IN THE CIRCUIT COURT FOR BALTIMORE CITY, MARYLAND

JANE DOE 1 **c/o** **GRANT & EISENHOFER P.A.** 3600 Clipper Mill Rd. Suite 240 Baltimore, MD 21211	:	
JANE DOE 2 **c/o** **GRANT & EISENHOFER P.A.** 3600 Clipper Mill Rd. Suite 240 Baltimore, MD 21211	:	
JANE DOE 3 **c/o** **GRANT & EISENHOFER P.A.** 3600 Clipper Mill Rd. Suite 240 Baltimore, MD 21211	:	**Case No. C-24-CV-25-002505**
JANE DOE 4 **c/o** **GRANT & EISENHOFER P.A.** 3600 Clipper Mill Rd. Suite 240 Baltimore, MD 21211	:	
JANE DOE 5 **c/o** **GRANT & EISENHOFER P.A.** 3600 Clipper Mill Rd. Suite 240 Baltimore, MD 21211	:	
JANE DOE 6 **c/o** **GRANT & EISENHOFER P.A.** 3600 Clipper Mill Rd. Suite 240 Baltimore, MD 21211	:	
Plaintiffs,	:	

v.	:
	:
UNIVERSITY OF MARYLAND	:
MEDICAL SYSTEM CORPORATION	:
Serve on: Registered Agent:	:
Adil A. Daudi	:
250 West Pratt St., 24th Floor	:
Baltimore, MD 21201	:
	:
	:
UNIVERSITY OF MARYLAND	:
MEDICAL CENTER, LLC	:
Serve on: Registered Agent:	:
University of Maryland Medical	:
System Co.	:
250 West Pratt St., 24th Floor	:
Baltimore, MD 21201	:
	:
Defendants.	:

FIRST AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Jane Doe 1[1] and Jane Does 2-6[2] ("Plaintiffs"), individually on behalf of themselves and on behalf of the class of similarly situated individuals, by and through their undersigned attorneys, bring this First Amended Class Action Complaint and Demand for Jury Trial against Defendants, University of Maryland Medical System Corporation ("UMMS") and the University of Maryland Medical Center, LLC ("UMMC" or the "Medical Center") (collectively the "Defendants") based upon their personal knowledge of their own acts and experiences, and, as to all other matters, upon information and belief.

[1] Along with the Complaint, Jane Doe 1 submitted a motion for leave to proceed under a pseudonym, which this Court granted on March 31, 2025. *See* Order dated March 31, 2025, Envelope: 20584257.

[2] Along with this First Amended Complaint, Jane Does 2-6 have submitted a motion for leave to proceed under pseudonyms setting forth the precise points and authorities supporting their request to proceed anonymously in this matter due to the highly sensitive and personal nature of the privacy invasions giving rise to their claims and the fear of retaliation from the criminal offender named herein.

I. INTRODUCTION TO THE ACTION

1. The scale of the privacy invasions giving rise to this action is as unprecedented as it is shocking. For nearly a decade, a single pharmacist named Matthew Bathula installed spyware on at least 400 computers in clinics, treatment rooms, labs and a variety of other locations at one of the nation's premier teaching hospitals. Bathula used this spyware to remotely access webcams to record videos of young doctors and medical residents pumping breastmilk in closed treatment rooms, and to use home security cameras to record women breastfeeding their babies, interacting with young children, and having sex with their husbands in the privacy of their homes. He accessed his coworkers' personal photo libraries and captured, downloaded, and retained their intimate photographs and personally-identifiable information.

2. UMMC's role in this case is best exemplified by the ancient legal concept of *res ipsa loquitur*—the thing speaks for itself. UMMC is a teaching hospital that conducts sensitive research and provides critical healthcare services to thousands of patients each year. Accordingly, UMMC (and UMMS) are subject to numerous state and federal regulations that require UMMC to implement measures to protect the sensitive information stored on its computer systems. Bathula could not have pulled off his decade-long cyber spying campaign unless Defendants' data security measures at UMMC were woefully inadequate.

3. Bathula was a Clinical Pharmacy Specialist at a clinic within UMMC. UMMC partners with the University of Maryland School of Pharmacy (the "School"), from which Bathula obtained a doctorate in pharmacy in 2008. In his work as a Clinical Pharmacy Specialist, Bathula interacted with and supervised pharmacy residents and numerous other medical professionals whom he ultimately targeted.

4. Upon information and belief, Bathula had no affiliation with UMMC's Information Technology ("IT") office and had no authority or reason to access or install hardware or software on any computers at UMMC.

5. Yet Bathula readily accessed approximately 400 computers he had no legitimate reason to access in buildings at both UMMC campuses and successfully installed key logging spyware on those devices.

6. Defendants are or should be aware of the dangers associated with the type of key logging hardware and/or software Bathula apparently used. One of UMMS's own vendors, Crowdstrike, warns that key logging spyware is widely available and proposes numerous solutions for dealing with the threat.[3]

7. Even though Defendants are subject to numerous laws regarding protected health information and data privacy, to date they have not issued data breach notices to the affected employees and/or patients which disclosed the far-reaching breadth of Bathula's cyber-stalking. The only specific notice victims have received came from the Federal Bureau of Investigation ("FBI"), which is investigating the incident.

8. Defendants' failure to take reasonable, readily available measures to protect its employees irreparably destroyed their sense of security, safety, intimacy, and well-being.

II. PARTIES

9. Plaintiff Jane Doe 1 is an adult individual who resides in Baltimore City, Maryland. Plaintiff Jane Doe 1 was a healthcare provider working at the Medical Center during the relevant period.

[3] CrowdStrike, *What is a Keylogger?*, CrowdStrike (last visited March 27, 2025), https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/keylogger/.

10. Plaintiff Jane Doe 2 is an adult individual who resides in Howard County, Maryland. Plaintiff Jane Doe 2 was a healthcare provider working at the Medical Center during the relevant period.

11. Plaintiff Jane Doe 3 is an adult individual who resides in Baltimore City, Maryland. Plaintiff Jane Doe 3 was a healthcare provider working at the Medical Center during the relevant period.

12. Plaintiff Jane Doe 4 is an adult individual who resides in Anne Arundel County, Maryland. Plaintiff Jane Doe 4 was a healthcare provider working at the Medical Center during the relevant period.

13. Plaintiff Jane Doe 5 is an adult individual who currently resides in North Carolina. Plaintiff Jane Doe 5 was a healthcare provider working at the Medical Center during the relevant period.

