E-FILED 2026 APR 15 12:52 PM JOHNSON - CLERK OF DISTRICT COURT

IN THE IOWA DISTRICT COURT FOR JOHNSON COUNTY

THOMAS GRANT, TINA BEERBOWER, AMANEE CLARK, AIRIKA KOTASKA, CLAIRE MOSELEY, JACK MOSELEY, ANNE WISER, TIMOTHY MALONEY, ROGER BRADLEY, JULIE PAULSEN, KRISTINA BENNETT and MICHAEL MARCUS, individually and on behalf of all others similarly situated, *Plaintiffs,* v. UNIVERSITY OF IOWA COMMUNITY MEDICAL SERVICES, LLC d/b/a UI COMMUNITY HOMECARE, *Defendant.*	**Case No. CVCV086807** **AMENDED CLASS ACTION PETITION AND JURY DEMAND**

Plaintiffs Thomas Grant, Tina Beerbower, Amanee Clark, Airika Kotaska, Claire Moseley, Jack Moseley, Anne Wiser, Timothy Maloney, Roger Bradley, Julie Paulsen, Kristina Bennett and Michael Marcus, individually and on behalf of a class of similarly situated persons, bring this Class Action Petition and allege the following against Defendant University of Iowa Community Medical Services, LLC d/b/a UI Community HomeCare ("UI HomeCare"), based upon personal knowledge with respect to Plaintiffs and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. Plaintiffs bring this class action against UI HomeCare for its failure to properly secure Plaintiffs' and Class Members' personally identifiable information ("PII") and personal

health information ("PHI"). The PII and PHI may have included victims' dates of birth, addresses, phone numbers, medical record numbers, providers, dates of service, health insurance information, and Social Security numbers.

2. UI HomeCare failed to comply with industry standards to protect information systems that contain PII and PHI. Plaintiffs seek, among other things, orders requiring UI HomeCare to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the disclosure (the "Data Breach") in the future.

3. UI HomeCare has disclosed that "[o]n July 3, 2025, UI Community HomeCare had someone access our computer system without our permission." UI HomeCare further disclosed that "a cybercriminal was able to see and take copies of data in our computer system, which included some data files containing information for UI Community HomeCare customers and others."

4. UI HomeCare concurrently disclosed that the PII and/or PHI of approximately 211,000 individuals was exposed by the Data Breach. UI HomeCare sent out notice letters ("Notice Letters") to some portion of those people, including Plaintiffs, on or around August 29, 2025.

5. As a health care provider, UI HomeCare knowingly obtained sensitive PII and PHI and had a resulting duty to securely maintain that information in confidence. Plaintiffs and Class Members would not have provided their PII and PHI to UI HomeCare if they had known that UI HomeCare would not ensure that it used adequate security measures.

6. Plaintiffs seek to remedy these harms individually and on behalf of all other similarly situated individuals whose PII and/or PHI were exposed in the Data Breach. Plaintiffs

seek remedies including compensation for time spent responding to the Data Breach and other types of harm, free credit monitoring and identity theft insurance, and injunctive relief including substantial improvements to UI HomeCare's data security policies and practices.

PARTIES

7. Plaintiff Thomas Grant is a resident of Dubuque County, Iowa and a patient of UI HomeCare. Mr. Grant received a Notice Letter from UI HomeCare on or around August 29, 2025.

8. Plaintiff Tina Beerbower is a resident of Pleasant Hill, Iowa, and a patient of UI HomeCare. Ms. Beerbower received a Notice Letter from UI HomeCare on or around August 29, 2025.

9. Plaintiff Amanee Clark is a resident of Waterloo, Iowa, and a patient of UI HomeCare. Ms. Clark received a Notice Letter from UI HomeCare on or around August 29, 2025.

10. Plaintiff Airika Kotaska is a resident of Cedar Rapids, Iowa, and a patient of UI HomeCare. Ms. Kotaska received a Notice Letter from UI HomeCare on or around August 29, 2025.

11. Plaintiff Claire Moseley is a resident of Iowa City, Iowa, and a patient of UI HomeCare. Ms. Moseley received a Notice Letter from UI HomeCare on or around August 29, 2025.

12. Plaintiff Jack Moseley is a resident of Iowa City, Iowa, and a patient of UI HomeCare. Mr. Moseley received a Notice Letter from UI HomeCare on or around August 29, 2025.

13. Plaintiff Anne Wiser is a resident of Iowa City, Iowa, and a patient of UI HomeCare. Ms. Wiser received a Notice Letter from UI HomeCare on or around August 29, 2025.

14. Plaintiff Timothy Maloney is a resident of Marengo, Iowa. Mr. Maloney received a Notice Letter from UI HomeCare on or around August 29, 2025.

15. Plaintiff Roger Bradley is a resident of Iowa, and a patient of UI HomeCare. Mr. Bradley received a Notice Letter from UI HomeCare on or around August 29, 2025.

16. Plaintiff Julie Paulsen is a resident of Clarence, Iowa, and a patient of UI HomeCare. Ms. Paulsen received a Notice Letter from UI HomeCare on or around August 29, 2025.

