plan to obtain authorization to initiate treatment.*

(3) Healthcare Operations: We may use or disclose your personal health information to support our business activities. These activities include, but are not limited to, quality assessment, employee review, training, conducting or arranging for legal or consulting services, and business planning. We may also disclose your personal health information to another entity that is subject to federal privacy protections to conduct certain business activities including

quality assessments and performance improvement activities, reviews of health care professional qualifications, evaluating provider performance or health care fraud and abuse detection or compliance.

We may disclose your personal health information to third party "business associates" that perform various activities for our organization such as billing, answering or transcription services. Whenever an arrangement between our Facility and a business associate involves the use or disclosure of personal health information, we will have a written contract that contains terms intended to protect the privacy of your personal health information.

Our Business Associates are held to a similar standard as we are, and must employ similar measures to protect your privacy. We may also use or disclose your personal health information to remind you of your appointments. We may also use or disclose your personal health information to provide you with information about treatment alternatives or other health-related benefits or services that we offer that may be of interest to you. *For example, we may use your treatment information to analyze clinical outcomes and measure quality.*

B. Uses and Disclosures of Personal Health Information With Your Written Authorization

Uses and disclosures of your personal health information other than for treatment, payment or healthcare operations purposes will be made only with your written authorization, unless we are otherwise permitted or required by law to use or disclose your personal health information as described below. For example we will not use or disclose your personal health information for marketing purposes or sale without obtaining your authorization. If we have records for you that include psychotherapy notes, we will not disclose those notes without your authorization. You may revoke an authorization, at any time, in writing, except to the extent that we have already taken an action based on the authorization or otherwise relied upon it.

C. Permitted and Required Uses and Disclosures with an Opportunity to Object

We may use and disclose your personal health information in the instances described below. You will be given the opportunity, when possible, to agree or object to the use or disclosure of all or part of your personal health information. If you are not present or able to agree or object to the use or disclosure of the personal health information, then we may, using professional judgment, determine whether the disclosure is in your best interest. In this case, only the personal health information that is relevant to your health care will be disclosed.

(1) Others Involved in Your Healthcare: Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your personal health information that directly relates to that person's involvement in your health care. If you are unable to agree or object, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment or the professional judgment of your healthcare provider.

(2) Notification Purposes: We may use or disclose personal health information to notify or assist in notifying a family member, personal representative or any person responsible for your care of your location, general condition, changes in your condition or death.

(3) Disaster Relief: We may use or disclose your personal health information to an authorized public or private entity to assist in disaster relief efforts and to coordinate with disaster relief agencies.

(4) Facility Directory: We may use and disclose your name, location, general condition, and religious affiliation for a patient directory for access by clergy and persons who specifically inquire about you by name, unless you object or otherwise restrict this use and disclosure. If you are incapacitated or an emergency treatment circumstance exists limiting your ability to object, some or all of the above information may be used in the patient directory if such use is not inconsistent with any of your prior expressed preferences, or it is believed by us to be in your best interests.

D. Other Permitted and Required Uses and Disclosures That May Be Made without Your Authorization or an Opportunity to Object

We may use or disclose your personal health information in the following situations without your authorization or without giving you an opportunity to object to the use or disclosure. These situations include but are not limited to:

(1) As Required By Law: We may use or disclose your personal health information to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law.

(2) Public Health: We may disclose your personal health information for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. The disclosure may be made for the purpose of controlling disease, injury or disability. For example, we may disclose your personal health information to public health authorities that are authorized to notify a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading disease. We may also disclose your personal health information, if directed by the public health authority, to a government agency that is collaborating with the public health authority.

(3) Health Oversight: We may disclose personal health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

(4) Abuse or Neglect: We may disclose your personal health information to a public health authority that is authorized by law to receive reports of child or vulnerable person abuse or

neglect. In addition, we may disclose your personal health information if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws and you will be informed of the report except in certain limited circumstances.

(5) Food and Drug Administration: We may disclose your personal health information to a person or company required by the United States Food and Drug Administration to report adverse events, product defects or problems, biologic product deviations, track products; enable product recalls; make repairs or replacements, or conduct post marketing surveillance.