14. Plaintiff Jane Doe 6 is an adult individual who resides in Howard County, Maryland. Jane Doe 6 was a healthcare provider working at the Medical Center during the relevant period.

15. Defendant UMMS is a private, not-for-profit corporation organized and existing under the laws of Maryland with its principal place of business in Baltimore City, Maryland. UMMS provides comprehensive healthcare services through an integrated regional network of hospitals and related clinical enterprises. UMMS claims to be one largest private employers in the state, with 28,000 employees and 4,000 affiliated physicians, who provide care in more than 150 locations and at 12 hospitals.

16. Defendant UMMC is a limited liability corporation organized and existing under the laws of Maryland with its principal place of business in Baltimore City, Maryland. The Medical

Center is the flagship academic campus of UMMS. It is registered as an LLC incorporated in Maryland. Its campus principally includes a 739-bed downtown Baltimore hospital and a 201-bed midtown hospital. The medical staff at the Medical Center comprises more than 1,500 attending physicians, as well as 950 residents and fellows in all medical specialties.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to Md. Code Ann., Cts. & Jud. Proc. §§ 1-501 and 4-401.

18. This Court has personal jurisdiction over Defendants pursuant to Md. Code Ann., Cts. & Jud. Proc. § 6-102(a) and § 6-103(b) because they are domiciled in and conduct business in Maryland.

19. Venue is proper in this County pursuant to Md. Code. Ann. Cts. § Jud. Proc. §6-201(a) because Defendants are domiciled in and carry on regular business in this judicial district.

20. This claim is instituted for the recovery of damages in an amount in excess of the Circuit Court's jurisdictional threshold of $30,000.00.

IV. COMMON FACTUAL ALLEGATIONS

A. Bathula Had Unfettered Access to Computers, Laptops and Cameras

21. Bathula was an actual and/or apparent agent, servant, and/or employee of UMMS, acting within the course and scope of his agency.

22. Bathula was an actual and/or apparent agent, servant, and/or employee of UMMC, acting within the course and scope of his agency.

23. Defendants employed, controlled, and supervised Bathula as a Clinical Pharmacy Specialist, assigned to work at the Medical Center campuses and its affiliated clinics, including the James Frenkil Building on Eutaw Street in Baltimore City, Maryland (the "Frenkil Building").

24. Defendants owned, operated, managed, maintained, and/or controlled the Medical Center and its computer system, including both stationary computers at the Medical Center campuses and the laptops issued to Medical Center employees, servants, and/or agents.

25. Defendants required Medical Center employees to log into stationary computers and work-issued laptops to conduct their business while in the Medical Center and its clinics or while conducting Medical Center business remotely.

26. In the Medical Center hospital, employees could log in to stationary computers either by manually typing in their UMMS usernames and passwords or, if they had already manually logged in earlier that day, via their Medical Center badges. To log into the computer stations in the Frenkil Building, the username and password was required. Employees also logged into their work-issued laptops via their UMMS usernames and passwords.

27. Bathula had unfettered access to hundreds of those stationary computer stations located within the Medical Center campuses, including within the Frenkil Building, and to rooms where laptops issued by Defendants were stored, housed, and/or kept.

28. The computer stations in patient-exam rooms in the Frenkil Building were also equipped with cameras. Bathula had unfettered access to those cameras.

29. Defendants required employees to swipe badges to access different floors, clinics, labs or other distinct areas of the Medical Center. Therefore, Bathula had to swipe his electronic badge before entering any of the rooms in which the devices on which he installed his spyware were located.

30. Upon information and belief, Defendants were able to track the location of any given employee by accessing the electronic record created by each employee badge swipe.

31. Accordingly, Defendants knew or should have known each location within the Medical Center and its clinics where Bathula was physically located on any given day.

32. Upon information and belief, Bathula routinely used his badge to gain admission to various sections and units of the Medical Center, including many locations where he had no legitimate business purpose to be. These admissions allowed him to then access hundreds of Medical Center computers, which were commonly used by pharmacists, residents, physicians and medical personnel staffing those individual units.

B. Bathula Used This Access to Invade the Privacy of His Coworkers at Work, Home, and in their Private Accounts

33. For approximately 10 years, Bathula used his widespread access to install keyloggers or keystroke loggers onto the Medical Center stationary computers and laptops.

34. A keylogger or keystroke logger (collectively referred to herein as "keyloggers") is a form of malware or hardware that keeps track of and records a computer user's keystrokes as they type. The malware/hardware retains the keystroke information and then sends that information to the person controlling it. Keyloggers with Wi-Fi capabilities can be accessed remotely once they have been installed on a target device. Keyloggers record everything that a computer user types, including passwords, account information, emails, searches, and personal information.

35. Keyloggers come in two primary forms: (1) software that is downloaded onto the computer by a user; or (2) hardware that is attached to the keyboard via a USB port. The latter form is visible to the naked eye; the former is easily detectable using antivirus tools.

36. Bathula downloaded and/or installed keyloggers on over 400 Medical Center stationary computers and laptops. Those keyloggers then sent him his coworkers' usernames and passwords for their personal accounts, including, but not limited to: bank accounts, emails, home

surveillance systems, Drop Box accounts, Google Drives, dating applications, Google Nests, and iCloud accounts. Because Bathula was able to learn username and password patterns, he was able to gain access to UMMC computer users' personal accounts even though the user had never specifically logged into that account on a UMMC computer.

37. Bathula captured and retained lists of Medical Center employees' login credentials. He used that information to then access the personal accounts of his coworkers. Once inside those accounts, he downloaded and retained Medical Center employees' private photographs, videos, and personally identifying information ("PII"). He also surveilled Medical Center employees in real-time in the privacy of their own homes and captured and recorded private and intimate moments with their spouses and families.

38. In addition to invading his coworkers' privacy through the theft of their usernames and passwords, he remotely activated webcams Defendants had installed in the Frenkil Building exam rooms for telehealth sessions. For several years, he remotely activated webcams in the patient exam rooms and watched, captured, and recorded his newly postpartum coworkers pumping breastmilk for their babies without their knowledge or consent.

C. Defendants Eventually Learned of Bathula's Attacks, But Failed to Notify Employees that Their Private Lives and Data Had Been Compromised

39. On October 1, 2024, Defendants sent a blast email to employees working within the Medical Center vaguely referencing "a serious IT incident that may have impacted patients and team members at the University of Maryland Medical Center Downtown Campus."