17. Plaintiff Kristina Bennett is a resident of North Liberty, Iowa, and a patient of UI HomeCare. Ms. Bennett received a Notice Letter from UI HomeCare on or around August 29, 2025.

18. Plaintiff Michael Marcus is a resident of Iowa City, Iowa, and a patient of UI HomeCare. Mr. Marcus received a Notice Letter from UI HomeCare on or around August 29, 2025.

19. Defendant University of Iowa Community Medical Services, LLC d/b/a UI Community HomeCare is an Iowa limited liability corporation, with its principal place of business in Iowa City, Iowa.

FACTUAL ALLEGATIONS

The Data Breach

20. UI HomeCare describes itself as "a full-service home infusion and medical equipment services provider" and claims to offer "[e]xceptional services and quality healthcare through compassionate experiences."[1]

21. Due to the nature of the services it provides, UI HomeCare acquires and electronically stores PII and PHI. UI HomeCare was therefore required to ensure that PII and PHI were not disclosed or disseminated to unauthorized third parties without Plaintiffs' and Class Members' express written consent.

22. On or around August 29, 2025, UI HomeCare disclosed on its website that "[o]n July 3, 2025, UI Community HomeCare had someone access our computer system without our permission."[2]

23. That disclosure further reflected that "[t]he data that may have been seen and taken … may have included name, date of birth, address, phone number, medical record number, provider, dates of service, health insurance information, Social Security number, and type of visit."[3]

24. UI HomeCare's disclosures are otherwise deficient. They do not include basic details concerning the Data Breach, including, but not limited to, why PII and PHI were stored on systems without adequate security, the deficiencies in the security systems that permitted

[1] https://www.uicommunityhomecare.org/ (last visited Mar. 31, 2026).

[2] https://www.uicommunityhomecare.org/information-on-ui-community-homecare-data-privacy-event/ (last visited Mar. 31, 2026).

[3] *Id*.

unauthorized access, whether the data was encrypted or otherwise protected, and what UI HomeCare knows about the degree to which the data has been disseminated.

25. UI HomeCare has not disclosed nearly all the details of the Data Breach and its investigation. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, UI HomeCare has taken to secure the PII and PHI still in its possession. Plaintiffs seek to determine the scope of the Data Breach and the information involved, obtain relief that redresses the harm to Plaintiffs' and Class Members' interests, and ensure that UI HomeCare has proper measures in place to prevent similar incidents from occurring in the future.

UI HomeCare's Security Representations

26. As of August 9, 2025, UI HomeCare's website included several links to its "HIPAA Notice of Privacy Practices."[4] Those links are no longer on the website.[5]

27. The HIPAA Notice nevertheless remains available by other means on UI HomeCare's website.[6] That Notice provides that UI HomeCare is "legally required to protect the privacy of your health information," and includes a long list of "Uses and Disclosures of Protected Health Information Without Your Authorization."[7] Nothing in that list allows UI HomeCare to disclose patient information to cybercriminals.

[4] *See, e.g.,* https://web.archive.org/web/20250809025018/https://www.uicommunityhomecare.org (last visited Mar. 31, 2026).

[5] *See* https://www.uicommunityhomecare.org (last visited Mar. 31, 2026).

[6] *See* https://www.uicommunityhomecare.org/wp-content/uploads/2024/08/Notice-of-Privacy-Practices-UI-Community-Home-Care2-2.docx (last visited Mar. 31, 2026).

[7] *Id.*

The Healthcare Sector is a Primary Target for Data Breaches

28. UI HomeCare's negligence in safeguarding Representative Plaintiffs' and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

29. The healthcare industry has experienced many high-profile cyberattacks in the last several years preceding this Petition's filing. Cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[8] According to the HIPAA Journal, the largest healthcare data breaches were reported in April 2021.[9]

30. For example, Universal Health Services experienced a cyberattack on September 29, 2020 similar to the attack on UI HomeCare. As a result of this attack, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[10] Similarly, in 2021, Scripps Health suffered a cyberattack, which effectively shut down critical healthcare services for a month and left numerous patients unable to speak to their physicians or access vital medical and prescription records.[11] University of San Diego Health suffered a similar attack a few months later.[12]

---

[8] https://www.hipaajournal.com/2020-healthcare-data-breach-report/ (last visited Mar. 31, 2026).

[9] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last visited Mar. 31, 2026).

[10] https://www.prnewswire.com/news-releases/universal-health-services-inc-reports-2020-fourth-quarter-and-full-year-financial-results-and-2021-full-year-earnings-guidance-301236075.html/ (last visited Mar. 31, 2026).

[11] https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (last visited Mar. 31, 2026).

[12] https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/ (last visited Mar. 31, 2026).

31. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[13]

32. The HIPAA Journal article explains that patient records, like those stolen from UI HomeCare, are "often processed and packaged with other illegally obtained data to create full record sets (full) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals, which "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[14]

33. Data breaches such as the one experienced by UI HomeCare have become so notorious that the Federal Bureau of Investigation ("FBI") and the U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully ward off a potential attack.

