UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF FLORIDA

MIAMI DIVISION

Master File No. 1:23-cv-21060-Williams

In re INDEPENDENT LIVING SYSTEMS DATA BREACH LITIGATION	)	CLASS ACTION
This Document Relates To: ALL ACTIONS.	)	JURY TRIAL DEMAND

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs David Asato ("Asato"), Michael Berg ("Berg"), Katrina Berres ("Berres"), Ge Xiao Fang ("Fang"), Melinda Geleng ("Geleng"), Mathew George ("George"), Maria Gomez ("Gomez"), Dimitri Gutierrez ("Gutierrez"), Chelsea Jensen ("Jensen"), Rhianna McMullen ("McMullen"), David Perez ("Perez"), Mark Salzano ("Salzano"), Ernest Scoggan ("Scoggan"), and Ryan Smith ("Smith") (collectively, "Plaintiffs"), bring this Consolidated Class Action Complaint against Independent Living Systems, LLC ("Defendant" or "ILS"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and upon information and belief and their counsel's investigations as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII")[1] and personal health information ("PHI")[2] of more than 4.2 million individuals, including, but not limited to, their name, Social Security number, taxpayer identification number, medical information, and health insurance information.[3]

2. As a direct and proximate result of Defendant's data-security failures, Plaintiffs and Class Members' PII and PHI was accessed and exfiltrated by unauthorized actors beginning on at

[1] PII generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. §200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] As defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191, and its implementing regulations. *See* 45 C.F.R. §160.103.

[3] Independent Living Systems, LLC Data Breach Notification to Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec.shtml (last visited Oct. 13, 2023).

least June 30, 2022 through at least July 5, 2022 (the "Data Breach") – a period when the unauthorized actors had unfettered access to Plaintiffs' and Class Members' PII and PII.

3. Upon information and belief, prior to and through the date of the Data Breach, ILS obtained Plaintiffs' and Class Members' PII and PHI and then maintained that sensitive data in a negligent and/or reckless manner. ILS inadequately maintained its network, platform, software, and failed to adequately monitor and audit its technology partners – rendering these easy prey for cybercriminals.

4. Upon information and belief, ILS was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

5. After the Data Breach, ILS failed to provide timely notice to the affected Plaintiffs and Class Members – thereby exacerbating their injuries. Ultimately, ILS deprived Plaintiffs and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, ILS impermissibly left Plaintiffs and Class Members in the dark – thereby causing their injuries to fester and the damage to spread.

6. Even when ILS finally notified Plaintiffs and Class Members of their PII's and PHI's exfiltration, ILS failed to adequately describe the Data Breach and its effects.

7. Plaintiffs' and Class Members' identifying information is compromised and in imminent jeopardy – all because of ILS's negligence. Some Plaintiffs and Class Members have already been victimized by identity theft and fraud as a result of the Data Breach, and as a result, all Plaintiffs and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial and medical accounts.

8. Armed with the PII and PHI stolen in the Data Breach, criminals can commit a litany of crimes, and in this case, already have. Specifically, they can now open new financial

accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

9. Plaintiffs and Class Members have already suffered and will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. Plaintiffs and Class Members have suffered – and will continue to suffer – from the loss of the benefit of their bargain with ILS, unexpected out-of-pocket expenses, diminished value of their PII and PHI, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

11. Through this action, Plaintiffs seek to remedy these injuries on behalf of themselves and all similarly situated individuals whose PII and PHI were exfiltrated and compromised in the Data Breach.

12. Plaintiffs seek remedies, including, but not limited to, compensatory damages, statutory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief – including, but not limited to, improvements to ILS's data security systems, future annual audits, and adequate credit monitoring services funded by ILS.

PARTIES

13. Plaintiff David Asato is a citizen of Hawaii, residing in Honolulu, Hawaii. Plaintiff Asato does not intend to move to another state in the next three years.

14. Plaintiff Michael Berg is a citizen of Florida, residing in Palm Harbor, Florida. Plaintiff Berg does not intend to move to another state in the next three years.

15. Plaintiff Katrina Berres is a citizen of Illinois, residing in Morris, Illinois. Plaintiff Berres does not intend to move to another state in the next three years.

16. Plaintiff Ge Xiao Fang is a citizen of Oregon, residing in Portland, Oregon. Plaintiff Fang does not intend to move to another state in the next three years.

17. Plaintiff Melinda Geleng is a citizen of Florida, residing in Palm Bay, Florida. Plaintiff Geleng does not intend to move to another state in the next three years.

18. Plaintiff Mathew George is a citizen of Colorado, residing in Denver, Colorado. Plaintiff George does not intend to move to another state in the next three years.

19. Plaintiff Maria Gomez is a citizen of California, residing in Baldwin Park, California. Plaintiff Gomez does not intend to move to another state in the next three years.

20. Plaintiff Dimitri Gutierrez is a citizen of California, residing in Murrieta, California. Plaintiff Gutierrez does not intend to move to another state in the next three years.

21. Plaintiff Chelsea Jensen is a citizen of South Carolina, residing in Greenville, South Carolina. Plaintiff Jensen does not intend to move to another state in the next three years.

22. Plaintiff Rhianna McMullen is a citizen of Florida, residing in Cape Coral, Florida. Plaintiff McMullen does not intend to move to another state in the next three years.

23. Plaintiff David Perez is a citizen of California, residing in La Verne, California. Plaintiff Perez does not intend to move to another state in the next three years.

24. Plaintiff Mark Salzano is a citizen of California, residing in Descanso, California. Plaintiff Salzano does not intend to move to another state in the next three years.

25. Plaintiff Ernest Scoggan is a citizen of California, residing in Palmdale, California. Plaintiff Scoggan does not intend to move to another state in the next three years.

26. Plaintiff Ryan Smith is a citizen of California, residing in San Francisco, California. Plaintiff Smith does not intend to move to another state in the next three years.

27. Defendant Independent Living Systems, LLC is a Florida-based limited liability company with its principal place of business located at 4601 NW 77th Avenue, Miami, Florida 33166. As a limited liability company, ILS is a citizen of each state in which one of its members is a citizen. ILS's members are all citizens of the State of Florida. According to ILS's records on Sunbiz.org, each of the following members of ILS reside in Miami, Florida and are citizens of the State of Florida: Nestor Plana; Jay A. Rosen; Michael O. Leavitt; Jacqueline Kosecoff; David A. Rogers; and Mark DiSalvo.[4] As such, ILS is a citizen of the State of Florida.

JURISDICTION AND VENUE

28. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because this is a class action involving more than 100 putative Class Members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because some Plaintiffs (and many members of the Class, defined herein) are citizens of states different than that of ILS.

29. This Court has general personal jurisdiction over ILS because ILS's principal place of business and headquarters is in this District. ILS also regularly conducts substantial business in this District.

[4] ILS, 2022 Florida Limited Liability Company Annual Report, SUNBIZ.ORG (Apr. 22, 2022), https://search.sunbiz.org/Inquiry/CorporationSearch/GetDocument?aggregateId=flal-l02000011126-eabaab8c-290b-4e72-b703-853a8e29f82e&transactionId=l02000011126-640c6c19-70d6-47a8-82fe-d82e1ed09856&formatType=PDF.

30. Venue is proper in this District under 28 U.S.C. §1391(a)(2), (b)(2), and (c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and ILS conducts substantial business in this District.

FACTUAL ALLEGATIONS

ILS Collected and Stored the PII and PHI of Plaintiffs and Class Members

31. Founded in 2001, ILS "offers a comprehensive range of turnkey payer services including clinical and third-party administrative services to managed care organizations and providers that serve high-cost, complex member populations in the Medicare, Medicaid, and Dual-Eligible Market."[5]

32. Specifically, ILS provides a variety of managed services to several partner health plans and their enrollees or referred individuals, including plan administration, nutrition support, and comprehensive care management.

33. According to its website, ILS has more than 800 employees in 10 office locations nationwide and services more than four million members including 250,000 Medicaid and dual eligible members.[6]

34. Upon information and belief, ILS received (through its web properties, website, and otherwise) and maintained the PII and PHI of Plaintiffs and Class Members. These records are stored on ILS's and its partners' computer systems.

35. Because of the highly sensitive and personal nature of the information ILS acquires and stores, ILS knew or reasonably should have known that it stored protected PII and PHI and

---

[5] *See About Us*, INDEP. LIVING SYS., https://ilshealth.com/about-ils/ (last visited Oct. 13, 2023).

[6] *History*, INDEP. LIVING SYS., https://ilshealth.com/history/ (last visited Oct. 17, 2023).

must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' and patients' PII and PHI and provide adequate notice to customers if their PII or PHI is disclosed without proper authorization.

36. When ILS collects this sensitive information, it promises to use reasonable measures to safeguard the PII and PHI from theft and misuse.

37. ILS acquired, collected, stored, and represented that it maintained reasonable security over Plaintiffs' and Class Members' PII and PHI.

38. By obtaining, collecting, receiving, and/or storing Plaintiffs' and Class Members' PII and PHI, ILS assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiffs' and Class Members' PII and PHI from unauthorized disclosure.

39. ILS represents and contractually binds itself in its Privacy Policy that:

> "We are required by law to maintain the privacy and security of your protected health information. We implement a variety of security measures to maintain the safety of your personal information when you access your personal information."
>
> * * *
>
> ILS does not disclose your PII to unauthorized parties.
>
> * * *
>
> "We will promptly notify you if a breach occurs that may have compromised the privacy or security of your information."[7]

40. Upon information and belief, ILS represented to its members and customers orally and in written contracts, marketing materials, and otherwise that it would properly protect all PII

[7] *Privacy Policy*, INDEP. LIVING SYS., https://ilshealth.com/privacy-policy/ (last visited Oct. 13, 2023).

and PHI it obtained. Upon information and belief, ILS knew or reasonably should have known that these representations would be passed on to Plaintiffs and Class Members.

41. A bailment was created (in contract and tort) between (a) ILS and (b) Plaintiffs and Class Members when:

(a) Plaintiffs and Class Members (directly or indirectly) conferred their PHI and PII, which is Plaintiffs' and Class Members' personal property, to ILS's exclusive control;

(b) ILS accepted Plaintiffs' and Class Members' PII and PHI; and

(c) Said actions were made in exchange for:

(i) ILS's promises to render services (including healthcare services and essential data security measures); and

(ii) Plaintiffs' and Class Members' promise to render valuable consideration (including monies, employment services, and their PII and PHI) to ILS from which ILS derived profits.

42. The existence of a bailment between (a) ILS and (b) Plaintiffs and Class Members created a duty on ILS's part to properly secure Plaintiffs' and Class Members' PII and PHI.

43. ILS's position as a custodian of Plaintiffs' and Class Members' medical information and records created a duty on ILS's part to properly secure Plaintiffs' and Class Members' PHI.

44. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI, including, but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

45. Upon information and belief, Plaintiffs and Class Members relied on ILS to keep their PII and PHI confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

46. ILS could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting its information technology partners.

47. ILS's negligence in safeguarding Plaintiffs' and Class Members' PII and PHI was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

48. The healthcare industry in particular has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint, and 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] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.[9]

49. In the context of data breaches, healthcare is "by far the most affected industry sector."[10] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly

---

[8] Steve Alder, *2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020*, HIPAA J. (Jan. 24, 2021), https://www.hipaajournal.com/2020-healthcare-data-breach-report/.

[9] Steve Alder, April 2021 Healthcare Data Breach Report, HIPAA J. (May 18, 2021) https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/.

[10] Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

sensitive and detailed PII.[11] And according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in recent years.[12]

50. Despite the prevalence of public announcements of data breaches and data security compromises, ILS failed to take appropriate steps to protect Plaintiffs' and Class Members' PII and PHI from being compromised.

51. ILS failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

52. ILS failed to ensure the proper monitoring and logging of file access and modifications.

53. ILS failed to ensure the proper training of its employees as to cybersecurity best practices.

54. ILS failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiffs and Class Members.

55. ILS failed to timely and accurately disclose that Plaintiffs' and Class Members' PII and PHI had been improperly acquired or accessed.

56. ILS knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII and PHI.

57. ILS failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

---

[11] *See id.*

[12] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SEC. MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

58. ILS failed to ensure the proper encryption of Plaintiffs' and Class Members' PII and PHI and monitor user behavior and activity to identify possible threats.

The Data Breach

59. On or about March 14, 2023, Defendant sent Plaintiffs and Class Members a *Notice of Data Security Incident* ("Notice of Data Breach" or "Notice") and submitted sample notices to various states' Attorneys General. Defendant informed Plaintiffs and other Class Members that:

> **What Happened?** On July 5, 2022, we experienced an incident involving the inaccessibility of certain computer systems on our network. We responded to the incident immediately and began an investigation with the assistance of outside cybersecurity specialists. Through our response efforts, we learned that an unauthorized actor obtained access to certain ILS systems between June 30 and July 5, 2022. During that period, some information stored on the ILS network was acquired by the unauthorized actor, and other information was accessible and potentially viewed. Upon containing the incident and reconnecting our computer systems, we began to review the potentially affected data to determine whether it contained any personal information or PHI, and if so, to whom such information related.
>
> **What Information Was Involved?** As previewed above, we conducted a comprehensive data review exercise to understand the scope of potentially affected information and identify the individuals to whom such information relates. On January 17, 2023, we received the results of this review and determined that the following types of information related to you were included in one or more files acquired by the unauthorized actor or present in one or more files that resided on an area of the ILS network that was accessed by the unauthorized actor: name, [Extra8][Extra9][Extra10]. Please note that we have no evidence or other indication that identity theft or fraud occurred as a result of this incident. We are providing this notice out of an abundance of caution[.][13]

60. Although the Data Breach allegedly began on June 30, 2022, it was not until July 5, 2022 – five days later – that ILS became aware of suspicious activity on its network.

61. Upon information and belief, Plaintiffs' and Class Members' PII and PHI was accessed, exfiltrated, and stolen in the Data Breach.

---

[13] Notice of Data Breach, *supra* note 3.

62. Upon information and belief, Plaintiffs' and Class Members' affected PII and PHI was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

63. It is likely the Data Breach was targeted at ILS due to its status as a large information technology provider to healthcare providers and other businesses that collect, create, and maintain both PII and PHI.

64. While ILS claims to have become aware of the Data Breach as early as July 5, 2022, ILS did not begin directly notifying victims of the Data Breach ***until March 2023*** – over eight months later.