40. In that correspondence, Defendants stated that "over the last number of weeks, we have uncovered a highly sophisticated and very difficult to detect cyberattack that has resulted in the theft of data from shared UMMS computers located at the University of Maryland Medical Center and the Frenkil Building."

41. Defendants admitted that "the theft of data has been ongoing for an indeterminate but sustained period and involves the use of software that captures and records information that could be used to steal logins and passwords, allowing a perpetrator to impersonate another user online."

42. Defendants further admitted that they had been investigating the privacy breach ahead of the October 1 email in conjunction with "highly specialized cybersecurity experts with experience in complex attacks."

43. Defendants promised to "contact potentially impacted team members and patients directly."

44. Defendants admitted that they were "evaluating several changes to [their] security practices" and that they would "communicate further about those developments in the coming days."

45. But Defendants' promises were hollow. Defendants failed to notify employees about: (1) whether their data was breached; (2) the extent of Bathula's access to webcams in exam rooms and in employees' homes, and his access into their private photo libraries, emails, and cloud storage; or (3) what, if anything they were doing to prevent future privacy breaches.

46. The only notice Plaintiffs and class members have received has been through interviews with FBI investigators.

47. In the interim, Defendants placed Bathula on administrative leave and subsequently terminated his employment. Bathula is currently working for another health system as a pharmacist. Upon information and belief, Defendants have not informed Bathula's new employer of his heinous crimes despite the impact those crimes had on so many Medical Center employees and (as Defendants themselves recognized) potentially patient safety and security.

48. Other than sending the generic October 1, 2024 correspondence, which was utterly deficient in terms of notifying victims of the full extent to which their lives had been invaded, Defendants have failed to inform Medical Center employees of precisely what Bathula accessed and retained. Defendants failed to notify former Medical Center employees of any breach whatsoever.

49. Instead, Bathula's victims have been individually contacted by agents working for the FBI who presented them with samplings of the PII, photographs, videos, and recordings that Bathula had stored on his devices and servers. Impacted employees still have no idea what all Bathula viewed but did not retain or what he viewed and then disclosed to third parties. Because the FBI only showed them samplings of the retained information, victims do not know what Bathula retained.

50. Although Defendants have done little to protect and support their employees, Defendants have taken measures to protect themselves. In one single day following the October 1 email, Defendants removed and replaced all 400 compromised computers, including both stationary computers and employee-issued laptops. Defendants also removed and replaced the cameras located in the patient exam rooms in the Frenkil Building. Defendants have failed to notify any employees who may have been surveilled in the Frenkil Building exam rooms and, upon information and belief, have failed to inform patients who may have been surveilled and/or recorded.

51. Defendants have since put IT protections in place that were readily available prior to Bathula's attacks and which are reasonable and standard in the industry. For example, Defendants have since disabled the use of thumb drives from their computer stations and have put protections in place to stop computer users from uploading or downloading any foreign

applications. These minimal protections were not in the place during Bathula's decade of criminal cyber activity.

D. Defendants Were on Notice of the Potential for Cyber Voyeurism and Data Breaches but Failed to Employ Reasonably Available Measures to Prevent and Uncover the Attacks

52. Defendants admitted in their October 1 email to employees that they were investigating suspicious activity for several weeks before they notified employees. But, according to statements made by Medical Center IT personnel at a winter event, Defendants knew about Bathula's hacking for several years.

53. Upon information and belief, an employee in Defendants' IT department stated that Defendants were aware of a potential hacking incident for years but were unable to "catch" the offender.

54. Upon information and belief, another employee of Defendants' IT department separately disclosed that Defendants were alerted in the summer of 2024 of a potential security breach but were, again, unable to catch the offender.

55. Defendants' failure to conduct a sufficient investigation to uncover Bathula as the offender and/or to understand the extent of the data breach is nothing short of negligence.

56. Upon and information and belief, Bathula continued his cyber voyeurism campaign after Defendants were on notice of his conduct.

57. Equally concerning, is Defendants failure to employ reasonably available measures to identify and protect the vulnerabilities within its computer system and prevent Bathula's attacks from ever occurring.

58. Defendants are subject to heightened cybersecurity requirements through, among other laws, regulations and industry standards, the Health Information Technology for Economic

and Clinical Health Act (the "HITECH Act" 42 U.S.C. § 156). That Act imposes strict requirements for securing electronically stored health records *and* strict requirements for providing prompt notice to individuals potentially impacted by data breaches.

59. Upon information and belief, Defendants have failed to comply with either central provision of the HITECH Act among other state and federal data protection laws and regulations.

60. Bathula is far from the technical genius Defendants' communications suggests he is.

61. Devices and software allowing remote keystroking are widely available and have been many years. Indeed, Defendants' own cybersecurity vendor has warned of the danger posed by keystroking devices and software.[4]

62. As an organization housing protected health records and other sensitive data and electronically stored information, Defendants were required to take measures to guard against threats posed by keystroking devices and software. These measures include, but are not limited to:

a. Restricting user permissions such that no user can install hardware/software other than an administrator;

b. Disabling USB, USBc and other computer ports to prevent users from inserting Keystroking and other devices into company computers;

c. Installing USB data blockers to prevent unauthorized hardware devices from transmitting data;

d. Conducting regular hardware inspections;

e. Installing Keystroke Encryption Software;

[4] *See supra* n.2.

f. Installing and updating robust firewalls to monitor and control network traffic and to prevent keyloggers from transmitting captured data to external servers;

g. Training users in how to recognize suspicious cyber activity;

h. Requiring users to use password managers and multi-factor authentication;

i. Using behavioral biometrics to detect anomalies that may indicate keylogger activity;

j. Restricting employee badge access to areas relating to the employee's job function;

k. Implementing zero trust security models where no user or device is trusted by default and, instead, must be verified to be granted access to systems; and

l. Conducting regular security audits of all IT systems.

JANE DOE 1'S FACTUAL ALLEGATIONS

63. Jane Doe 1 adopts and incorporates by reference all allegations contained in the paragraphs above as if fully set forth herein.

64. At all material times hereto, Jane Doe 1 was a medical professional who worked at the Medical Center.

65. Jane Doe 1 had a reasonable expectation of privacy in her personal accounts and home surveillance system.

66. Jane Doe 1 used Medical Center computer stations during the course and scope of her employment on a regular and routine basis.