34. Due to the high-profile nature of these breaches and other breaches of its kind, UI HomeCare was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

---

[13] *Editorial: Why Do Criminals Target Medical Records,* HIPAA J. (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/

[14] *Id.*

35. And yet, despite the prevalence of public announcements of data breaches and data security compromises, UI HomeCare failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PHI/PII from being compromised.

UI HomeCare Had a Duty to Protect the Stolen Information

36. In failing to adequately secure Representative Plaintiffs' and Class Members' sensitive data, UI HomeCare breached duties it owed Plaintiffs and Class Members under statutory and common law. Under HIPAA, health insurance providers and business associates have an affirmative duty to keep patients' protected health information private. As a covered entity, UI HomeCare has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' data. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data to UI HomeCare under the implied condition that UI HomeCare would keep it private and secure. Accordingly, UI HomeCare also had an implied duty to safeguard their data, independent of any statute.

37. Because UI HomeCare is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

38. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for protecting health information.

39. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

40. HIPAA requires UI HomeCare to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

41. "Electronic protected health information" is "individually identifiable health information […] that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

42. HIPAA's Security Rule requires UI HomeCare to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
1.
b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.
2.

43. HIPAA also requires UI HomeCare to "review and modify the security measures implemented […] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

44. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires UI HomeCare to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

45. UI HomeCare was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure

to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

46. According to the FTC, the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as UI HomeCare, should employ to protect against the unlawful exposure of PHI/PII.

47. 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. The guidelines explain that companies should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of PHI/PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

48. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

49. The FTC recommends that companies not maintain information longer than is necessary for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network and verify that third-party service providers have implemented reasonable security measures.

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

51. UI HomeCare's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PHI/PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

52. In addition to its obligations under federal and state laws, UI HomeCare owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in UI HomeCare's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. UI HomeCare owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' PHI/PII.

53. UI HomeCare owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that all PHI/PII in its possession was adequately secured and protected.

54. UI HomeCare owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all PHI/PII in its possession, including not sharing information with other entities who maintain sub-standard data security systems.

55. UI HomeCare owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

56. UI HomeCare owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

57. UI HomeCare owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft, because such an inadequacy would be a material fact in the decision to entrust this PHI/PII to UI HomeCare.

58. UI HomeCare owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

59. UI HomeCare owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity to identify possible threats.

The Sensitive Information Stolen in the Data Breach is Highly Valuable

60. It is well known that PHI/PII, including Social Security numbers and health records in particular, is a valuable commodity and a frequent, intentional target of cybercriminals. Companies that collect such information, including UI HomeCare, are well aware of the risk of being targeted by cybercriminals.

61. Individuals place a high value not only on their PHI/PII but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight the impact of identity theft.

62. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records

contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

63. The high value of PHI/PII to criminals is evidenced by the prices they will pay for it through the dark web. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[16] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[17]

64. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[18] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[19] In short, these sorts of data breaches are

[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Mar. 31, 2026).

[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 31, 2026).

[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Mar. 31, 2026).

[18] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last visited Mar. 31, 2026).

[19] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last visited Mar. 31, 2026).

increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[20]

65. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in Oklahoma. Such fraud will be an omnipresent threat for Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

66. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

67. Identity thieves can use PHI/PII, such as that of Plaintiffs and Class Members which UI HomeCare failed to keep secure, to perpetrate various crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

[20] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/ (last visited Mar. 31, 2026).

68. The ramifications of UI HomeCare's failure to secure Representative Plaintiffs' and Class Members' PHI/PII are long-lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PHI/PII of Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who purchase the PHI/PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

69. Individuals, like Plaintiffs and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and are likened to accessing DNA for hackers' purposes.

70. Data breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become victims of Social Security misuse.

71. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other government agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[21]

[21] *Identity Theft and Your Social Security Number*, SSA, No. 05-10064 (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 18, 2023).

72. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

73. The harm to Plaintiffs and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," more than identity thefts involving banking and finance, the government, and the military or education.[23]

74. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[24]

75. When cybercriminals access financial information, health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which UI HomeCare may have exposed Plaintiffs and Class Members.

---

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last visited Mar. 31, 2026).

[23] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited Mar. 31, 2026).

[24] *Id*.

76. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[25] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[26]

77. And data breaches are preventable.[27] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[28] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…."[29]

78. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. Appropriate information security controls, including encryption, must be implemented and enforced rigorously and disciplined so that a *data breach never occurs*.[30]

---

[25] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Mar. 31, 2026).

[26] *Id.*; *see also* Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited Mar. 31, 2026).

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

[28] *Id.* at 17.

[29] *Id.* at 28.