65. Time is of the essence when highly sensitive PII and PHI are subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and PHI of Plaintiffs and Class Members is believed to be available on the Dark Web as that is the *modus operandi* for criminals who perpetrate attacks of this type. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the publication of their PII and PHI onto the Dark Web. Plaintiffs and Class Members now face a lifetime risk of identity theft and fraud, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

66. Following the Data Breach and recognizing that each Plaintiff and Class Member is now subject to the present and continuing risk of identity theft and fraud, ILS advised impacted individuals to "remain vigilant for incidents of fraud and identity theft by reviewing account

statements and monitoring free credit reports" and to follow the below steps to further protect themselves:

(a) order your free credit report;

(b) if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, contact the Federal Trade Commission ("FTC") and/or your state's attorney general office about for information on how to prevent or avoid identity theft;

(c) place a security freeze; and

(d) place a fraud alert.[14]

67. ILS largely put the burden on Plaintiffs and Class Members to take measures to protect themselves.

68. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[15]

69. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[16] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable

---

[14] *Id*.

[15] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS (FEB. 2021), https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour.

[16] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC (Nov. 6, 2019), https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html.

income.'"[17] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

70. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

71. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PII and PHI with the intent of engaging in misuse of the PII and PHI, including marketing and selling Plaintiffs' and Class Members' PII and PHI.

72. ILS also offered credit monitoring services to a limited number of individuals for a limited amount of time. Such measures, however, are insufficient to protect Plaintiffs and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide Plaintiffs and Class Members identity theft protection services for their respective lifetimes.

73. ILS had and continues to have obligations created by the HIPAA, reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiffs' and Class Members' PII and PHI confidential and to protect such PII and PHI from unauthorized access.

[17] *Id.*

74. ILS's Breach Notice letter, as well as its website notice, both omit the size and scope of the Data Breach. ILS has demonstrated a pattern of providing untimely and inadequate notices and disclosures about the Data Breach.

75. Plaintiffs and the Class Members remain, even today, in the dark regarding the particular ransomware used, and what steps are being taken, if any, to secure their PII, PHI, and financial information going forward. Plaintiffs and Class Members are left to speculate as to the full impact of the Data Breach and how exactly ILS intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

76. Because hackers often release stolen PII and PHI in batches in order to maximize its value, instead of all at once, if not done already, each and every Plaintiffs' and Class Members' PII and PHI and financial information will likely end up for sale on the Dark Web, or simply fall into the hands of companies that will use the detailed PII and PHI and financial information for targeted marketing without the approval of Plaintiffs and/or Class Members. Either way, unauthorized individuals can now easily access the PII and PHI and/or financial information of Plaintiffs and Class Members, and in many instances, already have.

ILS Failed to Comply with FTC Guidelines

77. According to the FTC, the need for data security should be factored into all business decision-making.[18] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as ILS, should employ to protect against the unlawful exfiltration of PII and PHI.

[18] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF.

78. 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.[19] The guidelines explain that businesses should:

(a) protect the personal customer information that they keep;

(b) properly dispose of personal information 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.

79. 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.

80. The FTC recommends that companies not maintain PII and PHI longer than is needed 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.[20]

81. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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 of 1914 ("FTC

[19] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre.

[20] *See Start with Security*, *supra* note 18.

Act"), 15 U.S.C. §45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

82. These FTC enforcement actions include actions against healthcare providers and partners like ILS. *See, e.g.*, *In the Matter of LabMD, Inc., a Corp*, 2016-2 Trade Cas. (CCH) ¶79708, 2016 WL 4128215, at *32 (July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

83. ILS's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. §45.

ILS Failed to Follow Industry Standards

84. Despite its alleged commitments to securing sensitive patient data, ILS does not follow industry standard practices in securing patients' PII and PHI.

85. As shown above, experts studying cybersecurity routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

86. Several best practices have been identified that at a minimum should be implemented by healthcare providers like ILS, including, but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

87. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network

ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

88. ILS failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, but not limited to, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

89. Such frameworks are the existing and applicable industry standards in the healthcare industry. And ILS failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

ILS Violated the HIPAA

90. The HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. The HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[21]

[21] The HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

91. The HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[22]

92. The Data Breach itself resulted from a combination of inadequacies showing ILS failed to comply with safeguards mandated by the HIPAA. ILS's security failures include, but are not limited to:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. §164.306(a)(1);

(b) Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §164.306(a)(2);

(c) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

(d) Failing to ensure compliance with HIPAA security standards by ILS's workforce in violation of 45 C.F.R. §164.306(a)(4);

(e) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

(f) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

[22] *See* 45 C.F.R. §164.306 (security standards and general rules); 45 C.F.R. §164.308 (administrative safeguards); 45 C.F.R. §164.310 (physical safeguards); 45 C.F.R. §164.312 (technical safeguards).

(g) Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

(h) Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §§164.308(a)(5) and 164.530(b); and

(i) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. §164.530(c).

93. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrates ILS failed to comply with safeguards mandated by HIPAA regulations.

The Experiences and Injuries of Plaintiffs and Class Members

94. Plaintiffs and Class Members are customers of ILS and members of health plans to which ILS provides services.

95. Plaintiffs and Class Members provided valuable consideration (directly or indirectly) – including monies, PHI, and PII – to ILS in exchange for certain services. A portion of said consideration (and the profits derived from such) was intended to have been used by ILS for data security measures to secure Plaintiffs and Class Members' PII and PHI.

96. As a prerequisite of receiving treatment and/or services, ILS requires its employees and health plan members – like Plaintiffs and Class Members – to disclose their PII and PHI.

97. When ILS finally announced the Data Breach, it deliberately underplayed the Data Breach's severity and obfuscated the nature of the Data Breach. ILS's Breach Notice sent to Plaintiffs and Class Members fails to explain how the breach occurred (what security weakness

was exploited), who the Data Breach was perpetrated by, and the extent to which those data elements were compromised.

98. Because of the Data Breach, ILS inflicted injuries upon Plaintiffs and Class Members. And yet, ILS has done little to provide Plaintiffs and the Class Members with relief for the damages they suffered.

99. All Class Members were injured when ILS caused their PII and PHI to be exfiltrated by cybercriminals.

100. Plaintiffs and Class Members entrusted their PII and PHI to ILS. Thus, Plaintiffs had the reasonable expectation and understanding that ILS would take – ***at minimum*** – industry standard and legally mandated precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiffs would not have entrusted their PII and PHI to ILS had they known that ILS would not take reasonable steps to safeguard their information.

101. Plaintiffs and Class Members suffered actual injury from having their PII and PHI compromised in the Data Breach including, but not limited to: (a) damage to and diminution in the value of their PII and PHI – a form of property that ILS obtained from Plaintiffs; (b) violation of their privacy rights; (c) the theft of their PII and PHI; (d) fraudulent activity resulting from the Data Breach; (e) present and continuing injury arising from the increased risk of additional identity theft and fraud, such as the time and money spent mitigating the harm of the Data Breach.

102. Moreover, because of the Data Breach, Plaintiffs and Class Members have spent – and will continue to spend – considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff David Asato's Experience

103. As a condition of receiving services from his medical provider or insurer, Plaintiff Asato was required to provide his PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

104. Plaintiff Asato was insured by Kaiser Permanente ("Kaiser"). Kaiser is one of the nation's largest health plans, serving almost 13 million members, including in Hawaii. It operates 39 hospitals and more than 620 medical offices.[23]

105. Plaintiff Asato's PHI from Kaiser was, on information and belief, transferred to ILS and became part of its Data Breach, even though Plaintiff Asato did not otherwise have any connection to ILS but nonetheless received the ILS Notice.

106. Plaintiff Asato greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Asato took reasonable steps to maintain the confidentiality of his PII and PHI.

107. Plaintiff Asato received a letter dated March 14, 2023 from ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name, date of birth, Social Security number, and health insurance information.

108. Although ILS discovered the Data Breach in July 2022, Plaintiff Asato was not notified of the Data Breach until in or around March 14, 2023.

109. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Asato faces, ILS offered him a one-year subscription to a credit monitoring service.

[23] *Who We Are*, Kaiser Permanente, about.kaiserpermanente.org/who-we-are/fast-facts (last visited Nov. 10, 2023).

However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

110. Since learning of the Data Breach, Plaintiff Asato received notification that his personal information has been found on the dark web.

111. Since learning of the Data Breach, Plaintiff Asato has spent additional time dealing with the consequences of the Data Breach and continues to spend time dealing with the Data Breach, including time spent researching the Data Breach, considering credit monitoring and identity theft insurance options, and self-monitoring his accounts, all as a result of his PII and PHI being exposed in the Data Breach. Since March 2023, he has spent approximately five minutes each sitting periodically reviewing his accounts. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Asato intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

112. As a result of the Data Breach, Plaintiff Asato spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

113. Plaintiff Asato has also experienced an increase of other spam calls and texts after the Data Breach.

114. In addition, Plaintiff Asato has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and

PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

115. Plaintiff Asato plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

116. Additionally, Plaintiff Asato is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Asato stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

117. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Asato would take, and continue to take, necessary measures to protect his PII and PHI.

118. Plaintiff Asato has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

119. Plaintiff Asato has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII and PHI. Plaintiff Asato has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

120. Plaintiff Asato has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, especially his Social Security number, in combination with his name and date of birth, along with his sensitive health insurance information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

121. As a direct and traceable result of the Data Breach, Plaintiff Asato will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Michael Berg's Experience

122. As a condition of receiving services from his medical provider, Plaintiff Berg was required to provide his PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

123. Plaintiff Berg greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Berg took reasonable steps to maintain the confidentiality of his PII and PHI.

124. Plaintiff Berg received a letter dated March 14, 2023 from ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name, date of birth, driver's license, state identification, Social Security number, medical record number, Medicare or Medicaid identification, CIN#, mental or physical treatment/condition information, food delivery information, diagnosis code or diagnosis information, admission/discharge date, prescription information, billing/claims information, patient name, and health insurance information.

125. Although ILS discovered the Data Breach in July 2022, Plaintiff Berg was not notified of the Data Breach until March of 2023.

126. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Berg faces, ILS offered him a one-year subscription to a credit monitoring service. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

127. In October of 2022, Plaintiff Berg was alerted to the fact that his personal information had been put on the dark web. As a result, he was required to replace his credit cards. He believes this is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and he had never experienced this in the past. Additionally, Plaintiff Berg received a promotional inquiry from Kay Jewelers on his credit report on June 13, 2023, but he has never done business with that company, nor has he applied for financing with that company. Based on the timing, Plaintiff Berg believes this fraudulent activity is the result of the Data Breach.

128. Since learning of the Data Breach, Plaintiff Berg has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, finding representation, replacing credit cards, and self-monitoring his accounts, all as a result of his PII and PHI being exposed in the Data Breach. Since March 2023, he has spent approximately 10-12 hours reviewing his account statements, replacing credit cards, trying to get into contact with Defendant about the breach, and exploring credit monitoring options. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any

questionable activity to the associated institutions immediately." Plaintiff Berg intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

129. As a result of the Data Breach, Plaintiff Berg spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

130. Plaintiff Berg has also experienced an increase in spam calls, text messages and emails after the Data Breach, and he presently receives unwanted calls and text messages from strangers on a daily basis. Plaintiff Berg believes this is a result of the Data Breach.

131. In addition, Plaintiff Berg, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

132. Plaintiff Berg plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

133. Additionally, Plaintiff Berg is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Berg stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

134. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Berg would take, and continue to take, necessary measures to protect his PII and PHI.

135. Plaintiff Berg has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

136. Plaintiff Berg has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII and PHI. Plaintiff Berg has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

137. Plaintiff Berg has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, especially his Social Security number, date of birth, driver's license, state identification, medical record number, Medicare or Medicaid identification, CIN#, mental or physical treatment/condition information, prescription information, billing/claims information, patient name, and health insurance information, all of which is now in the hands of cybercriminals and other unauthorized third parties.

138. As a direct and traceable result of the Data Breach, Plaintiff Berg will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Katrina Berres's Experience

139. As a condition of being employed by ILS in 2014, Plaintiff Berres was required to provide her PII and other sensitive information to ILS, which was then entered into ILS's database and maintained by ILS.

140. Additionally, as a condition of receiving services from her medical provider or insurer, Plaintiff Berres was required to provide her PII and PHI, which was then obtained by Defendant ILS, entered into ILS's database, and maintained by ILS.

141. Plaintiff Berres greatly values her privacy and PII and PHI, and she took reasonable steps to maintain the confidentiality of her PII and PHI prior to the Data Breach.

142. Plaintiff Berres received a letter dated March 14, 2023 from Defendant ILS informing her of the Data Breach. The letter stated that unauthorized actors gained access to and acquired information from one or more files in ILS's computer systems that contained her name, date of birth, and social security number.

143. Although ILS discovered the Data Breach in July 2022, Plaintiff Berres was not notified of the Data Breach until in or around March of 2023.

144. After the Data Breach, Plaintiff Berres experienced multiple instances of identity fraud, including when an individual attempted to enroll in government assistance programs in her name, and open credit cards in her name. She believes the fraudulent activity is a result of the Data Breach given that it occurred relatively soon after the Data Breach. Additionally, Plaintiff Berres has received multiple text messages from Chase Bank alerting her to account inquiries that she herself did not make.

145. Since learning of the Data Breach, Plaintiff Berres has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach and self-monitoring her accounts, all as a result of her PII and PHI being exposed in the Data Breach. Since March 2023, she has spent approximately 4-5 hours reviewing her account statements and fraud alerts, managing an uptick in spam, and discussing the case with her attorneys. Plaintiff spent this time at ILS's direction. In the notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating her losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Berres intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

146. As a result of the Data Breach, Plaintiff Berres spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

147. Plaintiff Berres has also experienced an increase in other spam calls, text messages, and emails after the Data Breach.

148. In addition, Plaintiff Berres, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of her privacy which she would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

149. Plaintiff Berres plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

150. Additionally, Plaintiff Berres is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Berres stores any documents containing her PII or PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

151. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Berres would take, and continue to take, necessary measures to protect her PII and PHI.

152. Plaintiff Berres has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

153. Plaintiff Berres has suffered actual, concrete injury in the form of damages to, and diminution in, the value of her PII and PHI. Plaintiff Berres has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

154. Plaintiff Berres has suffered imminent and impending injury arising from actual fraud and/or identity theft, the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, which is now in the hands of cybercriminals and other unauthorized third parties.

155. As a direct and traceable result of the Data Breach, Plaintiff Berres will continue to suffer actual fraud and/or identity theft, be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Ge Xiao Fang's Experience

156. As a condition of receiving services from his medical provider or insurer, Plaintiff Fang was required to provide his PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

157. Plaintiff Fang was insured by Kaiser. Kaiser is one of the nation's largest health plans, serving almost 13 million members, including in Oregon. It operates 39 hospitals and more than 620 medical offices.[24]

158. Plaintiff Fang has received services through Medicare and Medicaid.

159. Plaintiff Fang's PHI from Kaiser was, on information and belief, transferred to ILS and became part of its data breach, even though Plaintiff Fang did not otherwise have any connection to ILS but nonetheless received the ILS Notice.