67. Between November, 2024, and February, 2025, Jane Doe 1 received an unsettling phone call from the FBI requesting a meeting.

68. During that meeting, Jane Doe 1 was informed that she was a victim of Bathula's cyber-voyeurism attack and was shown a sampling of what confidential and private information Bathula accessed, captured, and retained with respect to her individually.

69. Jane Doe 1 learned that Bathula had accessed the photos stored in her cloud (internet-based storage), viewed them, and retained the following:

a) photos of her breastfeeding her minor child;

b) photos of her children;

c) PII, including photos of her driver's license;

d) screenshots of phone numbers for romantic partners with whom she was communicating; and

e) photographs showing her private areas that she took and sent to a romantic partner.

70. Jane Doe 1 considered these photographs and this information private and deeply personal.

71. In addition to downloading and retaining her private photographs, Jane Doe 1 also learned that Bathula had used the keyloggers to obtain her username and password for her home surveillance system even though she had never logged into her home surveillance system from her UMMC computer.

72. Bathula used her login information to access her cameras in real-time, disable the light that would tell her that they were on, and actively surveille her and her family, including her minor child, in the privacy and sanctity of their home. During this active surveillance, Bathula took photos and recorded videos of Jane Doe 1 and her minor child and retained them on his servers.

73. Jane Doe 1 obtained logs of this access from her home surveillance provider. In the past year alone, Bathula actively surveilled Jane Doe 1 *on 12 separate occasions*, including on August 16, 2024, August 30, 2024, September 24, 2024, and September 30, 2024, *when*

Defendants admit that they had notice of Bathula's crimes but had not yet placed him on leave, taken away his access to their systems, or notified any potential victims.

74. Jane Doe 1 did not consent to Bathula's invasion.

JANE DOE 2'S FACTUAL ALLEGATIONS

75. Jane Doe 2 adopts and incorporates by reference all allegations contained in the paragraphs 1 through 62 as if fully set forth herein.

76. At all material times hereto, Jane Doe 2 was a medical professional who worked at the Medical Center.

77. Jane Doe 2 had a reasonable expectation of privacy in her personal accounts and home surveillance system.

78. Jane Doe 2 used Medical Center computer stations during the course and scope of her employment on a regular and routine basis.

79. At some point between November, 2024, and February, 2025, Jane Doe 2 received an unsettling phone call from the FBI requesting a meeting.

80. During that meeting, Jane Doe 2 was informed that she was a victim of Bathula's cyber-voyeurism attack and was presented with sampling of her confidential and private information that Bathula accessed, captured, and retained.

81. Jane Doe 2 learned that Bathula accessed the photos stored in her cloud, viewed them, and retained the following:

a) photos of her doing skin to skin contact with her newborn;

b) photos of her on vacation with her husband;

c) photos of her minor children; and

d) PII, including her driver's license and W2.

82. These photographs were not available to the public. Jane Doe 2 considers these photographs and this information private and deeply personal.

83. In addition to downloading and retaining her private photographs, Jane Doe 2 also learned that Bathula had used the keyloggers to obtain her username and password for her home surveillance system even though she had never logged into her home surveillance system from her UMMC computer.

84. Bathula used her login information to access her cameras in real-time and actively surveille her and her family, including her minor children. During this active surveillance, Bathula took photos and recorded videos of Jane Doe 2, her husband, and her minor children in the privacy and sanctity of their home, including still pictures and recorded videos which depicted:

a) Jane Doe 2 in various stages of undress;

b) Jane Doe 2 having sex with her husband;

c) Jane Doe 2 breastfeeding; and

d) Jane Doe 2's children.

85. Jane Doe 2 did not consent to Bathula's invasion.

JANE DOE 3's FACTUAL ALLEGATIONS

86. Jane Doe 3 adopts and incorporates by reference all allegations contained in the paragraphs 1 through 62 as if fully set forth herein.

87. At all material times hereto, Jane Doe 3 was a medical professional who worked at the Medical Center.

88. Jane Doe 3 had a reasonable expectation of privacy in her personal accounts.

89. Jane Doe 3 used Medical Center computer stations during the course and scope of her employment on a regular and routine basis.

90. At some point between November, 2024, and February, 2025, Jane Doe 3 received an unsettling phone call from the FBI requesting a meeting.

91. During that meeting, Jane Doe 3 was informed that she was a victim of Bathula's cyber-voyeurism attack and was shown a sampling of the confidential and private information Bathula accessed, captured, and retained from her.

92. Jane Doe 3 learned that Bathula had accessed the photos stored in her cloud, viewed them, and retained the following:

a) Private photos depicting intimate, private areas of her body; and

b) PII, including her license, passport, and credit cards.

93. Neither the photographs nor most of the PII and other information were publicly available. Jane Doe 3 considers these photographs and this information private and deeply personal.

94. Jane Doe 3 did not consent to Bathula's invasion.

JANE DOE 4's FACTUAL ALLEGATIONS

95. Jane Doe 4 adopts and incorporates by reference all allegations contained in the paragraphs 1 through 62 as if fully set forth herein.

96. At all material times hereto, Jane Doe 4 was a medical professional who worked at the Medical Center.

97. Jane Doe 4 had a reasonable expectation of privacy in her personal accounts.

98. Jane Doe 4 used Medical Center computer stations during the course and scope of her employment on a regular and routine basis.

99. At some point between November, 2024, and February, 2025, Jane Doe 4 received an unsettling phone call from the FBI requesting a meeting.

100. During that meeting, Jane Doe 4 was informed that she was a victim of Bathula's cyber-voyeurism attack and was presented with a sampling of what confidential and private information Bathula accessed, captured, and retained from her.

101. Jane Doe 4 learned that Bathula had accessed the photos stored in her cloud, viewed them, and retained the following:

c) Private, personal photos depicting her and her family, including a private photo of her getting dressed; and

d) PII, including her license.

102. Neither the photographs nor most of the PII and other information were publicly available. Jane Doe 4 considers these photographs and this information private and deeply personal.

103. Jane Doe 4 did not consent to Bathula's invasion.

JANE DOE 5's FACTUAL ALLEGATIONS

104. Jane Doe 5 adopts and incorporates by reference all allegations contained in the paragraphs 1 through 62 as if fully set forth herein.

