UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

EDDIE BASULTO and HERMINIA BASULTO, individually and on behalf of all others similarly situated, Plaintiffs, v. INDEPENDENT LIVING SYSTEMS, LLC, Defendant.	Case No. 1:23-cv-21061 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Eddie Basulto and Herminia Basulto (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, bring this Class Action Complaint against Defendant Independent Living Systems, LLC ("ILS" or "Defendant").

NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of themselves and all other individuals ("Class Members") who had their sensitive personal information ("PII") and protected health information ("PHI")—as defined by Health Insurance Portability and Accountability Act ("HIPPA")— disclosed to unauthorized third parties that accessed and removed the PII and PHI from ILS' system between at least June 30 and July 5, 2022, if not longer (the "Data Breach"). The compromised PII and PHI includes the following: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs")[1], (3) health insurance information (payer name, payer contract dates, health insurance policy number, and policy information including type and deductible amount); (4) medical and/or treatment information (mental or physical condition,

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec.shtml (last visited March 19, 2023).

admission date, dates of service, location, services requested or procedures performed, diagnosis, treatment information, prescription information, physician names, and Medical Record Numbers); and (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider).[2]

2. ILS has ten offices across the United States and provides managed care organizations and providers with clinical and third-party administrative services. In March 2023, ILS notified 4,226,508 individuals that it suffered the Data Breach and informed them that their PII and PHI was compromised thereby (the "Notice").[3]

3. According to the Notice—posted on the Maine Attorney General website[4]—on July 5, 2022, ILS experienced an incident involving the inaccessibility of certain computer systems on its network. The Notice states that ILS responded to the incident by opening an investigation with the assistance of outside cybersecurity specialists, which revealed that an unauthorized actor obtained access to ILS' systems between June 30 and July 5, 2022. The Notice states further that during that time, the unauthorized actor acquired the PII and PHI of over 4.226 million individuals. Thus, the Data Breach resulted from ILS' failure to adequately protect and safeguard that offline set of patient data.

4. Despite learning of the Data Breach on July 5, 2022, ILS waited more than ***eight months*** before notifying impacted individuals—in mid-March 2023—that their highly sensitive PII and PHI had been acquired by an unauthorized actor by way of the Data Breach.

---

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec/068bb4a0-32fa-48f7-822f-fa1083ae1a75/document.html (last visited March 19, 2023); *see also* https://www.securityweek.com/data-breach-at-independent-living-systems-impacts-4-million-individuals/ (last visited March 19, 2023).

[3] An example of ILS' Notice was uploaded to the Maine Attorney General's website, accessible at: https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec.shtml (last visited March 19, 2023).

[4] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec/068bb4a0-32fa-48f7-822f-fa1083ae1a75/document.html (last visited March 19, 2023).

5. ILS owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. ILS breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

6. As a result of ILS' inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII and PHI was accessed and disclosed by a malicious, unauthorized actor. This action seeks to remedy these failings and their consequences. Plaintiffs brings this action on behalf of themselves and all similarly situated individuals whose PII and/or PHI was exposed as a result of the Data Breach, which ILS learned of on or about July 5, 2022, but did not publicly disclose until mid-March 2023.

7. Plaintiffs, on behalf of themselves and all other Class members, asserts claims for negligence, negligence per se, unjust enrichment, violation of the Florida Deceptive and Unfair Trade Practices Act (FLA. STAT. §§ 501.201, *et seq.*), and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

8. Plaintiff Eddie Basulto is a citizen of the state of Florida and resides in Homestead, Florida. Believing that all of his current and former healthcare providers would implement and maintain reasonable security and practices to protect his PII and PHI, Plaintiff Eddie Basulto provided this information to his providers that upon information and belief utilized ILS' services. On or about March 18, 2023, ILS sent Plaintiff Eddie Basulto a letter dated March 14, 2023 confirming that his PII and PHI was impacted by the Data Breach. In the letter, ILS identified that the nature of the information involved includes: name, date of birth, mental or physical condition, treatment information, Food Delivery Information, admission date, billing/claims information,

health insurance policy number, and other health insurance information. Plaintiff Eddie Basulto has spent approximately an hour monitoring his accounts for fraudulent activity and will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