[30] *Id.*

79. Here, UI HomeCare knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Plaintiffs' and Class Members' PHI/PII was stolen, including the significant costs that would be placed on Plaintiffs and Class Members because of a breach of this magnitude. As detailed above, UI HomeCare knew or should have known that the development and use of such protocols was necessary to fulfill its statutory and common law duties to Plaintiffs and Class Members. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

80. Furthermore, UI HomeCare has not offered a subscription for identity theft monitoring and identity theft protection. It is inadequate when the victims will likely face many years of identity theft.

81. Moreover, UI HomeCare's credit monitoring offer and advice to Plaintiffs and Class Members squarely place the burden on Plaintiffs and Class Members, rather than on UI HomeCare, to monitor and report suspicious activities to law enforcement. In other words, UI HomeCare expects Plaintiffs and Class Members to protect themselves from its tortious acts resulting from the Data Breach. Rather than automatically enrolling Plaintiffs and Class Members in credit monitoring services upon discovery of the Data Breach, UI HomeCare merely sent instructions to Plaintiffs and Class Members about actions they could affirmatively take to protect themselves.

82. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PHI/PII.

83. UI HomeCare disregarded the rights of Plaintiffs and Class Members by, *inter alia*: (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequate security protocols and training practices in place to safeguard Plaintiffs' and Class Members' PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

Plaintiff Grant's Experience

84. Plaintiff Grant is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

85. Upon information and belief, UI HomeCare obtained Plaintiff Grant's PII and PHI in the course of conducting its regular business operations.

86. At the time of the Data Breach, UI HomeCare retained Plaintiff Grant's PII and PHI.

87. Plaintiff Grant greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Grant diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

88. UI HomeCare obtained and continues to maintain Plaintiff Grant's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

89. Plaintiff Grant received a letter from UI HomeCare dated August 29, 2025.

90. The Data Breach has caused Plaintiff Grant to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

91. As a result of the Data Breach, Plaintiff Grant is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

92. Plaintiff Grant has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Beerbower's Experience

93. Plaintiff Beerbower is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

94. Upon information and belief, UI HomeCare obtained Plaintiff Beerbower's PII and PHI in the course of conducting its regular business operations.

95. At the time of the Data Breach, UI HomeCare retained Plaintiff Beerbower's PII and PHI.

96. Plaintiff Beerbower greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Beerbower diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

97. UI HomeCare obtained and continues to maintain Plaintiff Beerbower's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

98. Plaintiff Beerbower received a letter from UI HomeCare dated August 29, 2025.

99. The Data Breach has caused Plaintiff Beerbower to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

100. As a result of the Data Breach, Plaintiff Beerbower is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

101. Plaintiff Beerbower has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Clark's Experience

102. Plaintiff Clark is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

103. Upon information and belief, UI HomeCare obtained Plaintiff Clark's PII and PHI in the course of conducting its regular business operations.

104. At the time of the Data Breach, UI HomeCare retained Plaintiff Clark's PII and PHI.

105. Plaintiff Clark greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Clark diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure, and stores any documents containing PII

and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

106. UI HomeCare obtained and continues to maintain Plaintiff Clark's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

107. Plaintiff Clark received a letter from UI HomeCare dated August 29, 2025.

108. The Data Breach has caused Plaintiff Clark to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

109. As a result of the Data Breach, Plaintiff Clark is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

110. Plaintiff Clark has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Kotaska's Experience

111. Plaintiff Kotaska is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

112. Upon information and belief, UI HomeCare obtained Plaintiff Kotaska's PII and PHI in the course of conducting its regular business operations.

113. At the time of the Data Breach, UI HomeCare retained Plaintiff Kotaska's PII and PHI.

114. Plaintiff Kotaska greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Kotaska diligently protects her PII and PHI and takes proactive

steps to ensure her PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

115. UI HomeCare obtained and continues to maintain Plaintiff Kotaska's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

116. Plaintiff Kotaska received a letter from UI HomeCare dated August 29, 2025.

117. The Data Breach has caused Plaintiff Kotaska to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

118. As a result of the Data Breach, Plaintiff Kotaska is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

119. Plaintiff Kotaska has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Claire Moseley's Experience

120. Plaintiff Claire Moseley is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

121. Upon information and belief, UI HomeCare obtained Plaintiff Moseley's PII and PHI in the course of conducting its regular business operations.

122. At the time of the Data Breach, UI HomeCare retained Plaintiff Moseley's PII and PHI.

123. Plaintiff Moseley greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Moseley diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

124. UI HomeCare obtained and continues to maintain Plaintiff Moseley's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

125. Plaintiff Moseley received a letter from UI HomeCare dated August 29, 2025.

126. The Data Breach has caused Plaintiff Moseley to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

127. As a result of the Data Breach, Plaintiff Moseley is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

128. Plaintiff Moseley has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Jack Moseley's Experience

129. Plaintiff Jack Moseley is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

130. Upon information and belief, UI HomeCare obtained Plaintiff Moseley's PII and PHI in the course of conducting its regular business operations.