105. At all material times hereto, Jane Doe 5 was a medical resident who worked at the Medical Center.

106. Jane Doe 5 had a reasonable expectation of privacy in her personal accounts.

107. Jane Doe 5 used Medical Center computer stations during the course and scope of her residency on a regular and routine basis.

108. As part of her residency program, she was specifically required to access documents using google drive. Because the Medical Center email domain was not Gmail, Jane Doe 5 was required to use her personal Gmail account to access google drive and, therefore, had to log into

her personal Gmail account on Medical Center computers. Upon information and belief, many other residents and employees of the Medical Center were required to do the same.

109. At some point between November, 2024, and February, 2025, Jane Doe 5 received an unsettling phone call from the FBI requesting a meeting.

110. During that meeting, Jane Doe 5 was informed that she was a victim of Bathula's cyber-voyeurism attack and was presented with a sampling of the confidential and private information Bathula accessed, captured, and retained from her.

111. Jane Doe 5 learned that Bathula had accessed the photos stored in her google drive, viewed them, and retained the following:

a) Private photos taken in the privacy of her home wearing bikinis;

b) Private, intimate photos taken of her in the nude; and

c) PII, including her license and passport.

112. Neither the photographs nor most of the PII and other information were publicly available. Jane Doe 5 considers these photographs and this information private and deeply personal.

113. Jane Doe 5 did not consent to Bathula's invasion.

JANE DOE 6's FACTUAL ALLEGATIONS

114. Jane Doe 6 adopts and incorporates by reference all allegations contained in the paragraphs 1 through 62 as if fully set forth herein.

115. At all material times hereto, Jane Doe 6 was a University of Maryland student and then an employee who worked at the Medical Center.

116. Jane Doe 6 had a reasonable expectation of privacy in her personal accounts.

117. Jane Doe 6 used Medical Center computer stations during the course and scope of her work as a student and as an employee in the Medical Center on a regular and routine basis.

118. As part of her employment, she was specifically required to access documents using google drive. Because the Medical Center email domain was not Gmail, Jane Doe 6 was required to use her personal Gmail account to access google drive and, therefore, had to log into her personal Gmail account on Medical Center computers. Upon information and belief, many other students, residents and employees of the Medical Center were required to do the same.

119. At some point between November, 2024, and February, 2025, Jane Doe 6 received an unsettling phone call from the FBI requesting a meeting.

120. During that meeting, Jane Doe 6 was informed that she was a victim of Bathula's cyber-voyeurism attack and was presented with a sampling of the confidential and private information Bathula accessed, captured, and retained from her.

121. Jane Doe 6 learned that Bathula had accessed the photos stored in her google drive, viewed them, and retained the following:

a) Partially-nude and sexually-suggestive photos of Jane Doe 6 taken in the privacy her home when she was a minor, under the age of 18;

b) PII, including her license and passport; and

c) All banking information and account usernames and passwords stored in her google chain.

122. Neither the photographs nor most of the PII and other information were publicly available. Jane Doe 6 considers these photographs and this information private and deeply personal.

123. Jane Doe 6 did not consent to Bathula's invasion.

CLASS ACTION ALLEGATIONS

124. Plaintiffs adopt and incorporate by reference all allegations contained in the paragraphs above as if fully set forth herein.

125. Plaintiffs brings this action on behalf of themselves and all others similarly situated, as a class action pursuant to Maryland Rule 2-231.

126. **Class Definition:** The putative class Plaintiffs seek to represent (the "Class") is defined as follows:

> All current and former Medical Center employees whose private personal data was accessed and/or whose privacy was otherwise invaded as a result of Matthew Bathula's unauthorized remote access of Defendants' desktop computers, laptops, web-cams or other electronic devices.

127. Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveals that the Class should be expanded or otherwise modified, including, but not limited to, to include Medical Center patients. Plaintiffs also reserve the right to establish a sub-class as appropriate.

128. This action is brought and properly maintained as a class action pursuant to Maryland Rules 2-231(b) and (c) because the prerequisites are satisfied and the class is maintainable. The term "Class Members" refer to the members of the putative class.

129. **Numerosity:** While the exact number of Class Members is unknown to Plaintiffs at this time and can only be determined by appropriate discovery, membership in the Class is ascertainable based upon records maintained by the Defendants, Class Members, and law enforcement. Notice can be provided to Class Members through direct mailing, publication, or otherwise using techniques and a form of notice like those customarily used in comparable matters. At this time, Plaintiff believes that the Class includes approximately 80 similarly situated members. Therefore, the Class is sufficiently numerous that joinder of all Class Members in a

single action is impracticable and resolution of their claims through the procedure of a class action will be of benefit to the parties and the Court.

130. **Commonality:** this case presents common questions of law and fact that predominate over any question affecting any one individual. The predominating questions include, but are not limited to:

a) Whether Matthew Bathula, PharmD, was a duly authorized agent and/or employee of Defendants at all relevant times.

b) Whether Matthew Bathula, PharmD, installed hardware keyloggers or keystroke loggers onto Medical Center computers and devices which enabled him to obtain Class Members' usernames and passwords for their personal accounts during work hours and during the course and scope of his employment.

c) Whether Matthew Bathula, PharmD, viewed, captured, recorded, and/or retained videos, photographs, and PII for Class Members without their authorization or consent, including photographs and recordings of Class Members engaging in private sexual activities or in various stages of undress, and/or invaded the privacy of the Class Members.

d) Whether Matthew Bathula, PharmD, reproduced, distributed, and/or sold Class Members' videos, photographs, and PII on the internet.

e) Whether Defendants were on notice of vulnerabilities within their computer system which allowed Bathula to compromise the system on such a large magnitude for such a time.

f) Whether Defendants knew or should have known of the vulnerabilities within Defendants' computer system which allowed Bathula to compromise the system on such a large magnitude for such a long period.

g) Whether Defendants failed to implement reasonable safeguards that would have prevented Bathula from remotely accessing its computers and electronic devices.

h) Whether Defendants had actual knowledge of Bathula's crimes prior to October 1, but failed to disclose the same to Class Members, allowing Bathula to continue his criminal voyeurism.

i) Whether Defendants' actions and/or failures to act directly and proximately resulted in injuries, damage, and harm to the Class Members.

131. **Typicality:** Plaintiffs' claims are typical of other members of the Class because Plaintiffs and the Class Members sustained damages arising out of Defendants' uniform wrongful conduct.