160. Plaintiff Fang greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Fang took reasonable steps to maintain the confidentiality of his PII and PHI.

[24] *Id.*

161. Plaintiff Fang received a letter dated March 14, 2023 from Defendant ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name and other PII and PHI.

162. Although ILS discovered the Data Breach in July 2022, Plaintiff Fang was not notified of the Data Breach until in or around March 14, 2023.

163. Since learning of the Data Breach, Plaintiff Fang has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, researching ILS, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts, all as a result of his PII and PHI being exposed in the Data Breach. After receiving notice of the Data Breach in March 2023, he initially spent approximately 30 minutes to an hour each day reviewing his accounts, monitoring his credit, and researching the Data Breach and ILS. He continues to spend approximately 30 minutes to an hour each week reviewing his accounts and monitoring his credit. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Fang intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

164. As a result of the Data Breach, Plaintiff Fang spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

165. Plaintiff Fang has also experienced an increase of other spam calls after the Data Breach.

166. In addition, Plaintiff Fang has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

167. Plaintiff Fang plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

168. Additionally, Plaintiff Fang is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Fang stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

169. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Fang would take, and continue to take, necessary measures to protect his PII and PHI.

170. Plaintiff Fang has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

171. Plaintiff Fang has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII and PHI. Plaintiff Fang has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

172. Plaintiff Fang has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

173. As a direct and traceable result of the Data Breach, Plaintiff Fang will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Melinda Geleng's Experience

174. As a condition of receiving services from her medical provider or insurer, Plaintiff Geleng was required to provide her PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

175. Plaintiff Geleng greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Geleng took reasonable steps to maintain the confidentiality of her PII and PHI.

176. Plaintiff Geleng received a letter dated March 14, 2023 from ILS informing her of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained her name, date of birth, Medicare

identification, Medicaid identification, Food Delivery Information, and other health insurance information.

177. Although ILS discovered the Data Breach in July 2022, Plaintiff Geleng was not notified of the Data Breach until in or around March of 2023.

178. Shortly after receiving the Notice letter from ILS, Plaintiff Geleng put a fraud alert on her Discover account. Despite this, Plaintiff Geleng experienced identity fraud in the form of unauthorized charges on her Discover credit account. As a result, she was required to contact Discover to dispute the charges, and she also contacted her other financial institutions. She believes the unauthorized charge is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and she had no other previous fraudulent charges on her credit card. Additionally, Plaintiff Geleng has received approximately 4-5 fraud monitoring alerts from Experian and Discover since the Data Brach, and she does not recall receiving any such alerts prior to the Data Breach.

179. Since learning of the Data Breach, Plaintiff Geleng has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts, all as a result of her PII and PHI being exposed in the Data Breach. Since March 2023, she has spent approximately 1-2 hours each week reviewing her account statements and fraud alerts, and she also spent additional time contacting her financial institutions and placing fraud alerts on her accounts. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating her losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated

institutions immediately." Plaintiff Geleng intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

180. As a result of the Data Breach, Plaintiff Geleng spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

181. Plaintiff Geleng has also experienced an increase in other spam calls, text messages, and emails after the Data Breach. Plaintiff Geleng recently changed her phone number, and this was in part due to the constant barrage of spam and phishing attempts she has experienced since the Data Breach.

182. In addition, Plaintiff Geleng, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of her privacy which she would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

183. Plaintiff Geleng plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

184. Additionally, Plaintiff Geleng is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Geleng stores any documents containing her PII or PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

185. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Geleng would take, and continue to take, necessary measures to protect her PII and PHI.

186. Plaintiff Geleng has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

187. Plaintiff Geleng has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his/her PII and PHI. Plaintiff Geleng has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

188. Plaintiff Geleng has suffered imminent and impending injury arising from actual fraud and/or identity theft, the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, which is now in the hands of cybercriminals and other unauthorized third parties.

189. As a direct and traceable result of the Data Breach, Plaintiff Geleng will continue to suffer actual fraud and/or identity theft, be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Mathew George's Experience

190. As a condition of receiving services from his medical provider or insurer, Plaintiff George was required to provide his PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

191. Plaintiff George greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff George took reasonable steps to maintain the confidentiality of his PII and PHI.

192. Plaintiff George received a letter dated March 14, 2023 from ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name, date of birth, Social Security number, and health insurance policy number.

193. Although ILS discovered the Data Breach in July 2022, Plaintiff George was not notified of the Data Breach until in or around March 2023.

194. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff George faces, ILS offered him a one-year subscription to a credit monitoring service. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

195. Since learning of the Data Breach, Plaintiff George has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts, all as a result of his PII and PHI being exposed in the Data Breach. Since March 2023, he has spent approximately one hour each month reviewing his account statements, and checking his credit reporting. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the

associated institutions immediately." Plaintiff George intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

196. As a result of the Data Breach, Plaintiff George spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

197. Plaintiff George has also experienced an increase of other spam calls, text messages and emails after the Data Breach.

198. In addition, Plaintiff George, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

199. Plaintiff George plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

200. Additionally, Plaintiff George is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff George stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

201. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and

expected that Plaintiff George would take, and continue to take, necessary measures to protect his PII and PHI.

202. Plaintiff George has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

203. Plaintiff George has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII and PHI. Plaintiff George has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

204. Plaintiff George has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, especially his Social Security number, in combination with his name, along with his sensitive medical information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

205. As a direct and traceable result of the Data Breach, Plaintiff George will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Maria Gomez's Experience

206. As a condition of receiving services from her insurer and/or healthcare provider, Kaiser, Plaintiff Gomez was required to provide her PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

207. Plaintiff Gomez greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Gomez took reasonable steps to maintain the confidentiality of her PII and PHI.

208. Plaintiff Gomez received a letter dated March 14, 2023 from ILS informing her of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained her name, date of birth, Social Security number, medical record numbers, CIN#, treatment information, food delivery information, admission dates, billing/claims information, and health insurance information.

209. Although ILS discovered the Data Breach in July 2022, Plaintiff Gomez was not notified of the Data Breach until in or around March 2023.

210. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Gomez faces, ILS offered her a one-year subscription to a credit monitoring service. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

211. For example, in the winter of 2022, after ILS knew of the Data Breach, but before ILS notified Plaintiff Gomez of it, Plaintiff Gomez experienced identity fraud when someone tried to use her information to purchase a vehicle. She first learned of the fraudulent activity when she received a letter informing her that her loan application was denied. She believes the identity fraud is a result of the Data Breach, given that it occurred relatively soon after the Data Breach, and she had no other previous related or similar incidents.

212. Since learning of the Data Breach, Plaintiff Gomez has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, trying to reach ILS for

additional information, contacting and engaging legal counsel, reviewing account statements, and self-monitoring her accounts, all as a result of her PII and PHI being exposed in the Data Breach. Since March 2023, she has spent approximately one hour each week reviewing her account statements, and mitigating the identify theft she suffered. Plaintiff spent this time at ILS's direction and due to the identity fraud she experienced after the Data Breach. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating her losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Gomez intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

213. As a result of the Data Breach, Plaintiff Gomez spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

214. Plaintiff Gomez has also experienced an increase in spam calls since the Data Breach.

215. In addition, Plaintiff Gomez, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of her privacy which she would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months, during which time she suffered from identity theft.

216. Plaintiff Gomez plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

217. Additionally, Plaintiff Gomez is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Gomez stores any documents containing her PII or PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

218. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Gomez would take, and continue to take, necessary measures to protect her PII and PHI.

219. Plaintiff Gomez has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

220. Plaintiff Gomez has suffered actual, concrete injury in the form of damages to, and diminution in, the value of her PII and PHI. Plaintiff Gomez has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

221. Plaintiff Gomez has suffered injury arising from actual fraud and identity theft, as well as the substantially increased risk of future fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, especially her Social Security number, in

combination with her name, along with her sensitive medical information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

222. As a direct and traceable result of the Data Breach, Plaintiff Gomez will continue to suffer actual fraud and/or identity theft, be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Dimitri Gutierrez's Experience

223. As a condition of receiving services from his medical provider or insurer, Plaintiff Gutierrez was required to provide his PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

224. Plaintiff Gutierrez greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Gutierrez took reasonable steps to maintain the confidentiality of his PII and PHI.

225. Plaintiff Gutierrez received a letter dated March 14, 2023 from ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name, date of birth, and health insurance information.

226. Although ILS discovered the Data Breach in July 2022, Plaintiff Gutierrez was not notified of the Data Breach until in or around late March 2023.

227. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Gutierrez faces, ILS offered him a one-year subscription to a credit monitoring service. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

228. Since learning of the Data Breach, Plaintiff Gutierrez has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts, all as a result of his PII and PHI being exposed in the Data Breach. Since March 2023, he has spent approximately 1-2 hours each week reviewing his account statements, emails, and texts. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Gutierrez intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

229. As a result of the Data Breach, Plaintiff Gutierrez spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

230. Plaintiff Gutierrez has also experienced an increase of other spam calls, text messages, and emails after the Data Breach.

231. In addition, Plaintiff Gutierrez, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

232. Plaintiff Gutierrez plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

233. Additionally, Plaintiff Gutierrez is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Gutierrez stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

234. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Gutierrez would take, and continue to take, necessary measures to protect his PII and PHI.

235. Plaintiff Gutierrez has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

236. Plaintiff Gutierrez has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his/her PII and PHI. Plaintiff Gutierrez has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

237. Plaintiff Gutierrez has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from

the compromise of his PII and PHI, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

238. As a direct and traceable result of the Data Breach, Plaintiff Gutierrez will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Chelsea Jensen's Experience

239. As Defendant's patient and as a condition of receiving medical treatment and services from Defendant, Plaintiff Jensen was required to provide her PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

240. Plaintiff Jensen greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Jensen took reasonable steps to maintain the confidentiality of her PII and PHI.

241. Plaintiff Jensen received a letter dated March 14, 2023 from ILS informing her of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained her name, date of birth, Medicare identification, Medicaid identification, and other health insurance information.

242. Although ILS discovered the Data Breach in July 2022, Plaintiff Jensen was not notified of the Data Breach until she received the letter from ILS in or around March of 2023.

243. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Jensen faces, ILS offered her a one-year subscription to a credit monitoring service. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

244. Shortly after being notified of the Data Breach, Plaintiff Jensen experienced identity fraud in the form of credit card charges, and the unauthorized sharing of her personal cell phone number. As a result, she was required to replace her credit cards, continuously monitor her bank accounts and credit report, change her account passwords, and obtain a credit freeze on her credit accounts. She believes the unauthorized charges on her credit card is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and she had no other previous fraudulent charges on her debit card.

245. Since learning of the Data Breach, Plaintiff Jensen has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts, all as a result of her PII and PHI being exposed in the Data Breach. Since March 2023, she has spent over one hundred hours reviewing her account statements, credit report, and changing passwords and authorizations. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating her losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Jensen intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

246. As a result of the Data Breach, Plaintiff Jensen spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

247. Plaintiff Jensen has also experienced an increase of other spam calls, text messages and emails after the Data Breach.

248. In addition, Plaintiff Jensen has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of her privacy which she would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

249. Plaintiff Jensen plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

250. Additionally, Plaintiff Jensen is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Jensen stores any documents containing her PII or PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

251. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Jensen would take, and continue to take, necessary measures to protect her PII and PHI.

252. Plaintiff Jensen has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

253. Plaintiff Jensen has suffered actual, concrete injury in the form of damages to, and diminution in, the value of her PII and PHI. Plaintiff Jensen has also suffered actual, concrete

injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach and has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

254. Plaintiff Jensen has suffered imminent and impending injury arising from identity fraud the substantially increased risk of fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

255. As a direct and traceable result of the Data Breach, Plaintiff Jensen will continue to suffer identity fraud and be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Rhianna McMullen's Experience

256. As a condition of receiving services from her Medicaid-affiliated insurer Vivida Health, Plaintiff McMullen was required to provide her PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

257. Plaintiff McMullen greatly values her privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff McMullen took reasonable steps to maintain the confidentiality of her PII and PHI.

258. Plaintiff McMullen received a letter dated March 14, 2023 from ILS informing her of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained her name, date of birth, driver's license information, state identification information, Social Security number, medical record numbers, Medicare or Medicaid identification, CIN#, mental or physical treatment/condition information, food delivery information, diagnosis code or diagnosis information, admission/discharge dates,

prescription information, billing/claims information, patient name, and health insurance information.

259. Although ILS discovered the Data Breach in July 2022, Plaintiff McMullen was not notified of the Data Breach until in or around March 2023.

260. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff McMullen faces, ILS offered her a one-year subscription to a credit monitoring service. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

261. For example, in February 2023, after ILS knew of the Data Breach, but before ILS notified Plaintiff McMullen of it, Plaintiff McMullen experienced identity fraud in the form of attempted criminal voter impersonation fraud. As a result, she was required to participate in criminal proceedings against the perpetrator. She believes the criminal voter fraud is a result of the Data Breach, given that it occurred relatively soon after the Data Breach, and she had no other previous related or similar incidents.

262. Since learning of the Data Breach, Plaintiff McMullen has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts, all as a result of her PII and PHI being exposed in the Data Breach. Since March 2023, she has spent approximately one hour each week reviewing her account statements, and mitigating the identify theft she suffered, including participating in criminal proceedings against the individual who attempted to steal her identity. Plaintiff spent this time at ILS's and law enforcement's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating her losses by "review[ing] your

account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff McMullen intends to spend additional time and effort taking steps to protect her PII and PHI in the future.

263. As a result of the Data Breach, Plaintiff McMullen spent valuable time she otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

264. Plaintiff McMullen has also experienced an increase of other spam calls after the Data Breach.

265. In addition, Plaintiff McMullen, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of her privacy which she would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months, during which time she suffered from identity theft.

266. Plaintiff McMullen plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

267. Additionally, Plaintiff McMullen is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff McMullen stores any documents containing her PII or PHI in a safe and secure

location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

268. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff McMullen would take, and continue to take, necessary measures to protect her PII and PHI.