(6) Legal Proceedings: We may disclose personal health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal and in certain conditions in response to a subpoena, discovery request or other lawful process.

(7) Law Enforcement: We may also disclose personal health information, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises, and (6) in a medical emergency (not on our premises) when it is likely that a crime has occurred.

(8) Coroners, Funeral Directors, and Organ Donation: We may disclose personal health information to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose personal health information to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may disclose such information in reasonable anticipation of death.
Personal health information may also be used and disclosed for organ, eye or tissue donation purposes.

(9) Research: We may disclose your personal health information to researchers when their research has been approved by an institutional review board or appropriate privacy board that has reviewed the research proposal and established protocols to ensure the privacy of your personal health information.

(10) Criminal Activity: Consistent with applicable federal and state laws, we may disclose your personal health information if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose personal health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

(11) Military Activity and National Security: When the appropriate conditions apply, we may use or disclose personal health information of individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military services. We may also disclose your personal health information to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

(12) Workers' Compensation: Your personal health information may be disclosed by us as authorized to comply with workers' compensation laws and other similar legally-established programs.

(13) Inmates: We may use or disclose your personal health information if you are an inmate of a correctional facility, your physician created or received your personal health information in the course of providing care to you and the disclosure of the information is necessary for your care, the health and safety of other inmates or correctional personnel or the administration of the correctional facility.

E. Required Uses and Disclosures

We are required by law to make disclosures to you upon request. We are also required to make disclosures of your personal health information when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements of the federal privacy requirements.

F. Use of Personal Health Information for Fundraising

We may contact you about fundraising activities for our organization; however, you have the right to opt out of receiving such fundraising communications from us at any time.

Your Health Information Rights

As a patient, you have certain rights related to your personal health information. The following information explains how you may exercise these rights. For additional information on these rights, please speak with the Privacy Officer.

A. You have the right to inspect and receive a copy of your personal health information.

This means you may look at and obtain electronic or paper copies of personal health information about you that is contained in a designated record set for as long as we maintain that information. A "designated record set" contains medical and billing records and any other records that is used for making decisions about you. You must submit a written request to the Privacy Officer to inspect or copy your personal health information. Such request may be orally

or in writing;
however, in order to better respond we ask that the request be made in writing on a form provided by the Facility. If your medical information is maintained in an electronic health record, you may request that an electronic copy of your record be sent to you or to another individual or entity. We have the right to charge you a reasonable fee for a copy of your medical record. This fee may be limited by state law.

However, you may not inspect or copy the following records: (1) psychotherapy notes that are maintained separately from your medical record; (2) information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and (3) personal health information that is subject to law that prohibits access to personal health information. In some circumstances, you may have a right to have this decision reviewed. Please contact the Privacy Officer if you have questions about access to your medical record.

B. You can request certain restrictions of your personal health information. This means you may ask us not to use or disclose certain parts of your personal health information. You may also request that any part of your personal health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Any such request must be in writing on a form provided by us, state the specific restriction, and to whom the restriction applies.

We must agree to a request to restrict disclosure if the disclosure is to a health plan for payment or other healthcare operations purposes, the disclosure is not otherwise required by law, and the information pertains solely to a health care item/service you have fully paid for out of pocket. Otherwise, we are not required to agree to a requested restriction. If we believe it is in your best interest to permit use and disclosure of your personal health information, or in the event of an emergency, your personal health information will not be restricted.

C. You have the right to request to receive confidential communications from us by alternative means or at an alternative location. We will accommodate reasonable, written requests to receive confidential communications of your personal health information. We may condition this accommodation by asking you for information as to how payment will be handled or to specify an alternative address or other method of contact.

D. You may have the right to amend your personal health information. This means you may request an amendment of personal health information about you in a designated record set for as long as we maintain this information. In certain cases, we may deny your request for an amendment. If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a response to your statement and will provide you with a copy of our response. Please contact the Privacy Officer to determine if you have questions about amending your medical record. Such requests must be made in writing on a form provided by the Facility.