9. Plaintiff Herminia Basulto is a citizen of the state of Florida and resides in Homestead, Florida. Believing that all of her current and former healthcare providers would implement and maintain reasonable security and practices to protect her PII and PHI, Plaintiff Herminia Basulto provided this information to her providers that upon information and belief utilized ILS' services. On or about March 18, 2023, ILS sent Plaintiff Herminia Basulto a letter dated March 14, 2023 confirming that her PII and PHI was impacted by the Data Breach. In the letter, ILS identified that the nature of the information involved includes: name, date of birth, mental or physical condition, treatment information, Food Delivery Information, admission date, billing/claims information, health insurance policy number, and other health insurance information. Plaintiff Herminia Basulto has spent approximately an hour monitoring her accounts for fraudulent activity and will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

10. Defendant ILS is a Florida Limited Liability Company and maintains its principal place of business at 4601 NW 77th Avenue, Miami, Floria 33166.[5] ILS describes itself as a company that provides 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 https://search.sunbiz.org/Inquiry/CorporationSearch/SearchResultDetail?inquirytype=EntityName&directionType=Initial&searchNameOrder=INDEPENDENTLIVINGSYSTEMS%20L020000111260&aggregateId=flal-l02000011126-eabaab8c-290b-4e72-b703-853a8e29f82e&searchTerm=independent%20living%20systems&listNameOrder=INDEPENDENTLIVINGSYSTEMS%20L020000111260 (last visited March 19, 2023).

11. An industry leader in managing home and community-based programs for almost 2 decades, ILS leverages an award winning technology platform. ILS provides assistance beyond the clinical realm at every stage of care from hospitalization to the treatment of chronic illnesses to personalized care management including nutritional support.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which one or more Class Members are citizens of states different from Defendant.

13. The Court has personal jurisdiction over Defendant because it maintains its principal place of business in this judicial district, conducts significant business in Miami, Florida, and/or otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Florida.

14. Venue properly lies in this district because, *inter alia,* Defendant maintains its principal place of business in this judicial district; transacts substantial business, has agents, and is otherwise located in this district; and/or a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Overview of Defendant

15. ILS markets itself as a provider of "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."[6]

[6] https://ilshealth.com/about-ils/ (last visited March 19, 2023).

16. ILS touts itself as "[a]n industry leader in managing home and community-based programs for almost 2 decades," that "leverages an award winning technology platform" through which it "provides assistance beyond the clinical realm at every stage of care from hospitalization to the treatment of chronic illnesses to personalized care management including nutritional support."[7]

17. Through its provision of those services, ILS advertises on its website that, "[i]n partnership with health plans, providers, hospitals, and pharmaceutical and medical device companies, ILS provides solutions aimed at improving health outcomes while rebalancing costs" with the "Mission" of "significantly impact[ing] the quality of life of members by providing innovative health and social support solutions."[8]

18. In the regular course of its business, Defendant collects and maintains the PII and PHI of its customers' patients, former patients, and patients parents, guardians, or guarantors, and other individuals. That information includes: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"), (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (4) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); (5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider); and (6) information of a parent, guardian, or guarantor. Defendant stores this information digitally.[9]