269. Plaintiff McMullen has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

270. Plaintiff McMullen has suffered actual, concrete injury in the form of damages to, and diminution in, the value of her PII and PHI. Plaintiff McMullen has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

271. Plaintiff McMullen has suffered injury arising from actual fraud and/or identity theft, as well as the substantially increased risk of future fraud, identity theft, and misuse of her PII and PHI resulting from the compromise of her PII and PHI, especially her Social Security number and driver's license information, in combination with her name, along with her sensitive medical information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

272. As a direct and traceable result of the Data Breach, Plaintiff McMullen will continue to suffer actual fraud and/or identity theft, be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff David Perez's Experience

273. As a condition of receiving services from his medical provider or insurer, Plaintiff Perez was required to provide his PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

274. Plaintiff Perez was insured by Kaiser. Kaiser is one of the nation's largest health plans, serving almost 13 million members, including in California, where it is based. It operates 39 hospitals and more than 620 medical offices.[25]

275. ILS announced that it partnered with Kaiser to build a California provider network.[26] Kaiser also has a facility called Independent Living Systems-Enhanced Care Management in California, offering Medi-Cal managed care.[27] Medi-Cal is California's Medicaid program. Kaiser offers Medicaid in eight states and DC, including in multiple counties in California.[28] Plaintiff Perez received services through Medi-Cal.

---

[25] *Id.*

[26] Independent Living Systems, https://ilshealth.com/ils-in-california/ (last visited Nov. 10, 2023).

[27] *Independent Living Systems - Enhanced Care Management (ECM)*, Kaiser Permanente, https://healthy.kaiserpermanente.org/southern-california/facilities/independent-living-systems-enhanced-care-management-ecm-136605 (last visited Nov. 10, 2023).

[28] *Medi-Cal Managed Care Health Plan Directory*, DHCS, https://www.dhcs.ca.gov/individuals/Pages/MMCDHealthPlanDir.aspx (last visited Nov. 10, 2023).

276. Plaintiff Perez's PHI from Kaiser was, on information and belief, transferred to ILS and became part of its Data Breach, even though Plaintiff Perez did not otherwise have any connection to ILS but nonetheless received the ILS Notice.

277. Plaintiff Perez greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Perez took reasonable steps to maintain the confidentiality of his PII and PHI.

278. Plaintiff Perez received a letter dated March 14, 2023 from ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name, date of birth, and health insurance information.

279. Although ILS discovered the Data Breach in July 2022, Plaintiff Perez was not notified of the Data Breach until in or around March 14, 2023.

280. Since the Data Breach, Plaintiff Perez has received notification that his personal information has been found on the dark web.

281. Plaintiff Perez drove to his bank, Navy Federal, twice to obtain a new card for his bank account, expending resources in the form of gas and time to drive 20 miles round trip each time.

282. Since learning of the Data Breach, Plaintiff Perez has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, self-monitoring his accounts, driving to the bank to obtain a new payment card from Navy Federal, and dealing with an increase in spam calls and texts, all as a result of his PII and PHI being exposed in the Data Breach. Since March 2023, he has spent approximately five to ten minutes each day reviewing his accounts for

fraudulent activity. He also spent time driving to and from his bank, which is 20 miles round trip, twice to obtain a new card from Navy Federal Credit Union. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Perez intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

283. As a result of the Data Breach, Plaintiff Perez spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

284. Plaintiff Perez has also experienced an increase of other spam calls, text messages and emails after the Data Breach.

285. In addition, Plaintiff Perez has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

286. Plaintiff Perez plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

287. Additionally, Plaintiff Perez is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured

source. Plaintiff Perez stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

288. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Perez would take, and continue to take, necessary measures to protect his PII and PHI.

289. Plaintiff Perez has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

290. Plaintiff Perez has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII and PHI. Plaintiff Perez has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

291. Plaintiff Perez has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

292. As a direct and traceable result of the Data Breach, Plaintiff Perez will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Mark Salzano's Experience

293. Plaintiff Salzano greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Salzano took reasonable steps to maintain the confidentiality of his PII and PHI.

294. Plaintiff Salzano received a letter dated March 14, 2023 from Defendant ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name, date of birth, Social Security number, and health insurance information.

295. Although ILS discovered the Data Breach in July 2022, Plaintiff Salzano was not notified of the Data Breach until in or around March 2023.

296. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Salzano faces, Defendant ILS offered him a one-year subscription to a credit monitoring service. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

297. Since learning of the Data Breach, Plaintiff Salzano has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, freezing his credit, self-monitoring his accounts, reviewing "dark web" notifications from credit monitoring services, and dealing with an increase in spam calls, texts, and emails, all as a result of his PII and PHI being exposed in the Data Breach. Since March 2023, he has spent approximately thirty minutes each week dealing with the consequences of the Data Breach. Plaintiff spent this time at ILS's direction. In the notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements,

explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Salzano intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

298. As a result of the Data Breach, Plaintiff Salzano spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

299. Plaintiff Salzano has also experienced an increase of other spam calls, text messages and emails after the Data Breach.

300. In addition, Plaintiff Salzano has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

301. Plaintiff Salzano plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

302. Additionally, Plaintiff Salzano is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Salzano stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

303. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Salzano would take, and continue to take, necessary measures to protect his PII and PHI.

304. Plaintiff Salzano has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

305. Plaintiff Salzano has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his/her PII and PHI. Plaintiff Salzano has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

306. Plaintiff Salzano has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, especially his Social Security number, in combination with his name, date of birth, and health insurance information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

307. As a direct and traceable result of the Data Breach, Plaintiff Salzano will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Ernest Scoggan's Experience

308. As a condition of receiving services from his medical provider or insurer, Plaintiff Scoggan was required to provide his PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

309. Plaintiff Scoggan greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Scoggan took reasonable steps to maintain the confidentiality of his PII and PHI.

310. Plaintiff Scoggan received a letter dated March 14, 2023 from ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name, date of birth, and health insurance information.

311. Although ILS discovered the Data Breach in July 2022, Plaintiff Scoggan was not notified of the Data Breach until in or around March 2023.

312. Shortly after receiving the Notice letter from ILS, Plaintiff Scoggan was contacted by a scammer posing as a streaming service provider. The individual obtained Plaintiff Scoggan's debit card number, and he attempted to ascertain Plaintiff Scoggan's driver's license number and additional information during a phone call with Plaintiff Scoggan. As a result, Plaintiff Scoggan immediately notified his bank and cancelled the debit card. He was required to spend several hours resolving the issues. Plaintiff Scoggan believes the targeted phishing attempt is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and he has never experienced similar fraudulent activity in the past.

313. Since learning of the Data Breach, Plaintiff Scoggan has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with

the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts, all as a result of his PII and PHI being exposed in the Data Breach. Since March 2023, he has spent approximately 30-40 hours reviewing his account statements and exploring ways to safeguard his personal information. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Scoggan intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

314. As a result of the Data Breach, Plaintiff Scoggan spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

315. Plaintiff Scoggan has also experienced an increase of other spam calls, text messages and emails after the Data Breach. He has received constant spam and phishing attempts since the Data Breach, and he believes this is a result of the Data Breach based on the timing and dramatic increase.

316. In addition, Plaintiff Scoggan, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the way ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

317. Plaintiff Scoggan plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

318. Additionally, Plaintiff Scoggan is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Scoggan stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

319. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Scoggan would take, and continue to take, necessary measures to protect his PII and PHI.

320. Plaintiff Scoggan has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

321. Plaintiff Scoggan has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII and PHI. Plaintiff Scoggan has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

322. Plaintiff Scoggan has suffered imminent and impending injury arising from actual fraud, the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, especially his name, date of birth, and health

insurance information, which is now in the hands of cybercriminals and other unauthorized third parties.

323. As a direct and traceable result of the Data Breach, Plaintiff Scoggan will continue be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Ryan Smith's Experience

324. As a condition of receiving services from his medical provider or insurer, Plaintiff Smith was required to provide his PII and PHI, which was then obtained by ILS, entered into ILS's database, and maintained by ILS.

325. Plaintiff Smith was insured by Kaiser. Kaiser is one of the nation's largest health plans, serving almost 13 million members, including in California, where it is based. It operates 39 hospitals and more than 620 medical offices.

326. ILS announced that it partnered with Kaiser to build a California provider network. Kaiser also has a facility called Independent Living Systems-Enhanced Care Management in California, offering Medi-Cal managed care. Medi-Cal is California's Medicaid program. Kaiser offers Medicaid in eight states and DC, including in multiple counties in California.

327. Plaintiff Smith's PHI from Kaiser was, on information and belief, transferred to ILS and became part of its Data Breach, even though Plaintiff Smith did not otherwise have any connection to ILS but nonetheless received the ILS Notice.

328. Plaintiff Smith greatly values his privacy and PII and PHI, especially when obtaining medical services. Prior to the Data Breach, Plaintiff Smith took reasonable steps to maintain the confidentiality of his PII and PHI.

329. Plaintiff Smith received a letter dated March 14, 2023 from ILS informing him of the Data Breach. The letter stated that unauthorized actors gained access to, and acquired information from, ILS's computer systems that contained his name, date of birth, Social Security number, and health insurance policy number.

330. Although ILS discovered the Data Breach in July 2022, Plaintiff Smith was not notified of the Data Breach until in or around March 14, 2023.

331. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Smith faces, ILS offered him a one-year subscription to a credit monitoring service. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

332. Since the Data Breach, Plaintiff Smith has received notification from McAfee that his personal information has been found on the dark web.

333. Since learning of the Data Breach, Plaintiff Smith has spent additional time dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including time spent researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts and credit reports, all as a result of his PII and PHI being exposed in the Data Breach. Since March 2023, he has spent approximately one hour each week reviewing his accounts online and monitoring his credit reports. Plaintiff spent this time at ILS's direction. In the Notice letter Plaintiff received, ILS directed Plaintiff to spend time mitigating his losses by "review[ing] your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately." Plaintiff Smith intends to spend additional time and effort taking steps to protect his PII and PHI in the future.

334. As a result of the Data Breach, Plaintiff Smith spent valuable time he otherwise would have spent on other obligations. This is time that has been lost forever and cannot be recaptured.

335. Plaintiff Smith has also experienced an increase of other spam calls, text messages and emails after the Data Breach.

336. In addition, Plaintiff Smith, has suffered and will continue to suffer as a result of the Data Breach and has increased concerns for the loss of his privacy which he would not have incurred had ILS implemented the necessary and proper safeguards to protect Plaintiff's PII and PHI from theft. Plaintiff's increased concerns have been compounded by the fact that ILS has not been forthright with information about the Data Breach, the manner in which ILS obtained Plaintiff's PII and PHI, and ILS's failure to notify impacted individuals for over eight months.

337. Plaintiff Smith plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his financial and other accounts for any unauthorized activity, and addressing any issues that may arise.

338. Additionally, Plaintiff Smith is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source. Plaintiff Smith stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

339. The PII and PHI that was accessed and acquired by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Smith would take, and continue to take, necessary measures to protect his PII and PHI.

340. Plaintiff Smith has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

341. Plaintiff Smith has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his/her PII and PHI. Plaintiff Smith has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

342. Plaintiff Smith has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII and PHI resulting from the compromise of his PII and PHI, especially his Social Security number, in combination with his name and date of birth, along with his sensitive medical information, which PII and PHI is now in the hands of cybercriminals and other unauthorized third parties.

343. As a direct and traceable result of the Data Breach, Plaintiff Smith will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiffs and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

344. Plaintiffs and Class Members suffered injury from the misuse of their PII and PHI that can be directly traced to ILS.

345. The ramifications of ILS's failure to keep Plaintiffs' and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license

number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

346. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[29]

347. As a result of ILS's failures to prevent – and to timely detect – the Data Breach, Plaintiffs and Class Members suffered and will continue to suffer damages, including monetary losses and lost time. More specifically, they have suffered or are at an increased risk of suffering:

(a) The loss of the ability to control how their PII and PHI is used;

(b) The diminution in value of their PII and PHI;

(c) The compromise and continuing publication of their PII and PHI;

(d) Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

(e) Lost opportunity costs and lost wages associated with the time and effort expended 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 and fraud;

(f) Delay in receipt of tax refund monies;

(g) Unauthorized use of stolen PII and PHI; and

[29] *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, JAVELIN (Feb. 20, 2013), https://javelinstrategy.com/press-release/more-12-million-identity-fraud-victims-2012-according-latest-javelin-strategy-research#:~:text=The%20study%20found%2012.6%20million,to%20be%20the%20most%20damaging.

(h) The continued risk to their PII and PHI, which remains in the possession of ILS and is subject to further breaches so long as ILS fails to undertake the appropriate measures to protect the PII and PHI in their possession.

348. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII and PHI can be worth up to $1,000.00 depending on the type of information obtained.[30]

349. The value of Plaintiffs' and the proposed Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee.

350. It can take victims years to spot or identify PII and PHI theft, giving criminals plenty of time to milk that information for cash.

351. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.[31]

---

[30] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[31] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information one has on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground*

352. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

353. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other Class Members' stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

354. According to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

355. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." ILS did not rapidly report to Plaintiffs and the Class that their PII and PHI had been stolen.

Stolen From Texas Life Insurance Firm, KREBS ON SECURITY (Sept. 18, 2014), https://krebsonsecurity.com/tag/fullz/.

356. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

357. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors. For example, Plaintiffs Geleng, Gomez, Jensen, and McMullen, each experienced identity fraud as a result of the Data Breach and have spent extensive time and energy resolving these issues and monitoring their accounts.

358. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII and PHI. To protect themselves, Plaintiffs and the Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

359. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated, "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[32]

[32] *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

360. An active and robust consumer marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[33] The data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[34,35] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[36]

361. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

362. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[37] According to the FTC, data security requires:

---

[33] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[34] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[35] Datacoup, *The personal data revolution: It's time to capture, control and profit from your personal data*, https://datacoup.com/ (last visited Nov. 10, 2023).

[36] World Data Exchange, https://worlddataexchange.com/ (last visited Nov. 10, 2023).

[37] *Start With Security, A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 21, 2022).

(a) encrypting information stored on computer networks; (b) retaining payment card information only as long as necessary; (c) properly disposing of personal information that is no longer needed; (d) limiting administrative access to business systems; (e) using industry-tested and accepted methods for securing data; (f) monitoring activity on networks to uncover unapproved activity; (g) verifying that privacy and security features function properly; (h) testing for common vulnerabilities; and (i) updating and patching third-party software.[38]

363. According to the FTC, unauthorized PII and PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[39] The FTC treats 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(a) of the FTC Act.

364. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Servs., Inc.*, No. C-4326, ¶7 (FTC June 15, 2011) ("[the defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶7 (FTC Mar. 7, 2006) ("[the defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (FTC Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify

---

[38] *Id.*

[39] *See Taking Charge, What to Do if Your Identity Is Stolen*, FED. TRADE COMM'M, at 3 (Jan. 2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen.

checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (FTC May 20, 2010) ("[the Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. ILS thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII and PHI.

365. The healthcare industry is a prime target for data breaches.

366. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[40] The next year, that number increased by nearly 45%.[41] The following year the healthcare sector was

[40] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RES. CTR. (Jan. 20, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"].