132. **Adequate Representation:** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs are adequate representatives of the Class because Plaintiffs have no interests adverse to the interests of the other Class Members. Plaintiffs are committed to the vigorous prosecution of this action and, to that end, Plaintiffs have retained counsel who are competent and experienced in handling complex litigation, including class action litigation, on behalf of similar plaintiffs. Plaintiffs have no interest antagonistic to those of the Class and Defendant has no defenses unique to any individual Plaintiff.

133. **Predominance and Superiority:** A class action is superior to all other available methods of the fair and efficient adjudication of the claims asserted in this action because:

a) the expense and burden of individual litigation make it economically unfeasible for Class Members to seek redress of their claims other than through the procedure of a class action;

b) Class Members may be too humiliated or isolated to seek individual redress of their claims in a public forum for fear of public embarrassment, workplace retaliation, and/or retaliation from Bathula, and a class action procedure allows redress without participation in extended and traumatizing litigation;

c) Class Members may suffer from severe mental health issues related to the invasion of privacy they experienced due to Defendants' failures and do not have the physical ability to withstand a deposition or trial to seek redress of their claims;

d) Plaintiffs are unaware of any other actions seeking the same relief that is sought through the class action procedure; and

e) concentrating the claims against Defendants would grant Defendants finality in litigation as well as guidance through injunctive orders.

134. This action is properly maintained as a class action under Rule 2-231(c)(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 class members as well as the Defendants.

135. This action is properly maintainable as a class action pursuant to Rule 2-231(c)(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 the other members not a party to the adjudications, or would substantially impair or impede their ability to protect themselves.

136. The requirement set forth in Rule 2-231(c)(2) is satisfied because Defendants' actions and omissions are the same for the Class Members and Plaintiffs.

137. This action is properly maintainable under Rule 2-231(c)(3) in that questions of law or fact common to Class Members predominate over any questions affecting only individual members, no other litigation has already been commenced, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy between the class and Defendants.

COUNT I
Negligence
(On Behalf of Jane Does 1-6 and the Class)

138. Plaintiffs restate and reallege by reference the foregoing paragraphs as though fully set forth herein.

139. Defendants, including their authorized agents and/or employees, owed to Plaintiffs and Class Members the duty to exercise the degree, care, skill, and judgment expected of a large medical corporation acting in the same or similar circumstances, which duty included ensuring that Medical Center computer systems were secure, safe to use, and inviolable by unauthorized parties. This common law duty of care is non-delegable and known or by the exercise of due care should be known to all health care providers, including Defendants.

140. Defendants, including their authorized agents and/or employees, owed to Plaintiffs and Class Members the duty to exercise reasonable care, skill, and judgment expected of a large medical corporation acting in the same or similar circumstances, which duty included the duty to use reasonable care to investigate, credential monitor and supervise its medical personal, including Bathula, and to discover, stop, and report any professional misconduct of which they knew or should have known was occurring or had occurred. This common law duty and standard of care is

non-delegable and known or by the exercise of due care should be known to all health care providers, including the Defendants herein.

141. Defendants knew or should have known that their computer system was unsecure and vulnerable to attack, like the attack described in this Class Action Complaint.

142. Defendants also knew or should have known that their exam-room cameras were compromised and able to accessed remotely.

143. Defendants knew or should have known that Bathula engaged in improper, unlawful and unprofessional conduct by accessing Plaintiffs' and Class Members' usernames and passwords and using those usernames and passwords to compromise the privacy of every aspect of Plaintiffs' and Class Members' personal and professional lives.

144. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures, including those described herein. Defendants knew or should have known of the inherent risks in allowing users to access their shared computers and webcams without adequate security protocols and safeguards.

145. Defendants, by and through their agents, employees, and independent contractors, breached these duties of care and were negligent in their acts and/or omissions by the following:

a) failing to ensure that reasonable and proper protocols and safeguards were in place so that employee and patient data and personal accounts could not be stolen and/or compromised;

b) failing to ensure that reasonable and proper protocols and safeguards were in place so that cameras within the Medical Center could not be accessed remotely;

c) failing to prevent keyloggers from being downloaded and/or installed on Medical Center computers, including by allowing users to plug thumb drives into the computers and download their contents;

d) failing to prevent keyloggers from being downloaded and/or installed on employee-issued laptops, including by allowing users to plug thumb drives into the computers and download their contents;

e) failing to detect keyloggers that Bathula had downloaded and/or installed on Medical Center computers, including by failing to employ reasonably available anti-virus detectors;

f) failing to detect keyloggers that Bathula had downloaded and/or installed on employee-issued laptops, including by failing to employ reasonably available anti-virus detectors;

g) failing to provide reasonable and adequate instruction and/or supervision to employees, agents, representatives, servants and/or IT personnel in connection with the security of the Medical Center's computer and camera system.

h) failing to take additional security measures after being put on notice by prior instances of data breaches and cyberattacks that security measures were inadequate;

i) failing to reasonably and effectively utilize and monitor existing security devices in place to detect cyberattacks;

j) failing to warn, protect, guard, and secure Plaintiffs' and Class Members' usage of the Medical Center computer systems and cameras, when the Defendants knew or

should have known of the foreseeability of cyberattacks and the danger to Plaintiffs' and Class Members' private and confidential login information;

k) failing to implement adequate security policies, security measures, and security proceedings necessary to protect Plaintiffs and Class Members from cyber and voyeurism attacks, like the cyber and voyeurism attack which forms the basis for this Class Action Complaint;

l) failing to implement adequate IT security policies, security measures, and security proceedings necessary to protect Plaintiffs and Class Members;

m) failing to guard, deter, and otherwise provide adequate protection for Plaintiffs and Class Members from cyber and voyeurism attacks, when Defendant knew or should have known of the foreseeable criminal acts committed Bathula;

n) failing to discover, stop, and report Bathula;

o) failing to notify Plaintiffs and Class Members of Bathula's invasion of their privacy;

p) failing to follow industry standard data security practices including:

    i. Restricting user permissions such that no user can install hardware/software other than an administrator;

    ii. Disabling USB, USBc and other computer ports to prevent users from inserting Keystroking and other devices into company computers;

    iii. Installing USB data blockers to prevent unauthorized hardware devices from transmitting data;

    iv. Conducting regular hardware inspections;

    v. Installing Keystroke Encryption Software;

vi. Installing and updating robust firewalls to monitor and control network traffic and to prevent keyloggers from transmitting captured data to external servers;

vii. Training users in how to recognize suspicious cyber activity;

viii. Requiring users to use password managers and multi-factor authentication;

ix. Using behavioral biometrics to detect anomalies that may indicate keylogger activity;

x. Restricting employee badge access to areas relating to the employee's job function;

xi. Implementing zero trust security models where no user or device is trusted by default, must be verified to be granted access to systems; and

xii. Conducting regular security audits of all IT systems.