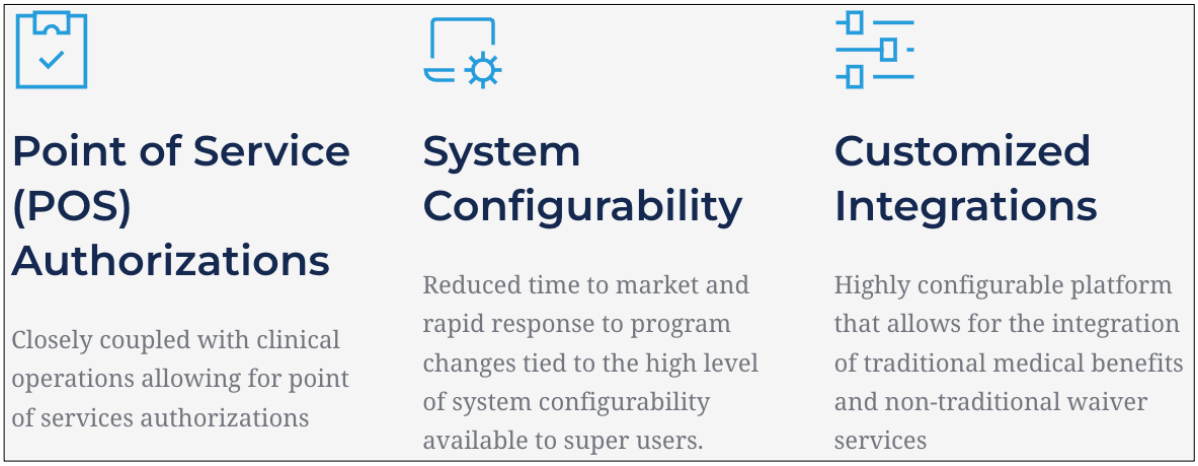
---

[7] *Id*.
[8] https://ilshealth.com/about-ils/ (last visited March 19, 2023).
[9] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec.shtml (last visited March 19, 2023); https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec/068bb4a0-32fa-48f7-822f-fa1083ae1a75/document.html (last visited March 19,

19. Specifically, one "suite" of services that ILS offers are technological administrative services that provide "[a] fully integrated business and technology offering to support **all administrative and financial reporting requirements** of health plans and risk bearing entities," which ILS claims will "support all operating requirements of health plans and risk bearing entities."[10] This service breaks down into multiple component services, many of which involve the collection, management, and storage of individuals' PII and PHI including but not limited to: (1) "claims imaging, adjudication, and payment"; (2) "Financial reporting and related functions"; (3) healthcare "Provider Services and Network Management"; (4) "Analytics and Data Warehousing"; (5) healthcare "Enrollment and Eligibility Processing"; and (6) patient customer service "Call Center and Inbound services," all of which ILS advertises on its website:[11]

ILS further advertises on its website that it has sophisticated systems and "platforms" through which it provides the foregoing services that collect, manage, and store individuals' PII and PHI[12]:

2023); *see also* https://www.securityweek.com/data-breach-at-independent-living-systems-impacts-4-million-individuals/ (last visited March 19, 2023).
[10] https://ilshealth.com/third-party-administration-tpa/ (last visited March 19, 2023).
[11] *Id.*
[12] *Id.*



ILS advertises on its website that the foregoing services are powered by "**state-of-the-art IT infrastructure** and a **knowledgeable world-class team** with decades of experience."[13]

20. Likewise, ILS' website advertises its "Managed Long-Term Services & Supports" service as being comprised of a "suite of solutions including assessments, care management, and coordination of home and community-based services, care planning, and back-office support."[14] ILS' website lists multiple technology/automated-driven components of this service that further involves the collection, management, and storage of individuals' PII and PHI, including but not limited to: (1) "Extensive library of integrated industry and proprietary assessment tools to support holistic evaluation of an individual's needs to achieve good health outcomes and foster independence"; (2) "Automated process for identification of need of clinical and social services, utilization management, authorization systems and reporting"; (3) "ILS has extensive experience contracting and credentialing a broad range of home and community-based and long-term care providers, and administering a broad variety of value based models"; (4) "Utilizing its proprietary technology, ILS provides clients with the necessary guardrails to satisfy regulatory compliance requirements"; (5) "Reporting tools to provide real time visibility on Care Management activities,

[13] *Id.*
[14] https://ilshealth.com/managed-long-term-services-and-supports/ (last visited March 19, 2023).

compliance and financial performance"; and (6) "Platform that can easily interface with other systems, process claims in multiple formats, in a timely and accurate manner with real visibility:[15]