131. At the time of the Data Breach, UI HomeCare retained Plaintiff Moseley's PII and PHI.

132. Plaintiff Moseley greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Moseley diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

133. UI HomeCare obtained and continues to maintain Plaintiff Moseley's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

134. Plaintiff Moseley received a letter from UI HomeCare dated August 29, 2025.

135. The Data Breach has caused Plaintiff Moseley to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

136. As a result of the Data Breach, Plaintiff Moseley is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

137. Plaintiff Moseley has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Wiser's Experience

138. Plaintiff Wiser is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

139. Upon information and belief, UI HomeCare obtained Plaintiff Wiser's PII and PHI in the course of conducting its regular business operations.

140. At the time of the Data Breach, UI HomeCare retained Plaintiff Wiser's PII and PHI.

141. Plaintiff Wiser greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Wiser diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

142. UI HomeCare obtained and continues to maintain Plaintiff Wiser's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

143. Plaintiff Wiser received a letter from UI HomeCare dated August 29, 2025.

144. The Data Breach has caused Plaintiff Wiser to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

145. As a result of the Data Breach, Plaintiff Wiser is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

146. Plaintiff Wiser has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Maloney's Experience

147. Plaintiff Maloney is or was, at all relevant times, a patient at one or more of UI HomeCare's corporate affiliates.

148. Upon information and belief, UI HomeCare obtained Plaintiff Maloney's PII and PHI in the course of conducting its regular business operations.

149. At the time of the Data Breach, UI HomeCare retained Plaintiff Maloney's PII and PHI.

150. Plaintiff Maloney greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Maloney diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

151. UI HomeCare obtained and continues to maintain Plaintiff Maloney's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

152. Plaintiff Maloney received a letter from UI HomeCare dated August 29, 2025.

153. The Data Breach has caused Plaintiff Maloney to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

154. As a result of the Data Breach, Plaintiff Maloney is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

155. Plaintiff Maloney has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Bradley's Experience

156. Plaintiff Bradley is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

157. Upon information and belief, UI HomeCare obtained Plaintiff Bradley's PII and PHI in the course of conducting its regular business operations.

158. At the time of the Data Breach, UI HomeCare retained Plaintiff Bradley's PII and PHI.

159. Plaintiff Bradley greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Bradley diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

160. UI HomeCare obtained and continues to maintain Plaintiff Bradley's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

161. Plaintiff Bradley received a letter from UI HomeCare dated August 29, 2025.

162. The Data Breach has caused Plaintiff Bradley to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

163. As a result of the Data Breach, Plaintiff Bradley is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

164. Plaintiff Bradley has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Paulsen's Experience

165. Plaintiff Paulsen is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

166. Upon information and belief, UI HomeCare obtained Plaintiff Paulsen's PII and PHI in the course of conducting its regular business operations.

167. At the time of the Data Breach, UI HomeCare retained Plaintiff Paulsen's PII and PHI.

168. Plaintiff Paulsen greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Paulsen diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

169. UI HomeCare obtained and continues to maintain Plaintiff Paulsen's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

170. Plaintiff Paulsen received a letter from UI HomeCare dated August 29, 2025.

171. The Data Breach has caused Plaintiff Paulsen to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

172. As a result of the Data Breach, Plaintiff Paulsen is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

173. Plaintiff Paulsen has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Bennett's Experience

174. Plaintiff Bennett is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

175. Upon information and belief, UI HomeCare obtained Plaintiff Bennett's PII and PHI in the course of conducting its regular business operations.

176. At the time of the Data Breach, UI HomeCare retained Plaintiff Bennett's PII and PHI.

177. Plaintiff Bennett greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Bennett diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

178. UI HomeCare obtained and continues to maintain Plaintiff Bennett's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

179. Plaintiff Bennett received a letter from UI HomeCare dated August 29, 2025.

180. The Data Breach has caused Plaintiff Bennett to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

181. As a result of the Data Breach, Plaintiff Bennett is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

182. Plaintiff Bennett has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

Plaintiff Marcus's Experience

183. Plaintiff Marcus is or was, at all relevant times, a patient at UI HomeCare or one or more of its corporate affiliates.

184. Upon information and belief, UI HomeCare obtained Plaintiff Marcus's PII and PHI in the course of conducting its regular business operations.

185. At the time of the Data Breach, UI HomeCare retained Plaintiff Marcus's PII and PHI.

186. Plaintiff Marcus greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Marcus diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure, and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

187. UI HomeCare obtained and continues to maintain Plaintiff Marcus's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

188. Plaintiff Marcus received a letter from UI HomeCare dated August 29, 2025.

189. The Data Breach has caused Plaintiff Marcus to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

190. As a result of the Data Breach, Plaintiff Marcus is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

191. Plaintiff Marcus has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in UI HomeCare's possession, are protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

192. Plaintiffs bring this action individually and on behalf of the following Class pursuant to Iowa Rules of Civil Procedure 1.261 *et seq*.:

> All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by UI HomeCare on July 3, 2025.