146. Beyond ordinary negligence, Defendants were grossly negligent because the acts or omissions of Defendants and their employees and agents were more than momentary thoughtlessness or inadvertence. Rather, the conduct, when viewed objectively from the standpoints of Defendants at the time of these events, involved an extreme degree of risk, considering the probability and magnitude of the potential harm to Plaintiffs and Class Members.

147. Moreover, Defendants had subjective knowledge of the risk of employees gaining unauthorized access to the Medical Center's computer stations and camera systems, but failed to disclose to Plaintiffs and Class Members the vulnerability of the Medical Center's computer and camera system and the ability of any employee to easily and frequently install malware to track Plaintiffs' and Class Members' every keystroke and surveille Plaintiffs and Class Members, and acted with conscious indifference to the rights, safety, and welfare of the same.

148. Defendants' ongoing breaches of the common law and violations of the standards of care proximately caused Plaintiffs and Class Members emotional anguish, fear, anxiety, humiliation, embarrassment, and the physical manifestations of those injuries and other harms and losses set forth in Plaintiffs' prayer for relief below.

COUNT II
Negligent Supervision and Retention
(On Behalf of Jane Does 1-6 and the Class)

149. Plaintiffs restate and reallege by reference the foregoing paragraphs as though fully set forth herein.

150. Between 2015 and 2024, Bathula was a duly authorized agent and/or employee of Defendants, holding a Clinical Pharmacy Specialist position.

151. Between 2015 and 2024, Defendants were responsible to assure and maintain employee and patient safety and privacy for the employee and patient data housed in its computer system and for the employees and patients using Frenkil Building examination rooms.

152. Between 2015 and 2024, Defendants had a duty to under applicable standards of medical practice and common law to properly investigate, credential, qualify, select, monitor, supervise, and retain only competent healthcare professionals, including pharmacists in accordance with the standard of care.

153. Between 2015 and 2024, Defendants had a duty under applicable standards of medical practice and common law to promulgate proper and effective standards, procedures, systems, and rules to ensure quality care, safety and privacy of their patients.

154. Defendants breached the applicable standards of medical practice and common law duties on a continuing and routine basis by, among other things:

a) failing to properly investigate Bathula during his employment and/or association with Defendants;

b) failing to properly investigate reports of misconduct;

c) failing to properly investigate breaches of Defendants' computer system, including the Medical Center's computer system;

d) failing to properly investigate breaches to the Frenkil Building's webcams;

e) failing to properly investigate Bathula's whereabouts in various locations throughout the Medical Center where he did not have patients;

f) failing to appropriately credential, qualify, select, investigate, monitor and supervise Bathula; and

g) continuing Bathula's privileges and employment when they knew or should have known that he engaged in wrongful, unlawful and outrageous conduct, including, but not limited to, the theft of Plaintiffs' and Class Members' usernames and passwords, the theft of Plaintiffs' and Class Members' PII, the theft of Plaintiffs' and Class Members' private photographs and recordings, and the videotaping and/or photography of Plaintiffs and Class Members, without authorization or consent, in addition to other privacy invasions.

155. Defendants' continuing breaches of the applicable standards of medical practice and their common law duties constituted negligence, gross negligence, carelessness, recklessness, and wanton misconduct.

156. Defendants' ongoing breaches of the common law and violations of the standards of care proximately caused Plaintiffs and Class Members emotional anguish, fear, anxiety, humiliation, embarrassment, and the physical manifestations of those injuries.

COUNT III
Negligent Security
(On Behalf of Jane Does 1-6 and the Class)

157. Plaintiffs restate and reallege by reference the foregoing paragraphs as though fully set forth herein.

158. At all relevant times, Defendants owned, controlled, maintained and/or were responsible for the supervision, control, security, safeguarding, and/or oversight the Medical Center, including the Medical Center computer system and the Frenkil Building.

159. Defendants owed a duty to all individuals working within the Medical Center, including Plaintiffs and Class Members, to exercise reasonable and ordinary care to keep and maintain Medical Center computer system and its cameras in a condition reasonably safe for employee use.

160. In particular, Defendants had a duty to take such precautions as were reasonably necessary to protect their employees and workers, including Plaintiffs and Class Members, from criminal attacks, including cyber and voyeurism attacks, which were reasonably foreseeable.

161. Defendants knew, or in the exercise of reasonable care, should have known, that the Medical Center computer system and cameras were vulnerable to attack, including via malware and data breaches, and that cyber-criminal acts and attacks were reasonably likely to be perpetrated on Defendants' systems, unless Defendants took steps to provide proper security and usage protocols for the same.

162. Defendants knew, or in the exercise of reasonable care should have known, that no individual, including Plaintiff and Class Members, had within their own power to take the measures necessary to provide for their own safety and security with respect to their usage of Defendants' computer system, which they were required to use as part of their daily jobs.

163. Defendants' failure to implement reasonable and necessary security measures was negligent, careless, reckless, intentional, willful, wanton, and outrageous given pervasive cyber-attacks being committed on institutional systems, including health systems, on a routine and regular basis and given the notice Defendants had of a breach or potential breach of the Medical Center computer systems.