[41] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, IDENTITY THEFT RES. CTR. (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"].

the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach.[42]

367. Data breaches within the healthcare industry continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[43]

368. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[44] Indeed, when compromised, healthcare-related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[45] Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the customers were never able to

---

[42] *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RES. CTR. (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[43] *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFO. & MGMT. SYS. SOC'Y, INC. (Feb. 8, 2019), https://bit.ly/3LJqUr6.

[44] *2018 End-of-Year Data Breach Report*, IDENTITY THEFT RES. CTR. (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[45] Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), https://cnet.co/33uiV0v.

resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[46]

369. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers."[47]

370. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

371. Charged with handling highly sensitive PII and PHI including healthcare information, financial information, and insurance information, ILS knew or should have known the importance of safeguarding the PII and PHI that was entrusted to it. ILS also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on ILS's customers' patients as a result of a

---

[46] *Id.*

[47] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08.

breach. ILS nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

372. ILS disclosed the PII and PHI of Plaintiffs and Class Members for criminals to use in the conduct of criminal activity. Specifically, ILS opened, disclosed, and failed to adequately protect the PII and PHI of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII and PHI.

373. ILS's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII and PHI of Plaintiffs and potentially millions of Class Members to unscrupulous operators, con artists, and outright criminals.

374. ILS's failure to properly and timely notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

375. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated (the "Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

376. Plaintiffs propose the following nationwide class definition, subject to amendment as appropriate:

> All persons residing in the United States whom Defendant sent a Notice of the Data Breach (the "Class").

377. Plaintiffs propose the following State Classes, subject to amendment as appropriate:

> All persons residing in the State of Florida whom Defendant sent a Notice of the Data Breach (the "Florida Class").
>
> All persons residing in the State of California whom Defendant sent a Notice of the Data Breach (the "California Class").
>
> All persons residing in the State of Colorado whom Defendant sent a Notice of the Data Breach (the "Colorado Class").
>
> All persons residing in the State of Illinois whom Defendant sent a Notice of the Data Breach (the "Illinois Class").
>
> All persons residing in the State of South Carolina whom Defendant sent a Notice of the Data Breach (the "South Carolina Class").
>
> All persons residing in the State of Hawaii whom Defendant sent a Notice of the Data Breach (the "Hawaii Class").
>
> All persons residing in the State of Oregon whom Defendant sent a Notice of the Data Breach (the "Oregon Class").[48]

378. The Class defined above is readily ascertainable from information in ILS's possession. Thus, identification of Class Members will be reliable and administratively feasible.

379. Excluded from the Class are: (a) any judge or magistrate presiding over this action and members of their families; (b) ILS, ILS's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which ILS or their parent has a controlling interest, and their current or former officers and directors; (c) persons who properly execute and file a timely request for exclusion from the Class; (d) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (e) Plaintiffs' counsel and ILS's counsel; (f) members of the jury; and (g) the legal representatives, successors, and assigns of any such excluded persons.

[48] For ease of reference, the Class and State Classes are referred to herein as the "Class" or "Class Members."

380. Plaintiffs reserve the right to amend or modify the Class definition(s) – including potential Subclasses – as this case progresses.

381. Plaintiffs and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

382. ***Numerosity***. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of millions individuals whom Defendant sent a Notice of the Data Breach.

383. ***Commonality***. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, but are not limited to:

(a) whether ILS unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII and PHI;

(b) whether ILS failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(c) whether ILS's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the HIPAA;

(d) whether ILS's data security systems prior to and during the Data Breach were consistent with industry standards;

(e) whether ILS owed a duty to Class Members to safeguard their PII and PHI;

(f) whether ILS breached its duty to Class Members to safeguard their PII and PHI;

(g) whether ILS knew or should have known that its data security systems and monitoring processes were deficient;

(h) whether ILS should have discovered the Data Breach earlier;

(i) whether ILS took reasonable measures to determine the extent of the Data Breach after it was discovered;

(j) whether ILS unreasonably delayed notifying Plaintiffs and Class Members of the Data Breach;

(k) whether ILS's method of informing Plaintiffs and Class Members of the Data Breach was unreasonable;

(l) whether ILS's conduct was negligent;

(m) whether Plaintiffs and Class Members were injured as a proximate cause or result of the Data Breach;

(n) whether Plaintiffs and Class Members suffered legally cognizable damages as a result of ILS's misconduct;

(o) whether ILS breached implied contracts with Plaintiffs and Class Members;

(p) whether ILS was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members; and

(q) whether Plaintiffs and Class Members are entitled to damages and/or injunctive relief.

384. ***Typicality***. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, received a Notice of the Data Breach from Defendant that their PII and/or PHI was compromised in the Data Breach. Moreover, all

Plaintiffs and Class Members were subjected to ILS's uniformly illegal and impermissible conduct.

385. ***Adequacy of Representation***. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating complex class actions. Plaintiffs has no interests that conflict with, or are antagonistic to, those of the Class.

386. ***Predominance***. ILS has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way. The common issues arising from ILS's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

387. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for ILS. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

388. The litigation of the claims brought herein is manageable. ILS'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 prosecuting this lawsuit as a class action.

389. Adequate notice can be given to Class Members directly using information maintained in ILS's records.

390. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

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

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS AND ALTERNATIVE STATE CLASSES

COUNT I

NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Classes)

392. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

393. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class or alternatively, the State Classes.

394. ILS owed several common law duties to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII and PHI within its control from being accessed, compromised, exfiltrated, and stolen by criminal third parties in foreseeable cyber-crimes.

395. First, a common law duty arose by the foreseeability of the cyber-crimes. Due to the ongoing threat and highly publicized cyber-attacks businesses like ILS that acquire and store PII and PHI, ILS was on notice of the substantial and foreseeable risk of a cyber-attack on its systems, and that Plaintiffs and Class Members would be harmed if ILS did not protect Plaintiffs' and Class Members' PII and PHI from threat actors.

396. ILS knew or should have known that its systems were vulnerable to unauthorized access and exfiltration by criminal third parties. ILS knew, or should have known, of the importance of safeguarding Plaintiffs' and Class Members' PII and PHI – including Social Security number, taxpayer identification number, medical information, and health insurance information. ILS further knew or should have known of the foreseeable consequences and harm to Plaintiffs and Class Members, if ILS's data security system and network were breached – including, specifically, the risk of identity theft and related costs imposed on Plaintiffs and Class Members as a result of a data breach. ILS knew or should have known about these risk and dangers to Plaintiffs and Class Members and taken steps to strengthen its data, information technology, and email handling systems accordingly.

397. Second, by obtaining, collecting, using, retaining, and deriving benefits from Plaintiffs' and Class Members' PII and PHI, Defendant assumed the legal duty to protect Plaintiffs' and Class Members' PII and PHI from foreseeable cyber-crimes.

398. Third, ILS's duty to use reasonable data security measures arose as a result of the special relationship that existed between ILS and the Plaintiffs and Class Members. The special relationship arose because ILS received Plaintiffs' and Class Members' confidential data as part its provision of payer and administrative services to healthcare providers and organizations. ILS

was in the sole position to ensure that it had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

399. Finally, ILS's duties arose by statute under Section 5 of the FTC Act, 15 U.S.C. §45, which prohibits "unfair or deceptive acts or practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of ILS's duty.

400. ILS breached its respective common law and statutory duties by failing to provide data security consistent with industry standards to ensure that its systems and networks adequately protected the PII and PHI it had been entrusted against foreseeable cyber-crimes. ILS did not use reasonable security procedures and practices appropriate for the nature of the sensitive information it was maintaining, causing Plaintiffs' and Class Members' PII and PHI to be exposed. As a result, ILS increased the risk to Plaintiffs and Class Members that their PII and PHI would be compromised and stolen in a cyber-crime.

401. Plaintiffs' and Class Members' PII and PHI would not have been compromised in the Data Breach but for ILS's wrongful and negligent breach of its duties.

402. Neither Plaintiffs nor, upon information and belief, the other Class Members contributed to the Data Breach or subsequent misuse of their PII and PHI as described in this Complaint.

403. ILS breached its obligations to Plaintiffs and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Upon information and belief, ILS could have prevented this Data Breach by encrypting,

or adequately encrypting, or otherwise protecting their equipment and computer files containing Plaintiffs' and Class Members' PII and PHI.

404. Upon information and belief, ILS's negligent conduct also includes, but is not limited to, one or more of the following acts and omissions:

(a) failing to maintain and update an adequate data security system to reduce the risk of data breaches;

(b) failing to adequately train employees to protect consumers' PII and PHI;

(c) failing to adequately monitor, evaluate, and ensure the security of its network and systems;

(d) failing to properly monitor its own data security systems for existing intrusions;

(e) failing to comply with the minimum FTC guidelines for cybersecurity, in violation of the FTC Act;

(f) failing to adhere to industry standards for cybersecurity;

(g) failing to encrypt or adequately encrypt the PII and PHI;

(h) failing to implement reasonable data retention policies; and

(i) was otherwise negligent.

405. Furthermore, ILS was plainly aware that it should destroy any PII and PHI that it no longer needed to provide payer and administrative services to its former clients, or at least should have ensured extra precautions were taken to secure such PII and PHI since, under such circumstances, there was effectively no longer a "legitimate business 'need to know'" for accessing it.

406. As a direct and proximate result of Defendant's negligent acts and/or omissions, Plaintiffs' and Class Members' PII and PHI was compromised, and they are all at a high risk of identity theft and financial fraud for many years to come. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the risk of future identity theft; (b) loss of time and loss of productivity incurred mitigating the risk of future identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of PII and PHI; and (f) the continued risk to their PII and PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

407. Plaintiffs seek to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose PII and PHI were compromised as a result of the Data Breach. Plaintiffs seek compensatory damages for loss of time, opportunity costs, out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

408. Accordingly, Plaintiffs, individually and on behalf of all those similarly situated, seek an Order awarding damages in an amount to be determined at trial.

COUNT II

NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Classes)

409. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

410. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class or alternatively, the State Classes.

411. The FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as ILS, of failing to use reasonable measures to protect PII. 15 U.S.C. §45(a)(1).

412. The FTC publications and orders described above also form part of the basis of ILS's duty in this regard.

413. ILS violated the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards. ILS's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as ILS, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

414. ILS's violations of the FTC Act, as interpreted by the FTC to include a duty to employ adequate and reasonable data security measures, constitute negligence per se.

415. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

416. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

417. Additionally, Defendant is an entity or business associate covered by the HIPAA (45 C.F.R. §160.102) and as such is required to comply with the HIPAA Privacy Rule and Security 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.

418. The HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. §164.530(c)(1). The HIPAA also requires covered entities' business associates to appropriately safeguard the protected health information they receive or create on behalf of covered entities. 45 C.F.R. §§164.502(e), 164.504(e), 164.532(d)-(e). The PII and PHI at issue in this case constitutes "protected health information" within the meaning of the HIPAA.

419. Defendant constitutes either a "covered entity" or a "business associate" within the meaning of the HIPAA.

420. HIPAA further requires Defendant to disclose the unauthorized access and theft of the PII and PHI to Plaintiffs and the Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII and PHI. *See* 45 C.F.R. §§164.404, 164.406, 164.410.

421. Defendant violated the HIPAA by failing to reasonably protect Plaintiffs' and Class Members' PII and PHI, as described herein.

422. Defendant's violations of the HIPAA constitute negligence *per se*.

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

424. The harm that occurred as a result of the Data Breach is the type of harm the HIPAA was intended to guard against.

425. As a direct and proximate result of Defendant's negligent *per se* acts and/or omissions, Plaintiffs' and Class Members' PII and PHI was compromised, and they are all at a high risk of identity theft and financial fraud for many years to come. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the risk of future identity theft; (b) loss of time and loss of productivity incurred mitigating the risk of future identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of PII and PHI; and (f) the continued risk to their PII and PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and PHI.

426. Plaintiffs seek to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose PII and PHI were compromised as a result of the Data Breach. Plaintiffs seek compensatory damages for loss of time, opportunity costs, out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

427. Accordingly, Plaintiffs, individually and on behalf of all those similarly situated, seek an Order awarding damages in an amount to be determined at trial.

COUNT III

BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Classes)

428. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

429. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class or alternatively, the State Classes.

430. ILS's Privacy Policy is an agreement between ILS and persons who provided their PII to ILS, including Plaintiffs and Class Members.

431. ILS's Privacy Policy provides certain protections, including that:

(a) "We are required by law to maintain the privacy and security of your protected health information. We implement a variety of security measures to maintain the safety of your personal information when you access your personal information."

(b) ILS does not disclose your PII to unauthorized parties.

(c) "We will promptly notify you if a breach occurs that may have compromised the privacy or security of your information."[49]

432. Plaintiffs and Class Members on the one hand and ILS on the other formed a contract when Plaintiffs and Class Members provided valuable consideration – including monies and their PII and PHI – to ILS subject to the Privacy Policy.

433. Plaintiffs and Class Members fully performed their obligations under the contract with ILS.

434. ILS breached its agreement with Plaintiffs and Class Members by failing to protect their PII and PHI. Specifically, ILS: (a) failed to use reasonable measures to protect that information; and (b) disclosed that information to unauthorized third parties, in violation of the agreement.

[49] *Privacy Policy*, *supra* note 7.

435. As a direct and proximate result of these breaches of contract, Plaintiffs and Class Members sustained actual losses and damages as described in detail above, including, but not limited to, that they did not get the benefit of the bargain for which they rendered valuable consideration to ILS for its services.

COUNT IV

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Classes)

436. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

437. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class or alternatively, the State Classes.

438. This Count is pleaded in the alternative to the breach of express contract count above.

439. Defendant required Plaintiffs and the Class to provide and entrust their PII and PHI as a condition of obtaining services from ILS.

440. Plaintiffs and the Class paid money to ILS in exchange for goods and services, as well as ILS's promises to protect their protected health information and other PII and PHI from unauthorized disclosure.

441. ILS promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' PII and PHI would remain protected.

442. Through its course of conduct, ILS, Plaintiffs, and Class Members entered into implied contracts with ILS by which ILS agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if its data had been breached and compromised or stolen.

443. ILS solicited and invited Plaintiffs and Class Members to provide their PII and PHI and financial information as part of ILS's regular business practices. Plaintiffs and Class Members accepted ILS's offers and provided their PII and PHI to ILS.

444. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII and PHI and financial information to ILS, in exchange for, amongst other things, the protection of their PII and PHI and financial information.

445. Plaintiffs and Class Members fully performed their obligations under the implied contracts with ILS.

446. ILS breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII and PHI and financial information and by failing to provide timely and accurate notice to them that their PII and PHI and financial information was compromised as a result of the Data Breach.

447. The failure to meet its confidentiality and privacy obligations resulted in ILS providing goods and services to Plaintiffs and Class Members that were of a diminished value.