193. Excluded from the Class are UI HomeCare, any entity in which UI HomeCare has a controlling interest, and UI HomeCare's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

194. Plaintiffs reserve the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiffs.

195. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. UI HomeCare has disclosed that the Data Breach affected approximately 211,000 individuals. All Class Members' names and addresses are available from UI HomeCare's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

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

a. Whether and to what extent UI HomeCare had a duty to protect the PII and PHI of Class Members;

b. Whether UI HomeCare was negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI;

c. Whether UI HomeCare had duties not to disclose the PII and PHI of Class Members to unauthorized third parties;

d. Whether UI HomeCare took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII and PHI;

e. Whether UI HomeCare failed to adequately safeguard the PII and PHI of Class Members;

f. Whether UI HomeCare failed to implement and maintain reasonable security policies and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

g. Whether UI HomeCare adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

h. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or punitive damages because of UI HomeCare's wrongful conduct;

i. Whether Plaintiffs and Class Members are entitled to restitution because of UI HomeCare's wrongful conduct;

j. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm they face because of the Data Breach; and

k. Whether Plaintiffs and Class Members are entitled to identity theft protection for their respective lifetimes.

197. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII and PHI, like that of every other Class Member, was disclosed by UI HomeCare. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through UI HomeCare's common misconduct. Plaintiffs are advancing the same claims and legal theories individually and on behalf of all other Class Members, and there are no defenses that are unique to Plaintiffs. Plaintiffs' claims and Class Members' claims arise from the same operative facts and are based on the same legal theories.

198. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against UI HomeCare to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' counsel are competent and experienced in litigating class actions, including extensive experience in data breach litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

199. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because UI HomeCare has acted or refused to act on grounds generally

applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. UI HomeCare's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on UI HomeCare's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

200. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like UI HomeCare. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

201. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because UI HomeCare would necessarily gain an unconscionable advantage in non-class litigation, since UI HomeCare would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of

conduct to which Plaintiffs were exposed is representative of that experienced by Class Members and will establish the right of each Class Member to recover on the causes of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

202. The litigation of Plaintiffs' claims is manageable. UI HomeCare's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with maintenance of this lawsuit as a class action.

203. Adequate notice can be given to Class Members directly using information maintained in UI HomeCare's records.

204. Unless a class-wide injunction is issued, UI HomeCare may continue to maintain inadequate security with respect to the PII and PHI of Class Members, UI HomeCare may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and UI HomeCare may continue to act unlawfully as set forth in this Petition.

205. UI HomeCare has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT I
NEGLIGENCE
(on behalf of Plaintiffs and the Class)

206. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

207. UI HomeCare owes a duty of care to protect the PII and PHI of Plaintiffs and Class Members. UI HomeCare also owes several specific duties including, but not limited to, the duties:

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

b. to protect patients' PII and PHI using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of PII and PHI in its possession;

d. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

e. to promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

208. UI HomeCare also owes these duties because Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 requires UI HomeCare to use reasonable measures to protect confidential data.

209. UI HomeCare also owes these duties because industry standards mandate that UI HomeCare protect its patients' PII and PHI.

210. UI HomeCare also owes these duties because it had a special relationship with Plaintiffs and Class Members. Plaintiffs and Class Members entrusted their PII and PHI to UI HomeCare based on their reasonable understanding that adequate security precautions would be taken to protect their information. Only UI HomeCare had the ability to protect its systems and the PII and PHI stored on them from attack.

211. UI HomeCare also maintains a duty to timely disclose any unauthorized access and/or theft of Plaintiffs' and Class Members' PII and PHI. This duty exists to allow Plaintiffs

and Class Members the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII and PHI.

212. UI HomeCare breached its duties to Plaintiffs and Class Members by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard their PII and PHI.

213. UI HomeCare also breached the duties it owed to Plaintiffs and Class Members by failing to timely and accurately disclose to Plaintiffs and Class Members that their PII and PHI had been improperly acquired and/or accessed.

214. As a direct and proximate result of UI HomeCare's conduct, Plaintiffs and Class Members were damaged. These damages include, and are not limited to:

a. Lost or diminished value of their PII and PHI;

b. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI;

c. Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and

d. Permanent increased risk of identity theft.

215. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of UI HomeCare and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

216. Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial and injunctive relief requiring UI HomeCare to, inter alia, strengthen its data security

systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(on behalf of Plaintiffs and the Class)

217. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

218. Section 5 of the FTCA imposes a duty on UI HomeCare to provide fair and adequate data security to secure, protect, and/or otherwise safeguard Plaintiffs' and Class Members' PII and PHI.

219. HIPAA imposes a duty on UI HomeCare to implement reasonable safeguards to protect Plaintiffs' and Class Members' PII and PHI. 42 U.S.C. § 1302(d), et seq.

220. HIPAA also requires UI HomeCare to render unusable, unreadable, or indecipherable all PII and PHI it collected. UI HomeCare was required to do so through "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." See 45 C.F.R. § 164.304.

221. UI HomeCare violated the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiffs' and Class Members' PII and PHI.

222. UI HomeCare violated HIPAA by failing to properly encrypt the PII and PHI it collected.

223. UI HomeCare's failure to comply with HIPAA and the FTCA constitutes negligence per se.

224. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect.