164. Defendants breached their duty of reasonable care for the safety and protection of the public and Plaintiffs and the Class Members in all or more of the following ways:

a) failing to ensure that reasonable and proper protocols and safeguards were in place so that employee and patient data and personal accounts could not be stolen and/or compromised;

b) failing to ensure that reasonable and proper protocols and safeguards were in place so that cameras within the Medical Center could not be accessed remotely;

c) failing to prevent keyloggers from being downloaded and/or installed on Medical Center computers, including by allowing users to plug thumb drives into the computers and download their contents;

d) failing to prevent keyloggers from being downloaded and/or installed on employee-issued laptops, including by allowing users to plug thumb drives into the computers and download their contents;

e) failing to detect keyloggers that Bathula had downloaded and/or installed on Medical Center computers, including by failing to employ reasonably available anti-virus detectors;

f) failing to detect keyloggers that Bathula had downloaded and/or installed on employee-issued laptops, including by failing to employ reasonably available anti-virus detectors;

g) failing to provide reasonable and adequate instruction and/or supervision to employees, agents, representatives, servants and/or IT personnel in connection with the security of the Medical Center's computer and camera system.

h) failing to take additional security measures after being put on notice by prior instances of data breaches and cyberattacks that security measures were inadequate;

i) failing to reasonably and effectively utilize and monitor existing security devices in place to detect cyberattacks;

j) failing to warn, protect, guard, and secure Plaintiff's and Class Members' usage of the Medical Center computer systems and cameras, when the Defendants knew or should have known of the foreseeability of cyberattacks and the danger to Plaintiff's and Class Members' private and confidential login information;

k) failing to implement adequate security policies, security measures, and security proceedings necessary to protect Plaintiff and Class Members from cyber and voyeurism attacks, like the cyber and voyeurism attack which forms the basis for this Class Action Complaint;

l) failing to implement adequate IT security policies, security measures, and security proceedings necessary to protect Plaintiff and Class Members;

m) failing to guard, deter, and otherwise provide adequate protection for Plaintiff and Class Members from cyber and voyeurism attacks, when Defendant knew or should have known of the foreseeable criminal acts committed Bathula;

n) failing to discover, stop, and report Bathula;

o) failing to notify Plaintiff and Class Members of Bathula's invasion of their privacy; and

p) failing to follow industry standard data security practices including:

    i. Restricting user permissions such that no user can install hardware/software other than an administrator;

    ii. Disabling USB, USBc and other computer ports to prevent users from inserting Keystroking and other devices into company computers;

    iii. Installing USB data blockers to prevent unauthorized hardware devices from transmitting data;

    iv. Conducting regular hardware inspections;

    v. Installing Keystroke Encryption Software;

    vi. Installing and updating robust firewalls to monitor and control network traffic and to prevent keyloggers from transmitting captured data to external servers;

    vii. Training users in how to recognize suspicious cyber activity;

    viii. Requiring users to use password managers and multi-factor authentication;

    ix. Using behavioral biometrics to detect anomalies that may indicate keylogger activity;

x. Restricting employee badge access to areas relating to the employee's job function;

xi. Implementing zero trust security models where no user or device is trusted by default, must be verified to be granted access to systems; and

xii. Conducting regular security audits of all IT systems.

165. Defendants' ongoing breaches of the common law and violations of the standards of care proximately caused Plaintiffs and Class Members emotional anguish, fear, anxiety, humiliation, embarrassment, and the physical manifestations of those injuries.

COUNT IV
Intrusion Upon Plaintiffs' Seclusion – Invasion of Privacy
(On Behalf of Jane Does 1-6 and the Class)

166. Plaintiffs restate and reallege by reference the foregoing paragraphs as though fully set forth herein.

167. Plaintiffs allege that Bathula maliciously and intentionally intruded upon Plaintiffs' and Class Members' solitude, seclusion, or private affairs and concerns by committing the following crimes without Plaintiffs' or Class Members' knowledge or consent:

a) surreptitiously obtaining Plaintiffs' and Class Members' usernames and passwords and using those usernames and passwords to access and breach Plaintiffs' and Class Members' personal accounts.

b) surreptitiously accessing Plaintiffs' and Class Members' personal accounts and viewin, retaining, and potentially republishing Plaintiffs' and Class Members' private emails, conversations, text messages, photographs, and videos, including nude photographs or photographs showing Plaintiffs' and Class Members' in stages of undress, including photographs of minors;

c) surreptitiously accessing, retaining, and potentially republishing Plaintiffs' and Class Members' PII without Plaintiffs' and Class Members' knowledge or consent;

d) surreptitiously accessing Plaintiffs' and Class Members' home surveillance systems and watching and recording Plaintiffs and Class Members in the sanctity of their private homes; and

e) surreptitiously accessing the cameras located in Medical Center exam rooms and surveilling, watching, and recording Medical Center employees and Class Members and potentially patients, including watching and recording Medical Center employees and Class Members in various stages of undress and while pumping breastmilk.

168. These systemic and repeated intrusions are highly offensive to a reasonable person, such as Plaintiffs and Class Members, and were totally unwarranted and unjustified, constituting invasion of privacy.

169. Defendants' ongoing breaches of the common law and violations of the standards of care which allowed Bathula to commit the invasions of privacy detailed herein proximately caused Plaintiffs and Class Members emotional anguish, fear, anxiety, humiliation, embarrassment, and the physical manifestations of those injuries and other harms and losses.

PRAYER FOR RELIEF

WHEREFORE, Jane Does 1-6, individually and on behalf of the Class of similarly situated individuals, pray for the following relief:

a) Certifying this case as a class action on behalf of the Class defined above, appointing Jane Does 1-6 as representatives of the Class, and appointing their counsel as class counsel;

b) Declaring that Defendants' actions, as set out above, constitute negligence and intrusion upon seclusion;

c) Awarding damages, including compensatory, exemplary, and punitive damages (pursuant to Maryland Rule 2-305, Plaintiffs state that the damages sought exceed $75,000);

d) Awarding Jane Does 1-6 and the Class their reasonable litigation expenses and attorneys' fees;

e) Awarding Jane Does 1-6 and the Class pre- and post-judgement interest, to the extent available;

f) Awarding such other injunctive and declaratory relief as is necessary to protect the interests of Jane Does 1-6 and the Class; and

g) Awarding such other and further relief as the Court deems reasonable and just.

DEMAND FOR JURY TRIAL

Plaintiffs hereby respectfully demand a trial by jury of all issues so triable pursuant to Maryland Rule 2-325(a).

Respectfully submitted,

JANE DOES 1-6, individually and on behalf of all similarly situated,

By: ***/s/ Steven J. Kelly***
Steven J. Kelly

GRANT & EISENHOFER P.A.
Steven J. Kelly (CPF 0312160392)
3600 Clipper Mill Road, Suite 240
Baltimore, Maryland 21211
Phone: (443) 531-1474
skelly@gelaw.com

M. Elizabeth Graham (pro hac vice forthcoming)
Cynthia B. Morgan (pro hac vice forthcoming
123 S. Justison Street

Wilmington, DE 19801
Phone: (415) 229-9720
egraham@gelaw.com
cmorgan@gelaw.com

Counsel for Plaintiffs