448. As a direct and proximate result of ILS's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT V

UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the State Classes)

449. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

450. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class or, alternatively, the State Classes in the alternative to all other Counts alleged herein.

451. This Count is pleaded in the alternative to the breach of express and breach of implied contract counts above.

452. For years and continuing to today, ILS's business model has depended upon it being entrusted with customers' PII and PHI. Trust and confidence are critical and central to the services provided by ILS in the healthcare industry. Unbeknownst to Plaintiffs and absent Class Members, however, ILS did not secure, safeguard, or protect Plaintiffs' and Class Members' PII and PHI and employed deficient security procedures and protocols to prevent unauthorized access to their PII and PHI. ILS's deficiencies described herein were contrary to their security obligations under statutory, regulatory, and common law.

453. Plaintiffs and Class Members received services from ILS, directly or indirectly, and ILS was provided with, and allowed to collect and store, their PII and PHI on the mistaken belief that ILS complied with its duties to safeguard and protect PII and PHI. Upon information and belief, putting their short-term profit ahead of safeguarding PII and PHI, and unbeknownst to Plaintiffs and Class Members, ILS knowingly sacrificed data security in an attempt to save money.

454. Upon information and belief, ILS knew that the manner in which it maintained and transmitted customer PII and PHI violated industry standards and its fundamental duties to Plaintiffs and Class Members by neglecting well-accepted security measures to ensure confidential

information was not accessible to unauthorized access. ILS had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

455. ILS had within its exclusive knowledge, and never disclosed, that it had failed to safeguard and protect Plaintiffs' and Class Members' PII and PHI. This information was not available to Plaintiffs, Class Members, or the public at large.

456. ILS also knew that Plaintiffs and Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, medical, and other PII and PHI.

457. Plaintiffs and Class Members did not expect that ILS would knowingly insecurely maintain and hold their PII and PHI when that data was no longer needed to facilitate a business transaction or other legitimate business reason. Likewise, Plaintiffs and Class Members did not know or expect that ILS would employ substantially deficient data security systems and fail to adequately protect the entrusted PII and PHI.

458. Had Plaintiffs and Class Members known about ILS's deficiencies and ineffective and substandard data security systems, Plaintiffs and Class Members would not have paid, directly or indirectly, for ILS's services.

459. By withholding the facts concerning the defective security and protection of customer PII and PHI, ILS put its own interests ahead of Plaintiffs and Class Members who placed their trust and confidence in ILS and benefitted itself to the detriment of Plaintiffs and Class Members.

460. As a result of its conduct as alleged herein, ILS sold more services than it otherwise would have, and was able to charge more for ILS's services than it otherwise could have. ILS was

unjustly enriched by charging for and collecting for those services that it would not have obtained to the detriment of Plaintiffs and Class Members.

461. It would be inequitable, unfair, and unjust for ILS to retain these wrongfully obtained fees and benefits. ILS's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

462. As a result, Plaintiffs and Class Members paid for services, directly or indirectly, that they would not have paid for had Defendant disclosed the inadequacy of its data security practices.

463. Alternatively, ILS should be ordered to disgorge the profits it reaped as a result of its failure to adequately fund adequate and legally required data security to protect PII and PHI.

464. Plaintiffs and each member of the proposed Class are each entitled to restitution and/or non-restitutionary disgorgement in the amount by which ILS were unjustly enriched, to be determined at trial.

COUNT VI

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §501.201, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Florida Class)

465. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

466. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class or, alternatively, the Florida Class.

467. This cause of action is brought pursuant the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), which, pursuant to Fla. Stat. §501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business

enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

468. ILS's offers, provisions, and sales or services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§501.201-213.

469. Plaintiffs and Class Members are "individual[s]," and are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. §501.203(7).

470. ILS provided payer and administrative services to healthcare providers and organizations on Plaintiffs' and Class Members' behalf.

471. ILS offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. §501.203.

472. Plaintiffs and Class Members paid for or otherwise availed themselves and received services from ILS, primarily for personal, family, or household purposes.

473. ILS engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the provision of payer and administrative services to healthcare providers and organizations on behalf or for the benefit of Plaintiffs and Class Members.

474. ILS's acts, practices, and omissions were done in the course of ILS's business of offering and providing payer and administrative services to healthcare providers and organizations throughout Florida and the United States.

475. The unfair, unconscionable, and unlawful acts and practices of ILS alleged herein, and in particular the decisions regarding data security, emanated and arose – with respect to Florida Class Members, within the State of Florida, within the scope of the FDUTPA.

476. ILS, operating in Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. §501.204(1), including, but not limited to, the following:

(a) failing to implement and maintain reasonable and adequate computer systems and data security practices to safeguard customer PII and PHI;

(b) failing to protect the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI;

(c) continuing to accept and store customer PII and PHI after ILS knew or should have known of the security vulnerabilities that were exploited in the Data Breach;

(d) continuing to accept and store customer PII and PHI after ILS knew or should have known of the Data Breach and before it allegedly remediated the Data Breach; and

(e) continuing to store and maintain the PII and PHI of former customers when ILS had no legitimate business need to do so. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. §41, *et seq.*, and the FDUTPA, Fla. Stat. §501.171(2).

477. ILS knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and PHI and that the risk of a data breach or theft was high.

478. Plaintiffs have standing to pursue this claim because as a direct and proximate result of ILS's violations of the FDUTPA, Plaintiffs and Class Members have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that ILS's acts or practices violate the FDUTPA. *See* Fla. Stat. §501.211(a).

479. Plaintiffs also have standing to pursue this claim because, as a direct result of ILS's knowing violation of the FDUTPA, Plaintiffs and the Class are at a present and continuing risk of identity theft. ILS still possesses Plaintiffs' and the Class Members' PII and PHI, and that PII and PHI has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of identity theft for Plaintiffs and all Class Members.

480. Plaintiffs and Class Members are entitled to injunctive relief to protect them from the substantial and imminent risk of identity theft, including, but not limited to:

(a) ordering that ILS engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

(b) ordering that ILS engage third-party security auditors and internal personnel to run automated security monitoring;

(c) ordering that ILS audit, test, and train security personnel regarding any new or modified procedures;

(d) ordering that ILS segment customer data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

(e) ordering that ILS purge, delete, and destroy customer PII and PHI not necessary for its provisions of services in a reasonably secure manner;

(f) ordering that ILS conduct regular database scans and security checks;

(g) ordering that ILS routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

(h) ordering ILS to meaningfully educate customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps present and former customers should take to protect themselves.

481. Plaintiffs also have standing to pursue this claim because as a direct and proximate result of ILS's violations of the FDUTPA, they suffered actual damages in the form of actual identity theft and lost time and money devoted to dealing with these.

482. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members, and the public from ILS's unfair methods of competition and unfair, unconscionable, and unlawful practices. ILS's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

483. The above unfair, unconscionable, and unlawful practices and acts by ILS were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

484. ILS's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices and described herein were negligent, knowing and willful, and/or wanton and reckless.

485. Plaintiffs and Class Members seek relief under the FDUTPA, Fla. Stat. §501.201, *et seq*., including, but not limited to, damages, restitution, a declaratory judgment that ILS's actions

and/or practices violate the FDUTPA; injunctive relief enjoining ILS, their employees, parents, subsidiaries, affiliates, executives, and agents from violating the FDUTPA; ordering that ILS engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors; ordering that ILS engage third-party security auditors and internal personnel to run automated security monitoring; ordering that ILS audit, test, and train security personnel regarding any new or modified procedures; ordering that ILS segment customer data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system; ordering that ILS purge, delete, and destroy customer PII and PHI not necessary for its provisions of services in a reasonably secure manner; ordering that ILS conduct regular database scans and security checks; ordering that ILS routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; ordering ILS to meaningfully educate customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps current and former customers should take to protect themselves; attorneys' fees and costs; and any other just and proper relief.

CLAIMS ON BEHALF OF THE ALTERNATIVE CALIFORNIA CLASS

COUNT VII

CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §1798.100, *et seq.*
(On Behalf of Plaintiffs Gomez, Gutierrez, Perez, Salzano, Scoggan, and Smith (the "California Plaintiffs") and the California Class)

486. California Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

487. Plaintiffs Gomez, Gutierrez, Perez, Salzano, Scoggan, and Smith (for the purposes of this Count, "California Plaintiffs") bring this claim on behalf of themselves and the California Class.

488. California Plaintiffs and California Class Members are residents of California.

489. Defendant is a corporation organized or operated for the profit or financial benefit of its owners. Defendant collects consumers' PII and PHI (for the purposes of this Count, "Personal Information") as defined in the California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code §1798.140(v)(1).

490. Defendant violated Section 1798.150 of the CCPA by failing to prevent California Plaintiffs' and California Class Members' nonencrypted Personal Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

491. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect California Plaintiffs' and California Class Members' Personal Information. As detailed herein, Defendant failed to do so.

492. As a direct and proximate result of Defendant's acts, California Plaintiffs' and California Class Members' Personal Information, including names, Social Security numbers, and medical information, and other sensitive medical records, was subjected to unauthorized access and exfiltration, theft, or disclosure.

493. California Plaintiffs and California Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter properly safeguards customer Personal Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customer Personal Information, including California Plaintiffs' and California Class Members' Personal Information. California Plaintiffs and California Class Members have an interest in ensuring that their Personal Information is reasonably protected.

494. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

495. In compliance with the statute, on October 17, 2023, counsel for Plaintiffs Gomez, Perez, and Salzano, provided written notice via certified mail to Defendant at its principal place of business of the intent to pursue claims under the CCPA and an opportunity for Defendant to cure. Plaintiffs' written notice set forth the violations of Defendant's duty to implement and maintain reasonable security procedures and practices alleged in this Complaint. Additionally, on March 23, 2023, counsel for Plaintiff Gomez provided written notice via certified mail to Defendant at its principal place of business of the intent to pursue claims under the CCPA and an opportunity for Defendant to cure.

496. To date, Defendant has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notices sent by Plaintiffs' counsel.

497. California Plaintiffs and the California Class seek actual damages, as well as all monetary and non-monetary relief allowed by law, including statutory damages; actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VIII

CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code §1798.80, *et seq.*
(On Behalf of California Plaintiffs and the California Class)

498. California Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

499. Plaintiffs Gomez, Gutierrez, Perez, Salzano, Scoggan, and Smith (for the purposes of this Count, "California Plaintiffs") bring this claim on behalf of themselves and the California Class.

500. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code §1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

501. Defendant is a business that owns, maintains, and licenses PII and PHI (or "Personal Information" within the meaning of Cal. Civ. Code §§1798.80(a) and 1798.81.5(b)), about California Plaintiffs and California Class Members.

502. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code §1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." *Id*.

503. Defendant is a business that owns or licenses computerized data that includes "Personal Information" as defined by Cal. Civ. Code §1798.80.

504. California Plaintiffs' and California Class Members' Personal Information includes Personal Information as covered by Cal. Civ. Code §1798.82.

505. Because Defendant reasonably believed that California Plaintiffs' and California Class Members' Personal Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code §1798.82.

506. Defendant failed to fully disclose material information about the Data Breach, including the types of Personal Information impacted.

507. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code §1798.82.

508. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §1798.82, Plaintiffs and California Class Members suffered damages, as alleged above.

509. California Plaintiffs and California Class Members seek relief under Cal. Civ. Code §1798.84, including actual damages and injunctive relief.

COUNT IX

CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code §56, *et seq.*
(On Behalf of California and the California Class)

510. California Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

511. Defendant is a "contractor," as defined in Cal. Civ. Code §56.05(d), or "a provider of health care," as defined in Cal. Civ. Code §56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§56.10(a), (d)-(e), 56.36(b), 56.101(a)-(b).

512. Defendant is a person licensed under California under California's Business and Professions Code, Division 2. *See* Cal. Bus. Prof. Code §4000, *et seq*. ILS therefore qualifies as a "provider of health care," under the CMIA.

513. Plaintiffs Gomez, Gutierrez, Perez, Salzano, Scoggan, and Smith (for purposes of this Count, "California Plaintiffs") and the California Class are "patients," as defined in CMIA, Cal. Civ. Code §6.05(l) ("'Patient' means a natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.").

514. Defendant disclosed California Plaintiffs' and California Class Members' "medical information," as defined in CMIA, Cal. Civ. Code §56.05(i), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code §56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of ILS's employees, which allowed the hackers to see, obtain, and access California Plaintiffs' and the California Class Members' medical information.

515. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to California Plaintiffs and the Class to unauthorized persons and the breach

of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of California Plaintiffs' and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§56.06 and 56.101(a).

516. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code §56.101(b)(1)(A).

517. California Plaintiffs and the California Class were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§56.35-56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

COUNT X

CALIFORNIA UNFAIR COMPETITION ACT
Cal. Bus. & Prof. Code §17200, *et seq.*
(On Behalf of California Plaintiffs and the California Class)

518. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

519. Plaintiffs Gomez, Gutierrez, Perez, Salzano, Scoggan, and Smith (for purposes of this Count, "California Plaintiffs") bring this claim on behalf of themselves and the California Class.

520. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

521. Defendant violated Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL") by engaging in unlawful and unfair business acts and practices.

522. Defendant's "unfair" acts and practices include:

(a) Defendant failed to implement and maintain reasonable security measures to protect California Plaintiffs' and California Class Members' PII and PHI from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

(b) Defendant failed to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as alleged herein. This conduct, with little if any utility, is unfair when weighed against the harm to California Plaintiffs and California Class Members, whose PII and PHI has been compromised;

(c) Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the HIPAA, the FTC Act, 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, California's Confidentiality of Medical Information Act, Cal. Civ. Code §56, *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code §1798.100;

(d) Defendant's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as alleged above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of Defendant's grossly inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

(e) Defendant engaged in unlawful business practices by violating the HIPAA, the FTC Act 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5,

California's Confidentiality of Medical Information Act, Cal. Civ. Code §56, *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code §1798.100.

523. Defendant has engaged in "unlawful" business practices by violating multiple laws, including the HIPAA, the FTC Act, 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, California's Confidentiality of Medical Information Act, Cal. Civ. Code §56, *et seq.*, California's Consumer Privacy Act, Cal. Civ. Code §1798.100, and common law.

524. Defendant's unlawful and unfair acts and practices include:

(a) failing to implement and maintain reasonable security and privacy measures to protect California Plaintiffs' and California Class Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

(b) failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) failing to comply with common law and statutory duties pertaining to the security and privacy of California Plaintiffs' and California Class Members' PII and PHI, including duties imposed by the HIPAA and, the FTC Act, 15 U.S.C. §45, which was a direct and proximate cause of the Data Breach; and

(d) failing to provide the Notice of Data Breach required by Cal. Civ. Code §1798.82(d)(1).