225. It was reasonably foreseeable that the failure to protect and secure Plaintiffs' and Class Members' PII and PHI in compliance with applicable laws and industry standards would result in that information being accessed and stolen by unauthorized actors.

226. As a direct and proximate result of UI HomeCare's negligence per se, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from the unauthorized access to their PII and PHI, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

227. Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial and injunctive relief requiring UI HomeCare to, inter alia, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of Plaintiffs and the Class)

228. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

229. Plaintiffs and Class Members provided UI HomeCare with their PII and PHI.

230. By providing their PII and PHI, and upon UI HomeCare's acceptance of this information, Plaintiffs and Class Members, on the one hand, and UI HomeCare, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

231. The implied contracts between UI HomeCare and Plaintiffs and Class Members obligated UI HomeCare to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiffs' and Class Members' PII and PHI. The terms of these implied contracts

are described in federal laws, state laws, and industry standards, as alleged above. UI HomeCare expressly adopted and assented to these terms in its public statements, representations and promises as described above.

232. The implied contracts for data security also obligated UI HomeCare to provide Plaintiffs and Class Members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII and PHI.

233. UI HomeCare breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure Plaintiffs and Class Members' PII and PHI; and allowing unauthorized persons to access Plaintiffs' and Class Members' PII and PHI.

234. As a direct and proximate result of UI HomeCare's breaches of the implied contracts, Plaintiffs and Class Members have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of PII and PHI, and are entitled to damages in an amount to be proven at trial.

COUNT IV
BREACH OF CONFIDENCE
(on behalf of Plaintiffs and the Class)

235. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

236. During Plaintiffs' and Class Members' interactions with UI HomeCare, UI HomeCare was fully aware of the confidential nature of the PHI/PII that Plaintiffs and Class Members provided to it.

237. As alleged herein and above, UI HomeCare's relationship with Plaintiffs and Class Members was governed by promises and expectations that Plaintiffs and Class Members' PHI/PII would be collected, stored, and protected in confidence, and would not be accessed by,

acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

238. Plaintiffs and Class Members provided their respective PHI/PII to UI HomeCare with the explicit and implicit understandings that UI HomeCare would protect and not permit the PHI/PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

239. Plaintiffs and Class Members also provided their PHI/PII to UI HomeCare with the explicit and implicit understanding that UI HomeCare would take precautions to protect their PHI/PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

240. UI HomeCare voluntarily received, in confidence, Plaintiffs' and Class Members' PHI/PII with the understanding that the PHI/PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

241. Due to UI HomeCare's failure to prevent, detect and avoid the Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiffs' and Class Members' PHI/PII, Plaintiffs' and Class Members' PHI/PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiffs' and Class Members' confidence and without their express permission.

242. As a direct and proximate cause of UI HomeCare's actions and/or omissions, Plaintiffs and Class Members have suffered damages, as alleged herein.

243. But for UI HomeCare's failure to maintain and protect Plaintiffs' and Class Members' PHI/PII in violation of the parties' understanding of confidence, their PHI/PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. The Data Breach was the direct and legal cause of the misuse of Plaintiffs' and Class Members' PHI/PII and the resulting damages.

244. The injury and harm Plaintiffs and Class Members suffered and will continue to suffer was the reasonably foreseeable result of UI HomeCare's unauthorized misuse of Plaintiffs' and Class Members' PHI/PII. UI HomeCare knew its data systems and protocols for accepting and securing Plaintiffs' and Class Members' PHI/PII had security and other vulnerabilities that placed Plaintiffs' and Class Members' PHI/PII in jeopardy.

245. As a direct and proximate result of UI HomeCare's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PHI/PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PHI/PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PHI/PII, which remains in UI HomeCare's possession and is subject to further unauthorized disclosures so long as UI HomeCare fails to undertake appropriate and adequate measures to protect Class Members' PHI/PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for

the remainder of the lives of Plaintiffs and Class Members, (vii) the diminished value of Plaintiffs' and Class Members' PHI/PII, and (viii) the diminished value of UI HomeCare's services for which Plaintiffs and Class Members paid and received.

COUNT V
BREACH OF FIDUCIARY DUTY
(on behalf of Plaintiffs and the Class)

246. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

247. In light of the special relationship between UI HomeCare and Plaintiffs and Class Members, whereby UI HomeCare became the guardian of Plaintiffs' and Class Members' PHI/PII, UI HomeCare became a fiduciary by its undertaking and guardianship of the PHI/PII to act primarily for Plaintiffs and Class Members, (i) for the safeguarding of Plaintiffs' and Class Members' PHI/PII, (ii) to timely notify Plaintiffs and Class Members of a data breach and disclosure, and (iii) to maintain complete and accurate records of what information (and where) UI HomeCare did has and continues to store.

248. UI HomeCare has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its customers' patients and former patients—in particular, to keep their PHI/PII secure.