E. You have the right to receive an accounting of certain disclosures we have made, if any, of your personal health information. This right applies to disclosures for purposes other than treatment, payment or healthcare operations as described in this Notice of Privacy Practices. It excludes disclosures made prior to April 14, 2003 and disclosures we make after April 14, 2003 that are (1) pursuant to an authorization; (2) to you, (3) to family members or friends involved in your care, (4) incidental to other permitted disclosures, (5) for national security purposes, (6) for inmates to correctional institutions, (7) part of a limited data set that does not include any direct identifiers and that is subject to an agreement that protects the confidentiality of the personal health information, or (8) for notification purposes. You have the right to receive specific information regarding these disclosures that occur after April 14, 2003 for a period of up to six (6) years or other requested shorter timeframe. The right to receive this information is subject to certain exceptions, restrictions and limitations. Such requests must be made in writing on a form provided by the Facility.

F. You have the right to obtain a paper copy of this notice from us. Even if you have agreed to accept this notice electronically, we will furnish a copy of this Notice of Privacy Practices upon request.

G. You have the right to receive notification of certain breaches of your health information. We will notify you of certain breaches of your personal health information, if they occur, as required by the HIPAA Privacy Rule requirements.

Changes to this Notice

We reserve the right to change our privacy practices and to make the new provisions effective for all health information we maintain. Should our privacy practices change, we will post the changes in a physical place within our building (if applicable) and on our website ("Website") www.Lorienhealth.com. A copy of the revised Notice will be available after the effective date of the changes upon request. You may request a copy from our privacy office or obtain a copy on our Website.

Complaints

You may submit a complaint to us if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying the Compliance & Privacy Office at Lorien Health Services, 3300 N. Ridge Road Suite 390, Ellicott City, MD 21043, and 443-574-1112. We will not retaliate against you for filing a complaint. You may also contact us about the complaint process. Additionally, you also have the right to submit a complaint to the United States Secretary of Health and Human Services if you believe your privacy rights have been violated by us.

Contact

For more information about this Notice of your privacy, you may contact our privacy officer at 443-574-1112 or hipaaprivacy@lorienhealth.com.

This Notice of Privacy Practices applies to Lorien Health Services and all of it's the following organizations.

Maryland Health Enterprise
Lorien Encore at Turf Valley
Lorien Harmony Hall
Lorien Bel Air
Lorien Bulle Rock
Lorien Columbia
Lorien Elkridge
Lorien Mays Chapel
Lorien Mt. Airy
Lorien Taneytown
Lorien at Home
Lorien Rehab & Fitness
Lorien Dialysis

JUNE WALTROP c/o Murphy, Falcon & Murphy 1 South Street 30th Floor Baltimore, Maryland 21202	*	IN THE CIRCUIT COURT FOR
WILLIAM WALTROP c/o Murphy, Falcon & Murphy 1 South Street 30th Floor Baltimore, Maryland 21202	*	BALTIMORE COUNTY CASE NO. C-03-CV-21-001062
Plaintiffs	*	
v.	*	
MARYLAND HEALTH ENTERPRISES, INC., d/b/a LORIEN HEALTH SERVICES 1205 York Road Lutherville, MD 21093	*	
SERVE ON: Resident Agent LINDA M. LICATA 1205 York Road Penthouse Suite Lutherville, MD 21093	*	
Defendant	*	

* * * * * * * * * * * * *

REQUEST FOR WRIT OF SUMMONS

Dear Clerk:

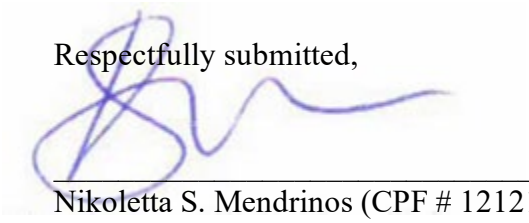
Please issue a writ of summons and return to undersigned counsel for service by private process for the following Defendant:

MARYLAND HEALTH ENTERPRISES,
INC., d/b/a LORIEN HEALTH
SERVICES
1205 York Road
Lutherville, MD 21093

SERVE ON:

Resident Agent
LINDA M. LICATA
1205 York Road
Penthouse Suite
Lutherville, MD 21093