[15] *Id.*

21. Mulitple pages of ILS' website—describing its various services that involve the collection, management, and storage of individuals' PII and PHI—state that ILS uses "**proprietary technology**" that offers an "**Award Winning** Care Management Platform … supported by eCare, a **proprietary technology and analytics platform** that integrates the spectrum of services for LTSS, Medicare and Medicaid beneficiaries":[16]

ILS further advertises that its services are safeguarded to ensure regulatory compliance by stating that it "[u]tiliz[es] its proprietary technology [to] provide[] clients with the **necessary guardrails** to **satisfy regulatory compliance requirements**."[17]

22. Viewing the foregoing website statements in the aggregate, the gist of ILS' business is to provide technological "solutions aimed at improving" the lives of its customers' patients. ILS' website statements and other advertisements give consumers, such as Plaintiffs, the false impression that ILS' services—which it claims are backed by "proprietary," industry-leading, and

[16] https://ilshealth.com/managed-long-term-services-and-supports/ (last visited March 19, 2023); and https://ilshealth.com/care-management/ (last visited March 19, 2023).
[17] *See, e.g.*, https://ilshealth.com/care-management/ (last visited March 19, 2023).

"award winning technology"—are safe and that their PII and PHI are in good hands and protected, but wholly fail to disclose the truth: that ILS lacks sufficient processes to protect the PII and PHI that is entrusted to it.

23. ILS' website also explains how—through its "Management Services Organization"—it not only offers additional services that involve the collection, management, and storage of individuals PII and PHI, but also shares in the revenue generated by its healthcare provider customers in exchange for providing those services by, *inter alia*, doing the following: (1) "When cost containment and revenue goals are exceeded, **ILS and the health plan share in the savings achieved**. In other words – we take all of the risk **and share the rewards!**"; (2) "Through a Management Services Organization (MSO) arrangement, Independent Living Systems (ILS) relieves health plans of the burden of managing costly segments of the membership. **ILS assumes the financial risk from health plans and physicians**, and **takes responsibility for a plan's Medicaid membership expenses** including hospitalizations, prescriptions, and other costs that the member incurs"; and (3) "Our MSO team becomes an extension of your health plan staff, and in doing so, **seamlessly reviews and analyzes data** on the membership, and presents a plan of improvement. Analytics dashboards provide both summaries and detailed information and include; early markers of potentially high cost members and providers, high cost medications, emergency room over utilization and high hospital readmission rates. Analyses available at the member, provider, group, and plan levels."[18]

24. As evidenced by, *inter alia*, their receipt of the Notice from ILS informing them that their PII and PHI were compromised in the Data Breach, Plaintiffs and Class members are, or were, patients of healthcare providers that used ILS' services, and thereby entrusted ILS with their PII and/or PHI, from which ILS profited.

[18] https://ilshealth.com/management-services-organization/ (last visited March 19, 2023).

B. The Data Breach

25. The Notice of the Data Breach disseminated by ILS states that on July 5, 2022, ILS experienced an incident involving the inaccessibility of certain computer systems on its network.[19]

26. The Notice states that ILS responded to the incident by opening an investigation with the assistance of outside cybersecurity specialists, which revealed that an unauthorized actor obtained access to ILS' systems between June 30 and July 5, 2022.[20]

27. ILS' report of the Data Breach on the website of Maine's Attorney General states that during that time, the unauthorized actor acquired the PII and PHI of over 4.226 million individuals.[21]

28. Thus, the Data Breach resulted from ILS' failure to adequately protect and safeguard the PII and PHI entrusted to it through its provision of various services to its healthcare provider clients.

29. Despite learning of the Data Breach on July 5, 2022, ILS waited more than ***eight months*** before notifying impacted individuals—in mid-March 2023—that their highly sensitive PII and PHI had been acquired by an unauthorized actor by way of the Data Breach.