249. UI HomeCare breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

250. UI HomeCare breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' PHI/PII.

251. UI HomeCare breached its fiduciary duties to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

252. UI HomeCare breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI/PII.

253. As a direct and proximate result of UI HomeCare's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PHI/PII, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PHI/PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, contest, and recover from identity theft, (v) the continued risk to their PHI/PII, which remains in UI HomeCare's possession and is subject to further unauthorized disclosures so long as UI HomeCare fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, and (vii) the diminished value of UI HomeCare's services they received.

254. As a direct and proximate result of UI HomeCare's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
UNJUST ENRICHMENT
(on behalf of Plaintiffs and the Class)

255. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

256. Plaintiffs and Class members have a legal and equitable interest in the PII and PHI that was collected and maintained by UI HomeCare.

257. UI HomeCare benefited from the conferral upon it of Plaintiffs' and Class Members' PII and PHI and by its ability to retain and use that information.

258. UI HomeCare also understood and appreciated that Plaintiffs' and Class Members' PII and PHI was private and confidential and its value depended upon UI HomeCare maintaining the privacy and confidentiality of that information.

259. But for UI HomeCare's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class Members would not have provided or authorized their PII and PHI to be provided to UI HomeCare, and UI HomeCare would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers, gaining the reputational advantages conferred upon it by Plaintiffs and Class Members, collecting excessive advertising and sales revenues, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

260. As a result of UI HomeCare's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiffs, Class Members, and the public regarding the nature and scope of the Data Breach; its failure to employ adequate data security measures; its

continued maintenance and use of the PII and PHI belonging to Plaintiffs and Class Members without having adequate data security measures; and its other conduct facilitating the theft of that PII and PHI), UI HomeCare has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

261. UI HomeCare's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiffs' and Class Members' PII and PHI, while at the same time failing to maintain that information secure from intrusion.

262. It is inequitable for UI HomeCare to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and Class Members. UI HomeCare's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

263. The benefit conferred upon, received, and enjoyed by UI HomeCare was not conferred officiously or gratuitously, and it would be inequitable and unjust for UI HomeCare to retain the benefit.

264. UI HomeCare is therefore liable to Plaintiffs and Class Members for restitution in the amount of the benefit conferred on UI HomeCare as a result of its wrongful conduct, including specifically the value to UI HomeCare of the PII and PHI that was accessed and exfiltrated in the Data Breach and the profits UI HomeCare receives from the use and sale of that information.

265. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from UI HomeCare and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by UI HomeCare from its wrongful conduct.

266. Plaintiffs and Class Members may not have an adequate remedy at law against UI HomeCare, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, individually and on behalf of all others similarly situated, prays for relief as follows:

a. for an Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

b. for equitable relief enjoining UI HomeCare from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

c. for equitable relief compelling UI HomeCare to use appropriate cybersecurity methods and policies with respect to PII and PHI collection, storage, and protection, and to disclose with specificity to Class Members the types of PII and PHI compromised;

d. for an award of damages, including actual, nominal, consequential, enhanced compensatory, and punitive damages, as allowed by law in an amount to be determined;

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

f. for prejudgment interest on all amounts awarded; and

g. such other and further relief as this Court may deem just and proper.

E-FILED 2026 APR 15 12:52 PM JOHNSON - CLERK OF DISTRICT COURT

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: April 15, 2026

Respectfully submitted,

BULLOCK LAW, PLLC

/s/ Lori A. Bullock
Lori Bullock
309 East 5th Street
Suite 202B
Des Moines, IA 50309
(515) 423-0551
lbullock@bullocklawpllc.com

Liaison Counsel for Plaintiffs and the Proposed Class

Daniel Srourian (admitted *pro hac vice*)
SROURIAN LAW FIRM, P.C.
468 N. Camden Dr. Suite 200
Beverly Hills, CA 90210
(213) 474-3800
daniel@slfla.com

Bart D. Cohen (admitted *pro hac vice*)
BAILEY GLASSER LLP
1055 Thomas Jefferson Street, NW
Suite 540
Washington, DC 20007
(202) 463-2101
bcohen@baileyglasser.com

Proposed Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

Mark S. Reich
LEVI & KORSINSKY, LLP
33 Whitehall Street, 27th Floor
New York, NY 10004
(212) 363-7500
mreich@zlk.com

E-FILED 2026 APR 15 12:52 PM JOHNSON - CLERK OF DISTRICT COURT

Amber L. Schubert
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
(415) 788-4220
aschubert@sjk.law

Raina Borelli
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
raina@straussborrelli.com

Leanna A. Loginov
SHAMIS & GENTILE P.A.
14 NE 1st Avenue, Suite 705
Miami, Florida 33132
(305) 479-2299
lloginov@shamisgentile.com

M. Anderson Berry
EMERY | REDDY, PC
600 Stewart Street, Suite 1100
Seattle, WA 98101
(916) 823-6955
anderson@emeryreddy.com

Gerald D. Wells III
LYNCH CARPENTER, LLP
760 Market Street, Suite 600
Philadelphia, PA 19103
(267) 609-6910
jerry@lcllp.com

Proposed Executive Committee for Plaintiffs and the Proposed Class