Respectfully submitted,



Nikoletta S. Mendrinos (CPF # 1212120253)
Kaitlyn T. Holzer (CPF # 2012170242)
One South Street, 30th Floor
Baltimore, Maryland 21202
T: (410) 951-8744
F: (410) 539-6599
nikoletta.mendrinos@murphyfalcon.com
kaitlyn.holzer@murphyfalcon.com

IN THE CIRCUIT COURT FOR Baltimore County
(City or County)

CIVIL - NON-DOMESTIC CASE INFORMATION REPORT

DIRECTIONS

Plaintiff: This Information Report must be completed and attached to the complaint filed with the Clerk of Court unless your case is exempted from the requirement by the Chief Judge of the Court of Appeals pursuant to Rule 2-111(a).

Defendant: You must file an Information Report as required by Rule 2-323(h).

THIS INFORMATION REPORT CANNOT BE ACCEPTED AS A PLEADING

FORM FILED BY: ☒PLAINTIFF ☐DEFENDANT CASE NUMBER C-03-CV-21-001062 (Clerk to insert)

CASE NAME: June C. Waltrop, et al. (Plaintiff) vs. Maryland Health Enterprises, Inc. (Defendant)

PARTY'S NAME: June C. Waltrop PHONE: 410-951-8744

PARTY'S ADDRESS: 8 Flanders Ridge Court Cockeysville, MD 21030

PARTY'S E-MAIL: nikoletta.mendrinos@murphyfalcon.com

If represented by an attorney:

PARTY'S ATTORNEY'S NAME: Nikoletta Mendrinos PHONE: 410-951-8824

PARTY'S ATTORNEY'S ADDRESS: 1 South Street, 30th Floor, Baltimore, MD 21202

PARTY'S ATTORNEY'S E-MAIL: nikoletta.mendrinos@murphyfalcon.com

JURY DEMAND? ☒Yes ☐No

RELATED CASE PENDING? ☒Yes ☐No If yes, Case #(s), if known: C-03-CV-20-002899

ANTICIPATED LENGTH OF TRIAL?: ____hours 7 days

PLEADING TYPE

New Case: ☒Original ☐Administrative Appeal ☐Appeal

Existing Case: ☐Post-Judgment ☐Amendment

If filing in an existing case, skip Case Category/ Subcategory section - go to Relief section.

IF NEW CASE: CASE CATEGORY/SUBCATEGORY (*Check one box.*)

TORTS
- ☐Asbestos
- ☐Assault and Battery
- ☐Business and Commercial
- ☐Conspiracy
- ☐Conversion
- ☐Defamation
- ☐False Arrest/Imprisonment
- ☐Fraud
- ☐Lead Paint - DOB of Youngest Plt: _____
- ☐Loss of Consortium
- ☐Malicious Prosecution
- ☐Malpractice-Medical
- ☐Malpractice-Professional
- ☐Misrepresentation
- ☐Motor Tort
- ☒Negligence
- ☐Nuisance
- ☐Premises Liability
- ☐Product Liability
- ☐Specific Performance
- ☐Toxic Tort
- ☐Trespass
- ☐Wrongful Death

CONTRACT
- ☐Asbestos
- ☐Breach
- ☐Business and Commercial
- ☐Confessed Judgment (Cont'd)
- ☐Construction
- ☐Debt
- ☐Fraud
- ☐Government
- ☐Insurance
- ☐Product Liability

PROPERTY
- ☐Adverse Possession
- ☐Breach of Lease
- ☐Detinue
- ☐Distress/Distrain
- ☐Ejectment
- ☐Forcible Entry/Detainer
- ☐Foreclosure
  - ☐Commercial
  - ☐Residential
  - ☐Currency or Vehicle
  - ☐Deed of Trust
  - ☐Land Installments
  - ☐Lien
  - ☐Mortgage
  - ☐Right of Redemption
  - ☐Statement Condo
- ☐Forfeiture of Property / Personal Item
- ☐Fraudulent Conveyance
- ☐Landlord-Tenant
- ☐Lis Pendens
- ☐Mechanic's Lien
- ☐Ownership
- ☐Partition/Sale in Lieu
- ☐Quiet Title
- ☐Rent Escrow
- ☐Return of Seized Property
- ☐Right of Redemption
- ☐Tenant Holding Over