525. As a direct and proximate result of Defendant's unfair and unlawful acts and practices, California Plaintiffs and California Class Members were injured and suffered monetary and non-monetary damages, as alleged herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial and medical accounts for fraudulent

activity; an increased, imminent risk of fraud and identity theft; deprivation of value of access to their PII and PHI; overpayment for Defendant's services; and the value of identity protection services made necessary by the Data Breach.

526. Defendant acted intentionally, knowingly, and maliciously to violate California's UCL, and recklessly disregarded California Plaintiffs' and California Class Members' rights.

527. California Plaintiffs and California Class Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair and unlawful business practices or use of their PII and PHI; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure §1021.5; injunctive relief; and other appropriate equitable relief.

CLAIM ON BEHALF OF THE ALTERNATIVE COLORADO CLASS

COUNT XI

COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. §6-1-101, *et seq.*
(On Behalf of Plaintiff Matthew George and Colorado Class Members)

528. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

529. Plaintiff George (for the purposes of this Count, "Plaintiff") brings this claim on behalf of himself and Colorado Class Members.

530. ILS is a "person" as defined by Colo. Rev. Stat. §6-1-102(6).

531. ILS engaged in "sale[s]" as defined by Colo. Rev. Stat. §6-1-102(10).

532. Plaintiff and Colorado Class Members, as well as the general public, are actual or potential consumers of the products and services offered by ILS or successors in interest to actual consumers.

533. ILS engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. §6-1-105(1), including:

(a) Making a false representation as to the characteristics of products and services;

(b) Representing that services are of a particular standard, quality, or grade, though ILS knew or should have known that there were another;

(c) Advertising services with intent not to sell them as advertised;

(d) Employing "bait and switch" advertising, which is advertising accompanied by an effort to sell goods, services, or property other than those advertised or on terms other than those advertised; and

(e) Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

534. ILS's deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Colorado Class Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Class Members' PII and PHI, including duties imposed by the FTC Act, 5 U.S.C. §45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Colorado Class Members' PII and PHI, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Colorado Class Members' PII and PHI; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. §45.

535. ILS's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ILS's data security and ability to protect the confidentiality of consumers' PII and PHI.

536. ILS intended to mislead Plaintiff and Colorado Class Members and induce them to rely on its misrepresentations and omissions.

537. Had ILS disclosed to Plaintiff and Colorado Class Members that its data systems were not secure and, thus, vulnerable to attack, ILS would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. ILS was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Colorado Class Members. ILS accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public.

Accordingly, Plaintiff and the Colorado Class Members acted reasonably in relying on ILS's misrepresentations and omissions, the truth of which they could not have discovered.

538. ILS acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Colorado Class Members' rights. ILS's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

539. As a direct and proximate result of ILS's deceptive trade practices, Plaintiff and Colorado Class Members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; deprivation of value of their PII and PHI; overpayment for ILS's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

540. ILS's deceptive trade practices significantly impact the public, because many members of the public are actual or potential consumers of ILS's services and the ILS Data Breach affected millions of Americans, which include members of the Colorado Class.

541. Plaintiff and Colorado Class Members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XII

COLORADO SECURITY BREACH NOTIFICATION ACT
Colo. Rev. Stat. §6-1-716, *et seq.*
(On Behalf of Plaintiff Matthew George and Colorado Class Members)

542. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

543. Plaintiff George (for the purposes of this Count, "Plaintiff") brings this claim on behalf of himself and Colorado Class Members.

544. ILS is a business that owns or licenses computerized data that includes PII as defined by Colo. Rev. Stat. §6-1-716(1)-(2).

545. Plaintiff and Colorado Class Members' PII (*e.g.*, Social Security numbers) includes "Personal Information" as covered by Colo. Rev. Stat. §6-1-716(1)-(2).

546. ILS is required to accurately notify Plaintiff and Colorado Class Members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. §6-1-716(2).

547. Because ILS was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. §6-1-716(2).

548. By failing to disclose the ILS Data Breach in a timely and accurate manner, ILS violated Colo. Rev. Stat. §6-1-716(2).

549. As a direct and proximate result of ILS's violations of Colo. Rev. Stat. §6-1-716(2), Plaintiff and Colorado Class Members suffered damages, as described above.

550. Plaintiff and Colorado Class Members seek relief under Colo. Rev. Stat. §6-1-716(4), including actual damages and equitable relief.

CLAIM ON BEHALF OF THE ALTERNATIVE HAWAII CLASS

COUNT XIII

VIOLATIONS OF HAWAII'S SECURITY BREACH NOTIFICATION ACT
Haw. Rev. Stat. §487N-1, *et seq.*
(On behalf of Plaintiff David Asato and the Hawaii Class Members)

551. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

552. Plaintiff Asato (for the purposes of this Count, "Plaintiff") brings this claim on behalf of himself and Hawaii Class Members.

553. ILS is a business that owns or licenses computerized data that includes "personal information" as defined by Haw. Rev. Stat. §487N-2(a).

554. Plaintiff and Hawaii Class Members' Private Information includes "personal information" as covered under Haw. Rev. Stat. §487N-2(a).

555. ILS is a business that owns or licenses computerized data that includes "personal information" as defined by Haw. Rev. Stat. §487N-2(a).

556. Plaintiff and Hawaii Class Members' Private Information includes "personal information" as covered under Haw. Rev. Stat. §487N-2(a).

557. ILS is required to accurately notify Plaintiff and Hawaii Class Members if it becomes aware of a breach of its data security program without unreasonable delay under Haw. Rev. Stat. §487N-2(a).

558. Because ILS was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. §487N-2(a).

559. By failing to disclose the Data Breach in a timely and accurate manner, ILS violated Haw. Rev. Stat. §487N-2(a).

560. As a direct and proximate result of ILS's violations of Haw. Rev. Stat. §487N-2(a), Plaintiff and Hawaii Class Members suffered damages and will continue to suffer damages, as described above.

561. Plaintiff and Hawaii Class Members seek relief under Haw. Rev. Stat. §487N-3(b), including actual damages.

COUNT XIV

VIOLATIONS OF HAWAII'S UNFAIR PRACTICES AND UNFAIR COMPETITION ACT
Haw. Rev. Stat. §480-1, *et seq.*
(On behalf of Plaintiff David Asato and the Hawaii Class Members)

562. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

563. Plaintiff Asato (for the purposes of this Count, "Plaintiff") brings this claim on behalf of himself and Hawaii Class Members.

564. ILS is a "person" under Haw. Rev. Stat. §480-1 because it is a corporation.

565. Plaintiff is an individual and thus a person under Haw. Rev. Stat. §480-2(e)

566. Haw. Rev. Stat. §480-2 states "[i]n construing this section, the courts and the office of consumer protection shall give due consideration to the rules, regulations, and decisions of the Federal Trade Commission and the federal courts interpreting section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. §45(a)(1)) . . ."

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

by businesses, such as ILS, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of ILS's duty in this regard.

568. Despite this, ILS failed to properly implement basic data security practices.

569. ILS's failure to employ reasonable and appropriate security measures to protect against unauthorized access to Plaintiff's and Class Members' PII and PHI, and its failure to comply with applicable industry standards, constitutes unfair acts and practices prohibited by Section 5 of the FTC Act, 15 U.S.C. §45.

570. ILS's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

571. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

572. Likewise, the harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

573. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

574. The specific negligent acts and omissions committed by ILS include, but are not limited to, the following:

(a) Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII and PHI;

(b) Failing to adequately monitor the security of their networks and systems;

(c) Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

(d) Allowing unauthorized access to Class Members' PII and PHI;

(e) Failing to detect in a timely manner that Class Members' PII and PHI had been compromised and failing to provide notice and a timely manner;

(f) Failing to remove former patients' PII and PHI it was no longer required to retain pursuant to regulations;

(g) Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

(h) Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the Data Breach.

575. ILS's misconduct and/or unfair acts had a detrimental impact on its medical competitors. By saving necessary costs that should have been spent on data security measures to ensure its patients' PII and PHI was secure, ILS's misconduct allowed it to spend money on other business-related functions instead of providing adequate data security.

576. ILS's misconduct and/or unfair acts negatively affected its competition in the healthcare industry because the misconduct reduced business expenditures for ILS as compared to its competitors that did properly safeguard their patients' PII and PHI.

577. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of ILS's inadequate security practices.

578. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

579. At all relevant times, ILS knew or reasonably should have known that its data security measures were inadequate.

580. Plaintiff and other members of the Hawaii Class reasonably and justifiably relied upon ILS to fully disclose issues concerning data security and to correct those issues once they became known to ILS.

581. Likewise, Plaintiff and members of the Hawaii Class reasonably and justifiably relied on ILS to adequately safeguard their PII and PHI, to encrypt it, and to delete or destroy it after it was no longer required to maintain it.

582. Plaintiff and Class Members and/or their health care providers would not have obtained, used, and/or consented to use ILS's services had they known of its inadequate data security practices.

583. Moreover, based on the materiality of ILS's acts and omissions, reliance may be presumed or inferred for Plaintiff and members of Hawaii Class.

584. Under Haw. Rev. Stat. §480-13, Plaintiff and members of the Hawaii Class seek injunctive relief to prevent ILS from continuing to engage in the wrongful acts and unfair and unlawful business practices described herein.

585. Plaintiff further requests an injunction requiring ILS to implement adequate and reasonable data security practices and to encrypt data that it maintains and to delete or destroy data that it is no longer required to maintain.

586. Plaintiff also seeks actual and treble damages, attorneys' fees and costs and all other remedies this Court deems proper pursuant to Haw. Rev. Stat. §480-13.

COUNT XV

VIOLATIONS OF HAWAII'S UNIFORM DECEPTIVE TRADE PRACTICES ACT
Haw. Rev. Stat. §481-3, *et seq.*
(On behalf of Plaintiff David Asato and the Hawaii Class Members)

587. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

588. Plaintiff Asato (for the purposes of this Count, "Plaintiff") brings this claim on behalf of himself and Hawaii Class Members. ILS engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. §481A-3, including:

(a) Representing that goods or services have characteristics that they do not have;

(b) Representing that goods or services are of a particular standard, quality, or grade if they are of another;

(c) Advertising goods or services with intent not to sell them as advertised; and

(d) Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

589. ILS's unfair and deceptive trade practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. §45, the HIPAA, 42 U.S.C. §1320d, and the Children's Online Privacy Protection Rule ("COPPA"), 15 U.S.C. §§6501-6505;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Class Members' Private Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. §45, the HIPAA, 42 U.S.C. §1320d, and COPPA, 15 U.S.C. §§6501-6505;

(f) Failing to timely and adequately notify Plaintiff and Hawaii Class Members of the Data Breach;

(g) Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

(h) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Class Members' Private Information;

(i) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. §45, the HIPAA, 42 U.S.C. §1320d, and COPPA, 15 U.S.C. §§6501-6505.

590. ILS's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ILS's data security and ability to protect the confidentiality of consumers' Private Information.

591. ILS's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Hawaii Class Members, that their Private Information was not exposed and misled Plaintiff and the Hawaii Class Members into believing they did not need to take actions to secure their identities.

592. The above unfair and deceptive practices and acts by ILS were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Hawaii Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

593. As a direct and proximate result of ILS's unfair, unlawful, and deceptive trade practices, Plaintiff and Hawaii Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

CLAIMS ON BEHALF OF THE ALTERNATIVE ILLINOIS CLASS

COUNT XVI

ILLINOIS PERSONAL INFORMATION PROTECTION ACT
815 Ill. Comp. Stat. §530/10(a), *et seq.*
(On Behalf of Plaintiff Katrina Berres and the Illinois Class)

594. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

595. Plaintiff Berres (for the purposes of this Count, "Plaintiff") brings this claim on behalf of herself and the Illinois Class.

596. As a corporation which handles, collects, disseminates, and otherwise deals with nonpublic PII and PHI (for the purpose of this section, "Personal Information"), Defendant is a Data Collector as defined in 815 Ill. Comp. Stat. §530/5.

597. Defendant is a Data Collector that owns or licenses computerized data that includes Personal Information. Defendant also maintains computerized data that includes Personal Information which Defendant does not own.

598. Plaintiff's and Illinois Class Members' Personal Information includes "Personal Information" as defined by 815 Ill. Comp. Stat. §530/5.

599. Defendant is required to give immediate notice of a breach of a security system to owners of Personal Information which Defendant does not own or license, including Plaintiff and Illinois Class Members, pursuant to 815 Ill. Comp. Stat. §530/10(b).

600. By failing to give immediate or even reasonably prompt notice to Plaintiff and Illinois Class Members, Defendant violated 815 Ill. Comp. Stat. §530/10(b).

601. Defendant is required to notify Plaintiff and Illinois Class Members of a breach of its data security system which may have compromised Personal Information which Defendant owns or licenses in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. §530/10(a).

602. By failing to disclose the Data Breach to Plaintiff and Illinois Class Members in the most expedient time possible and without unreasonable delay, Defendant violated 815 Ill. Comp. Stat. §530/10(a).

603. Pursuant to 815 Ill. Comp. Stat. §530/20, a violation of 815 Ill. Comp. Stat. §530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA").

604. As a direct and proximate result of Defendant's violations of 815 Ill. Comp. Stat. §530/10(a), Plaintiff and Illinois Class Members suffered damages, as alleged above.

605. Plaintiff and Illinois Class Members seek relief under 815 Ill. Comp. Stat. §510/3 for the harm they suffered because of Defendant's willful violations of 815 Ill. Comp. Stat. §530/10(a), including equitable relief, costs, and attorneys' fees.

COUNT XVII

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 Ill. Comp. Stat. §510/1, *et seq.*
(On Behalf of Plaintiff Katrina Berres and the Illinois Class)

606. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

607. Plaintiff Berres (for the purposes of this Count, "Plaintiff") brings this claim on behalf of herself and the Illinois Class.

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

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

610. The ICFA is a "regulatory and remedial statue intended to protect consumers, borrowers, and business persons against fraud, unfair methods of competition, and other unfair

and deceptive business practices." *Robinson v. Toyota Motor Credit Corp.*, 775 N.E.2d 951, 960 (Ill. 2002); *Hill v. PS Ill. Tr.*, 856 N.E.2d 560, 568 (Ill. App. Ct. 2006). It is to be liberally construed to effectuate its purpose. *Robinson*, 775 N.E.2d at 960.

611. Recovery under the ICFA may be had for unfair conduct, as well as deceptive conduct. *Robinson*, 775 N.E.2d at 960. In determining whether conduct is unfair under the ICFA, courts consider: (a) whether the practice offends public policy; (b) whether it is oppressive, immoral, unethical, or unscrupulous; and (c) whether it causes consumers substantial injury. *Boyd v. U.S. Bank, N.A.*, 787 F. Supp. 2d 747, 751 (N.D. Ill. 2011); *Duby v. Pub. Storage, Inc.*, 918 N.E.2d 265, 277 (Ill. App. Ct. 2009). A practice can be unfair without meeting all three criteria. *Id*.