30. The Notice that Defendant sent to Plaintiff and the Class state that the information that was accessed included:

(1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth);

(2) Social Security Numbers ("SSNs")[22],

---

[19] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec/068bb4a0-32fa-48f7-822f-fa1083ae1a75/document.html (last visited March 19, 2023).
[20] *Id*.
[21] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec.shtml (last visited March 19, 2023).
[22] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-

(3) health insurance information (payer name, payer contract dates, health insurance policy number, and policy information including type and deductible amount);

(4) medical and/or treatment information (mental or physical condition, admission date, dates of service, location, services requested or procedures performed, diagnosis, treatment information, prescription information, physician names, and Medical Record Numbers); and

(5) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider).[23]

C. Defendant Knew that Criminals Target PII/PHI

31. At all relevant times, Defendant knew, or should have known, its customers' patients', Plaintiffs', and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyber-attacks that Defendant should have anticipated and guarded against.

32. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[24] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[25]

---

f03280b2c4ec.shtml (last visited March 19, 2023).

[23] https://apps.web.maine.gov/online/aeviewer/ME/40/aacdb720-e082-4ef6-b7e6-f03280b2c4ec/068bb4a0-32fa-48f7-822f-fa1083ae1a75/document.html (last visited March 19, 2023); *see also* https://www.securityweek.com/data-breach-at-independent-living-systems-impacts-4-million-individuals/ (last visited March 19, 2023).

[24] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Nov. 15, 2021).

[25] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Nov. 15, 2021).

33. PII/PHI is a valuable property right.[26] The value of PII/PHI as a commodity is measurable.[27] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[28] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[29] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

34. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

35. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[30] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten

---

[26] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

[27] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[28] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[29] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[30] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for

personal identifying characteristics of an individual."[31] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[32]

36. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[33] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[34]

37. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[35] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[36]

---

criminals.").
[31] *Id.*
[32] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[33] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[34] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[35] *What Happens to Stolen Healthcare Data*, *supra* at n.10.
[36] *Id.*

38. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[37]

39. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Theft of PII/PHI Has Grave and Lasting Consequences for Victims

40. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[38]

41. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[39] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things:

---

[37] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[38] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[39] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[40]

42. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[41]

43. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[42]

44. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to

[40] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.
[41] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).
[42] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).

demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

45. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[43]

46. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[44] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[45] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[46] The FTC also warns, "If the thief's health information is mixed with yours, your

[43] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[44] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf
[45] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.
[46] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 15, 2021).

treatment, insurance and payment records, and credit report may be affected."[47]

47. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[48]

48. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[49]

---

[47] *Id*.
[48] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.
[49] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

49. It is within this harsh and dangerous reality that Plaintiffs and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Damages Sustained by Plaintiffs and the Other Class Members

50. Plaintiffs and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

51. Plaintiffs bring this action on behalf of themselves and the following classes:

> Nationwide Class: All residents of the United States who were notified by Defendant that their PHI and PII may have been compromised as a result of the Data Breach.
>
> Florida Subclass: All residents of Florida who were notified by Defendant that their PHI and PII may have been compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class."

52. Excluded from the Class are: (1) the Judges presiding over the Action, Class Counsel, and members of their families; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or their parents, have a controlling interest, and their current or former officers and directors; (3) Persons who properly opt out; and (4) the successors or assigns of any such excluded Persons.

53. **Numerosity**: Members of the class are so numerous that their individual joinder is impracticable, as the proposed class includes 4.226 million members who are geographically dispersed.

54. **Typicality**: Plaintiffs' claims are typical of class members' claims. Plaintiffs and all class members were injured through Defendant's uniform misconduct, and Plaintiffs' claims are identical to the claims of the class members they seek to represent. Accordingly, Plaintiffs' claims are typical of class members' claims.

55. **Adequacy**: Plaintiffs' interests are aligned with the class they seek to represent and Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and their counsel intend to prosecute this action vigorously. The class's interests are well-represented by Plaintiffs and undersigned counsel.

56. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other class member's claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Defendants' wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

57. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII/PHI;

c. Whether an implied contract existed between Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

d. Whether Defendant breached its duties to protect Plaintiffs' and Class members' PII/PHI; and

e. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

58. Given that Defendants engaged in a common course of conduct as to Plaintiffs and the class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Florida Subclass)

59. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

60. Defendant owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

61. Defendant knew the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted healthcare providers in recent years.

62. Given the nature of Defendant's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

63. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class members' PII/PHI.

64. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

65. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII/PHI would not have been compromised.

66. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—

risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Florida Subclass)

67. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

68. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA 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 (collectively, "HIPAA Privacy and Security Rules").

69. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

70. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable

consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

71. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

72. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

73. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

74. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

75. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost

time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Florida Subclass)

76. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

77. This claim is pleaded in the alternative to the breach of implied contract claim.

78. Plaintiffs and Class Members have both a legal and equitable interest in their PHI and PII that was collected by, stored by, and maintained by Defendant—thus conferring a benefit upon Defendant—that was ultimately compromised by the Data Breach.

79. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendant also benefitted from the receipt of Plaintiffs' and Class members' PHI.

80. As a result of Defendant's failure to safeguard and protect Plaintiffs' PII and PHI, conduct, Plaintiffs and Class members suffered actual damages.

81. Defendant should not be permitted to retain the benefit belonging to Plaintiffs and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that were mandated by federal, state, and local laws and industry standards.

82. Defendant should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT IV
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Florida Subclass)

83. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

84. An actual controversy has arisen and exists between Plaintiffs and members of the Class, on the one hand, and Defendant, on the other hand, concerning the Data Breach and Defendants' failure to protect Plaintiffs' and class members' PHI and PII, including with respect to the issue of whether Defendant took adequate measures to protect that information. Plaintiffs and class members are entitled to judicial determination as to whether Defendant has performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiffs' and class members PHI and PII from unauthorized access, disclosure, and use.

85. A judicial determination of the rights and responsibilities of the parties regarding Defendant's privacy policies and whether they failed to adequately protect PHI and PII is necessary and appropriate to determine with certainty the rights of Plaintiffs and the class members, and so that there is clarity between the parties as to Defendant's data security obligations with respect to PHI and PII going forward, in view of the ongoing relationships between the parties.

COUNT V
VIOLATIONS OF THE OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Florida Subclass)

86. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

87. ILS engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Data Breach occurred through the use of the internet,

an instrumentality of interstate commerce.

88. As alleged herein this Complaint, ILS engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard PII and PHI;

b. failure to make only authorized disclosures of individuals' PII and PHI;

c. failure to timely and accurately disclose the Data Breach to Plaintiffs and Class members; and

d. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII and PHI from unauthorized access and/or theft.

89. ILS' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, ILS engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to individuals impacted by the Data Breach.

90. In committing the acts alleged above, ILS engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to individuals impacted by the Data Breach that it did not follow industry best practices for the collection, use, and storage of their sensitive, valuable PII and PHI.

As a direct and proximate result of ILS' conduct, Plaintiffs and other members of the Class have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

91. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

92. Also as a direct result of ILS' knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiffs and Class members are entitled to damages as well as injunctive relief, 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 ILS' systems on a periodic basis, and ordering ILS to promptly correct 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 its security personnel regarding any new or modified procedures;

D. Ordering that ILS segment PII and PHI by, among other things, creating firewalls and access controls so that if one area of ILS is compromised, hackers cannot gain access to other portions of ILS' systems;

E. Ordering that ILS purge, delete, and destroy in a reasonable secure manner PII and PHI not necessary for its provisions of services;

F. Ordering that ILS conduct regular database scanning and securing 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.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the class members, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as class representatives and undersigned counsel as class counsel;

B. Award Plaintiffs and class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

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

Dated: March 19, 2023

Respectfully submitted,

By: */s/ Mark B. DeSanto*

Joseph G. Sauder (*pro hac vice* forthcoming)
Mark B. DeSanto (FL Bar No. 107688)
SAUDER SCHELKOPF LLC
1109 Lancaster Avenue
Berwyn, PA 19312
Telephone: (888) 711-9975
Facsimile: (610) 421-1326
jgs@sstriallawyers.com
mbd@sstriallawyers.com

Attorneys for Plaintiffs