PUBLIC LAW
- ☐Attorney Grievance
- ☐Bond Forfeiture Remission
- ☐Civil Rights
- ☐County/Mncpl Code/Ord
- ☐Election Law
- ☐Eminent Domain/Condemn.
- ☐Environment
- ☐Error Coram Nobis
- ☐Habeas Corpus
- ☐Mandamus
- ☐Prisoner Rights
- ☐Public Info. Act Records
- ☐Quarantine/Isolation
- ☐Writ of Certiorari

EMPLOYMENT
- ☐ADA
- ☐Conspiracy
- ☐EEO/HR
- ☐FLSA
- ☐FMLA
- ☐Workers' Compensation
- ☐Wrongful Termination

INDEPENDENT PROCEEDINGS
- ☐Assumption of Jurisdiction
- ☐Authorized Sale
- ☐Attorney Appointment
- ☐Body Attachment Issuance
- ☐Commission Issuance
- ☐Constructive Trust
- ☐Contempt
- ☐Deposition Notice
- ☐Dist Ct Mtn Appeal
- ☐Financial
- ☐Grand Jury/Petit Jury
- ☐Miscellaneous
- ☐Perpetuate Testimony/Evidence
- ☐Prod. of Documents Req.
- ☐Receivership
- ☐Sentence Transfer
- ☐Set Aside Deed
- ☐Special Adm. - Atty
- ☐Subpoena Issue/Quash
- ☐Trust Established
- ☐Trustee Substitution/Removal
- ☐Witness Appearance-Compel

PEACE ORDER
- ☐Peace Order

EQUITY
- ☐Declaratory Judgment
- ☐Equitable Relief
- ☐Injunctive Relief
- ☐Mandamus

OTHER
- ☐Accounting
- ☐Friendly Suit
- ☐Grantor in Possession
- ☐Maryland Insurance Administration
- ☐Miscellaneous
- ☐Specific Transaction
- ☐Structured Settlements

IF NEW OR EXISTING CASE: RELIEF (Check All that Apply)

- ☐ Abatement
- ☐ Administrative Action
- ☐ Appointment of Receiver
- ☐ Arbitration
- ☐ Asset Determination
- ☐ Attachment b/f Judgment
- ☐ Cease & Desist Order
- ☐ Condemn Bldg
- ☐ Contempt
- ☐ Court Costs/Fees
- ☐ Damages-Compensatory
- ☐ Damages-Punitive
- ☐ Earnings Withholding
- ☐ Enrollment
- ☐ Expungement
- ☐ Findings of Fact
- ☐ Foreclosure
- ☐ Injunction
- ☐ Judgment-Affidavit
- ☐ Judgment-Attorney Fees
- ☐ Judgment-Confessed
- ☐ Judgment-Consent
- ☐ Judgment-Declaratory
- ☐ Judgment-Default
- ☐ Judgment-Interest
- ☐ Judgment-Summary
- ☐ Liability
- ☐ Oral Examination
- ☐ Order
- ☐ Ownership of Property
- ☐ Partition of Property
- ☐ Peace Order
- ☐ Possession
- ☐ Production of Records
- ☐ Quarantine/Isolation Order
- ☐ Reinstatement of Employment
- ☐ Return of Property
- ☐ Sale of Property
- ☐ Specific Performance
- ☐ Writ-Error Coram Nobis
- ☐ Writ-Execution
- ☐ Writ-Garnish Property
- ☐ Writ-Garnish Wages
- ☐ Writ-Habeas Corpus
- ☐ Writ-Mandamus
- ☐ Writ-Possession

*If you indicated **Liability** above*, mark one of the following. This information is not an admission and may not be used for any purpose other than Track Assignment.

☐ Liability is conceded. ☐ Liability is not conceded, but is not seriously in dispute. ☐ Liability is seriously in dispute.