612. Here, Defendant's conduct is unfair under the ICFA. First, Defendant failed to comply with applicable state and federal laws and industry standards pertaining to data security, including the HIPAA and the FTC Act for safeguarding PII and PHI. In allowing the Data Breach to occur, Defendant failed to: (a) maintain adequate data security to keep Plaintiff's and Illinois Class Members' PII and PHI from being stolen by cybercriminals; (b) properly secure and protect Plaintiff's and Illinois Class Members' PII and PHI; (c) adequately train employees to protect Plaintiff's and Illinois Class Members' PII and PHI; (d) adequately monitor its own data security systems for existing intrusions; (e) encrypt or adequately encrypt Plaintiff's and Illinois Class Members' PII and PHI; (f) timely and adequately inform Plaintiff and the Illinois Class of the Data Breach; and (g) take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Illinois Class Members' PII and PHI from further unauthorized disclosure, release, data breaches, and theft. Accordingly, Defendant's inability to safeguard Plaintiff's and Illinois Class Members' PII and PHI offends public policy.

613. Second, Defendant's conduct against Plaintiff and Illinois Class Members is oppressive in that Plaintiff and the Illinois Class had no choice but share their PII and PHI with Defendant and/or Defendant's clients. Moreover, Defendant was obligated by statutes and regulations to secure Plaintiffs and Illinois Class Members' PII and PHI, but once their PII and PHI was in Defendant's possession, they had no ability on their own to protect the PII and PHI that was provided to Defendant.

614. Third, Defendant's failure to safeguard Plaintiff's and Illinois Class Members' PII and PHI and leaving it exposed to cyber criminals and unauthorized actors constitutes a substantial injury since they are at a substantial and imminent risk of identity theft. Defendant still possesses Plaintiff's and Illinois Class Members' PII and PHI, and that PII and PHI has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of identity theft for Plaintiff and the Illinois Class. Plaintiff and the Illinois Class will have to spend the remainder of their lives at greater risk for identity theft and fraud (having to constantly monitor for the same).

615. Additionally, Defendant violated FTC guidelines by failing to: (a) promptly dispose of PII and PHI when no longer required to be stored; (b) encrypt information stored on computer networks; (c) understand vulnerabilities of its network; (d) implement policies to correct security problems; (e) use an intrusion detection system to expose a breach as soon as it occurs; (f) monitor all incoming traffic for activity indicating someone is attempting to hack the system; (g) watch for large amounts of data being transmitted from the system; and (h) have a response plan ready in the event of a breach. These failures constitute unfair acts or practices, subjecting them to an ICFA claim. 15 U.S.C. §45.

616. In sum, Defendant's numerous failures in safeguarding Plaintiff's and Illinois Class Members' PII and PHI violates the ICFA.

617. As a result, Plaintiff and the Illinois Class have suffered and will suffer substantial injury, including, but not limited to: (a) the compromise, publication, theft, and/or unauthorized use of their PII and PHI: (b) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; (c) lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and the future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; (d) the continued risk to the publication of their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect PII and PHI in its possession; and (e) current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and the Illinois Class.

618. Defendant's failure to safeguard Plaintiff's and Illinois Class PII and PHI in violation of FTC guidelines was the direct and proximate cause of damages incurred by Plaintiff and the Illinois Class.

619. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Class.

620. Plaintiff and the Illinois Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

621. As a result of Defendant's wrongful conduct, Plaintiff and the Illinois Class were substantially injured in that they never would have provided their PII and PHI to Defendant, would

not have authorized Defendant's clients to release their PII and PHI to Defendant, or paid for Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being hacked and taken and misused by others.

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

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

COUNT XVIII

OREGON UNLAWFUL TRADE PRACTICES ACT
Or. Rev. Stat. §646.608, *et seq*.
(On Behalf of Plaintiff Ge Xiao Fang and Oregon Class Members)

624. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

625. Plaintiff Fang (for the purposes of this Count, "Plaintiff") brings this claim on behalf of himself and Oregon Class Members.

626. ILS is a "person," as defined by Or. Rev. Stat. §646.605(4).

627. ILS engaged in the sale of "goods and services," as defined by Or. Rev. Stat. §646.605(6)(a).

628. ILS sold "goods or services," as defined by Or. Rev. Stat. §646.605(6)(a).

629. ILS advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

630. ILS engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. §646.608, included the following:

(a) Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. §646.608(1)(e);

(b) Representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. §646.608(1)(g);

(c) Advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. §646.608(1)(i); and

(d) Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. §646.608(1)(t).

631. ILS's unlawful practices include:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oregon Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. §45, the HIPAA, 42 U.S.C. §1320d, COPPA, 15 U.S.C. §§6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§646A.600, *et seq.*, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oregon Class Members' Private Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. §45, the HIPAA, 42 U.S.C. §1320d, COPPA, 15 U.S.C. §§6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §646A.600, *et seq.*;

(f) Failing to timely and adequately notify Plaintiff and Oregon Class Members of the Data Breach;

(g) Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

(h) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oregon Class Members' Private Information; and

(i) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Class Members' Private Information, including duties imposed by the FTC Act, 15

U.S.C. §45, the HIPAA, 42 U.S.C. §1320d, COPPA, 15 U.S.C. §§6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §646A.600, *et seq*.

CLAIM ON BEHALF OF THE ALTERNATIVE SOUTH CAROLINA CLASS

COUNT XIX

SOUTH CAROLINA UNIFORM TRADE PRACTICES ACT
S.C. Code §39-5-10, *et seq.*
(On Behalf of Plaintiff Chelsea Jensen and the South Carolina Class)

632. Plaintiffs repeat the allegations contained in paragraphs 1 through 391 as if fully set forth herein.

633. Plaintiff Jensen (for the purposes of this Count, "Plaintiff") brings this claim on behalf of herself and the South Carolina Class.

634. ILS is a "person," as defined by S.C. Code Ann. §39-5-10(a).

635. South Carolina Unfair Trade Practices Act ("SCUTPA") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. §39-5-20.

636. ILS advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. §39-5-10(b).

637. ILS engaged in unfair and deceptive acts and practices, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and South Carolina Class Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

(b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and South Carolina Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. §45, which was a direct and proximate cause of the Data Breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and South Carolina Class Members' PII and PHI, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and South Carolina Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. §45;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and South Carolina Class Members' PII and PHI; and

(g) Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and South Carolina Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. §45.

638. ILS's acts and practices had, and continue to have, the tendency or capacity to deceive.

639. ILS's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ILS's data security and ability to protect the confidentiality of consumers' PII and PHI.

640. ILS intended to mislead Plaintiff and South Carolina Class Members and induce them to rely on its misrepresentations and omissions.

641. Had ILS disclosed to Plaintiff and South Carolina Class Members that its data systems were not secure and, thus, vulnerable to attack, ILS would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. ILS was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and South Carolina Class Members. ILS accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the South Carolina Class Members acted reasonably in relying on ILS's misrepresentations and omissions, the truth of which they could not have discovered.

642. ILS had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensiveness of the PII and PHI in its possession, and the generally accepted professional standards. Such a duty is also implied by law due to the nature of the relationship between consumers-including Plaintiff and South Carolina Class Members – and ILS, because consumers are unable to fully protect their interests with regard to the PII and PHI in ILS's possession, and placed trust and confidence in ILS. ILS's duty to disclose also arose from its:

(a) possession of exclusive knowledge regarding the security of the data in its systems;

(b) active concealment of the state of its security; and/or

(c) incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and South Carolina Class Members that contradicted these representations.

643. ILS's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. ILS's acts and practices offend established public policies that seek to protect consumers' PII and PHI, and ensure that entities entrusted with PII and PHI use

appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. §45; and the South Carolina Data Breach Security Act, S.C. Code §39-1-90, *et seq.*

644. ILS's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of ILS's long history of inadequate data security; the sensitivity and extensiveness of PII and PHI in its possession; its role in the healthcare system; and its admitted duty of trustworthiness and care as an entrusted protector of data.

645. ILS's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; ILS engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including many South Carolinians impacted by the ILS Data Breach, nearly half the state's population.

646. ILS's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including numerous past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, ILS's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

647. ILS's violations present a continuing risk to Plaintiff and South Carolina Class Members as well as to the general public.

648. ILS intended to mislead Plaintiff and South Carolina Class Members and induce them to rely on its misrepresentations and omissions.

649. ILS acted intentionally, knowingly, and maliciously to violate the SCUTPA, and recklessly disregarded Plaintiff and South Carolina Class Members' rights. ILS's involvement in the healthcare industry and that industry's numerous data breaches put it on notice that its security and privacy protections were inadequate. In light of this conduct, punitive damages would serve

the interest of society in punishing and warning others not to engage in such conduct, and would deter ILS and others from committing similar conduct in the future.

650. As a direct and proximate result of ILS's unfair and deceptive acts or practices, Plaintiff and South Carolina Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for ILS's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

651. Plaintiff and South Carolina Class Members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, individually and on behalf of all others similarly situated, requests the following relief:

1. An Order certifying this action as a class action and appointing Plaintiffs as Class and Subclass representatives and the undersigned as Class counsel;

2. A mandatory injunction directing ILS to adequately safeguard the PII and PHI of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures, including, but not limited to, an Order:

(a) prohibiting ILS from engaging in the wrongful and unlawful acts described herein;

(b) requiring ILS to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

(c) requiring ILS to delete and purge the PII and PHI of Plaintiffs and Class Members unless ILS can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

(d) requiring ILS to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII and PHI;

(e) requiring ILS to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on ILS's systems on a periodic basis;

(f) prohibiting ILS from maintaining Plaintiffs' and Class Members' PII and PHI on a cloud-based database until proper safeguards and processes are implemented;

(g) requiring ILS to segment data by creating firewalls and access controls so that, if one area of ILS's network is compromised, hackers cannot gain access to other portions of ILS's systems;

(h) requiring ILS to conduct regular database scanning and securing checks;

(i) requiring ILS to monitor ingress and egress of all network traffic;

(j) requiring ILS to establish an information security training program that includes at least annual information security training for all employees, with

additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII and PHI, as well as protecting the PII and PHI of Plaintiffs and Class Members;

(k) requiring ILS to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with ILS's policies, programs, and systems for protecting personal identifying information;

(l) requiring ILS to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor ILS's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

(m) requiring ILS to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves: and

(n) Appointing a qualified independent auditor to ensure compliance with the injunctive relief imposed by the Court, and to report to the Court and to Plaintiffs' counsel periodic reports as appropriate of such auditor's assessment of compliance, including any failure to cure deficiencies in compliance with the Court's injunctive relief.

3. A mandatory injunction requiring that ILS provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII and PHI to unauthorized persons;

4. Enjoining ILS from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

5. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

6. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

7. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

8. Granting the Plaintiffs and the Class leave to amend this Complaint to conform to the evidence produced at trial;

9. For all other Orders, findings, and determinations identified and sought in this Complaint; and

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

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demands a trial by jury for any and all issues in this action so triable as of right.

DATED: November 13, 2023

Respectfully submitted,

ROBBINS GELLER RUDMAN
& DOWD LLP
STUART A. DAVIDSON
Florida Bar No. 84824

s/ Stuart A. Davidson
STUART A. DAVIDSON

225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
sdavidson@rgrdlaw.com

MORGAN & MORGAN
JOHN A. YANCHUNIS
Florida Bar No. 324681
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: 813/223-5505
jyanchunis@ForThePeople.com

MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
ALEXANDRA M. HONEYCUTT[#]
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: 866/252-0878
ahoneycutt@milberg.com

Plaintiffs' Co-Lead Counsel

BILZIN SUMBERG
MICHAEL A. HANZMAN
Florida Bar No. 510637
1450 Brickell Avenue, 23rd Floor
Miami, FL 33131
Telephone: 305/350-2424
305/351-2253 (fax)
mhanzman@bilzin.com

Plaintiffs' Liaison Counsel

NUSSBAUM LAW GROUP, P.C.
LINDA P. NUSSBAUM#
1333 Avenue of the Americas, 31st Floor
New York, NY 10036
Telephone: 917/438-9189
lnussbaum@nussbaumpc.com

LYNCH CARPENTER LLP
ELIZABETH POLLACK-AVERY#
1133 Penn Avenue, Floor 5
Pittsburgh, PA 15222
Telephone: 412/322-9243
412/231-0246 (fax)
Elizabeth@lcllp.com

GEORGE FELDMAN McDONALD, PLLC
BRITTANY L. BROWN
Florida Bar No. 105071
9897 Lake Worth Road, Suite 302
Lake Worth, FL 33467
Telephone: 561/232-6002
BBrown@4-justice.com

HAUSFELD LLP
STEVEN M. NATHAN#
888 16th Street N.W., Suite 300
Washington, DC 20006
Telephone: 202/540-7200
202/540 7201 (fax)
snathan@hausfeld.com

Members of Plaintiffs' Executive Committee

ROBBINS GELLER RUDMAN
& DOWD LLP
ALEXANDER C. COHEN
Florida Bar No. 1002715
225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
acohen@rgrdlaw.com

STUEVE SIEGEL HANSON LLP
JORDAN A. KANE[#]
460 Nichols Road
Kansas City, MO 64112
Telephone: 816/714-7100
kane@stuevesiegel.com

KOPELOWITZ OSTROW FERGUSON
WEISELBERG GILBERT
STEVEN SUKERT
Florida Bar No. 1022912
1 West Las Olas Boulevard, 5th Floor
Fort Lauderdale, FL 33301
Telephone: 954/525-4100
954/525-4300 (fax)
sukert@kolawyers.com

LEVIN SEDRAN & BERMAN
NICHOLAS J. ELIA[*]
510 Walnut Street, Suite 500
Philadelphia, PA 19106-3697
Telephone: 877/882-1011
215/592-4663 (fax)
NElia@lfsblaw.com

ZIMMERMAN REED LLP
MICHAEL J. LAIRD[#]
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: 612/341-0400
michael.laird@zimmreed.com

AYLSTOCK, WITKIN, KREIS
& OVERHOLTZ, PLLC
MAURY GOLDSTEIN
Florida Bar No. 1035936
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: 844/794-7402
mgolstein@awkolaw.com

BRADLEY/GROMBACHER LLP
FERNANDO VALLE*
313 Oak Crest Drive, Suite 240
Westlake Village, CA 91361
Telephone: 805/270-7100
fvalle@bradleygrombacher.com

Members of Plaintiffs' Leadership Development Committee

Pro hac vice granted

* *Pro hac vice* forthcoming