MONETARY DAMAGES (Do not include Attorney's Fees, Interest, or Court Costs)

☐ Under $10,000 ☐ $10,000 - $30,000 ☐ $30,000 - $100,000 ☒ Over $100,000

☐ Medical Bills $_____ ☐ Wage Loss $_____ ☐ Property Damages $_____

ALTERNATIVE DISPUTE RESOLUTION INFORMATION

Is this case appropriate for referral to an ADR process under Md. Rule 17-101? (Check all that apply)

A. Mediation	☒ Yes	☐ No	C. Settlement Conference	☒ Yes	☐ No
B. Arbitration	☐ Yes	☒ No	D. Neutral Evaluation	☐ Yes	☒ No

SPECIAL REQUIREMENTS

☐ If a Spoken Language Interpreter is needed, **check here and attach form CC-DC-041**

☐ If you require an accommodation for a disability under the Americans with Disabilities Act, **check here and attach form CC-DC-049**

ESTIMATED LENGTH OF TRIAL

*With the exception of Baltimore County and Baltimore City, please fill in the estimated **LENGTH OF TRIAL**.*

(Case will be tracked accordingly)

- ☐ 1/2 day of trial or less
- ☐ 1 day of trial time
- ☐ 2 days of trial time
- ☐ 3 days of trial time
- ☐ More than 3 days of trial time

BUSINESS AND TECHNOLOGY CASE MANAGEMENT PROGRAM

***For all jurisdictions**, if Business and Technology track designation under Md. Rule 16-308 is requested, attach a duplicate copy of complaint and check one of the tracks below.*

☐ **Expedited**- Trial within 7 months of Defendant's response

☐ **Standard** - Trial within 18 months of Defendant's response

EMERGENCY RELIEF REQUESTED

COMPLEX SCIENCE AND/OR TECHNOLOGICAL CASE MANAGEMENT PROGRAM (ASTAR)

FOR PURPOSES OF POSSIBLE SPECIAL ASSIGNMENT TO ASTAR RESOURCES JUDGES under Md. Rule 16-302, attach a duplicate copy of complaint and check whether assignment to an ASTAR is requested.

☐ **Expedited** - Trial within 7 months of Defendant's response

☐ **Standard** - Trial within 18 months of Defendant's response

IF YOU ARE FILING YOUR COMPLAINT IN BALTIMORE CITY, OR BALTIMORE COUNTY, PLEASE FILL OUT THE APPROPRIATE BOX BELOW.

CIRCUIT COURT FOR BALTIMORE CITY (CHECK ONLY ONE)

☐	Expedited	Trial 60 to 120 days from notice. Non-jury matters.
☐	Civil-Short	Trial 210 days from first answer.
☐	Civil-Standard	Trial 360 days from first answer.
☐	Custom	Scheduling order entered by individual judge.
☐	Asbestos	Special scheduling order.
☐	Lead Paint	Fill in: Birth Date of youngest plaintiff _____.
☐	Tax Sale Foreclosures	Special scheduling order.
☐	Mortgage Foreclosures	No scheduling order.

CIRCUIT COURT FOR BALTIMORE COUNTY

☐	Expedited (Trial Date-90 days)	Attachment Before Judgment, Declaratory Judgment (Simple), Administrative Appeals, District Court Appeals and Jury Trial Prayers, Guardianship, Injunction, Mandamus.
☐	Standard (Trial Date-240 days)	Condemnation, Confessed Judgments (Vacated), Contract, Employment Related Cases, Fraud and Misrepresentation, International Tort, Motor Tort, Other Personal Injury, Workers' Compensation Cases.
☐	Extended Standard (Trial Date-345 days)	Asbestos, Lender Liability, Professional Malpractice, Serious Motor Tort or Personal Injury Cases (medical expenses and wage loss of $100,000, expert and out-of-state witnesses (parties), and trial of five or more days), State Insolvency.
☒	Complex (Trial Date-450 days)	Class Actions, Designated Toxic Tort, Major Construction Contracts, Major Product Liabilities, Other Complex Cases.

April 9, 2021
Date

1 South Street, 30th Floor
Address

Baltimore — MD — 21202
City — State — Zip Code

Signature of Counsel / Party

Kaitlyn Holzer
Printed Name