IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

HEATHER ERICA BETZ, on behalf of herself and all others similarly situated, Plaintiffs, v. ST. JOSEPH'S/CANDLER HEALTH SYSTEM, INC., Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Heather Erica Betz ("Plaintiff"), individually and on behalf of all others similar situated (collectively, the "Class," "Class Members," or "Plaintiffs"), by and through her attorneys, brings this Class Action Complaint against Defendant St. Joseph's/Candler Health System, Inc. ("Defendant" or "SJ/C"), seeking damages, restitution, and injunctive relief for the Class, upon investigation of her counsel, personal knowledge, facts that are a matter of public record, and information and belief as to all other matters.

NATURE OF THE ACTION

1. SJ/C is a healthcare provider rendering medical services to patients in 117 locations spanning 4,000 square miles of Georgia and South Carolina.

2. On or about December 18, 2020, unauthorized individuals hacked SJ/C's IT network and accessed the private and confidential medical information of approximately 1,400,000 individuals[1] (the "Data Breach"), including names, addresses, Social Security numbers, dates of birth, driver's license numbers, billing account information, financial information, health insurance information, employment information, family member and emergency contact information, medical record numbers, dates of service, provider names, and medical and clinical treatment information (collectively, "Personally Identifiable Information" or "PII" and "Personal Health Information" or "PHI").

3. For a full six months after these cyber criminals first accessed SJ/C's IT system, the hackers were able to move freely and undetected through the hospital system's IT network.[2]

4. It was not until June 17, 2021, that "SJ/C identified suspicious activity in its IT network."[3]

---

[1] Department of Health and Human Services Office of Civil Rights, *Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Sept. 9, 2021).

[2] St. Joseph's/Candler, *Notice to Our Patients of a Data Security Incident*, https://www.sjchs.org/patient-privacy/policy/notice-to-our-patients-of-a-data-security-incident (last accessed Sept. 9, 2021).

[3] *Id.*

5. That "suspicious activity" detected on June 17, 2021 was the *coup de grâs* of the hackers' six-month attack. They were holding the hospital system's IT system hostage, and "demanding an as-yet unknown payment in order to release their hold on the system.[4]

> At approximately 4 a.m. on Thursday, June 17, all of the information systems at St. Joseph's/Candler Hospital system in Savannah went down. It wasn't a simple software glitch or temporary power outage. It was, instead, a complete information technology (IT) meltdown. Everything, from electronic medical record[s] (EMR) used to document encounters to the lab, radiology and billing software, went down. Even the phones, which are formatted as voice over internet protocol (VOIP) devices, stopped working. All of St. Joseph's/Candler usual patient encounter protocols were immediately rendered ineffective. The hospital system was, in essence, flying blind.[5]

6. Caught unaware, the hospital system was forced to improvise:

> [SJ/C went] "back to the future" with paper charting, handwritten notes, and lab runners taking lab and x-ray results to the floors, the emergency room and the operating room. For the system's 4,200 employees, 714-plus hospital beds between the two hospitals, and more than 500 doctors, the crisis forced and unexpected on-the-fly adaptation which increased the risk of error—and, potentially, of adverse patient outcomes.[6]

7. It took more than two weeks, until July 2, 2021, for the hospital's IT system to "slowly begin to come back online," but the reboot was "slow and

---

[4] Mark Murphy, *St. Joseph's/Candler Health System Cyberattack Offers Lessons for Us All*, Savannah Morning News (Jul. 9, 2021 at 6:00 AM), https://www.savannahnow.com/story/news/2021/07/09/learning-savannah-st-josephs-candler-hospitals-cyberattack/7907374002/.

[5] *Id.*

[6] *Id.*

deliberate," and it took much longer for the hospital to return to normal operations.[7]

8. On information and belief, SJ/C's rapid switch to pre-internet medical practice was necessitated by Defendant's failure to adequately and regularly back up data and/or failure to create a reasonable data recovery plan, despite having been warned to do so by multiple federal agencies, include the U.S. Department of Health and Human Services ("HHS"), the Cybersecurity and Infrastructure Security Agency ("CSIA"), and the Federal Bureau of Investigation ("FBI").[8]

9. SJ/C was on clear notice that cyber criminals were planning *precisely* this type of attack on hospitals.[9]

10. On June 4, 2020, HHS warned of the Maze Ransomware, which was being used to target healthcare organizations.[10] The HHS warning included detailed information on the Maze Ransomware, including file names that would be installed by hackers, where those file names could be found in a computer

---

[7] *Id.*

[8] Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector, AA20-302A (Oct. 28, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

[9] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware* (Nov. 18, 2019 at 9:44 PM), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware ("Senior FBI and U.S. Secret Service officials said Monday that cybercriminals are increasingly using ransomware to target vulnerable entities like hospitals and municipalities, and urged victims to report attacks to authorities regardless of whether they capitulate and pay ransoms.").

[10] HHS Cybersecurity Program, *Maze Ransomware*, Report # 202006041030 (Jun. 4, 2020), *available at* https://www.hhs.gov/sites/default/files/maze-ransomware.pdf.

system, IP addresses known to host the malware and launch it into hospitals' systems, the text and mechanisms of phishing emails used to gain access to the systems, web links known to launch the malware, commands associated with the malware, and several other tools for preventing and detecting precisely this type of attack.

11. On October 28, 2020, CSIA, FBI, and HHS issued an unprecedented joint advisory (the "Joint Cybersecurity Advisory") warning hospitals that they were in hackers' crosshairs.[11]

12. The Joint Cybersecurity Advisory again included detailed information on file names that would be installed by hackers, where those file names could be found in a computer system, IP addresses known to host the malware and launch it into hospitals' systems, the text and mechanisms of phishing emails used to gain access to the systems, web links known to launch the malware, commands associated with the malware, and several other tools for preventing and detecting precisely this type of attack.[12]

[11] Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector, AA20-302A (Oct. 28, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

[12] *Id.*; FireEye, *Threat Research Blog: Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser* (Oct. 28, 2020), https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html (blog linked in Joint Cybersecurity Advisory "[f]or a comprehensive list of indicators of compromise regarding the BazarLocker malware); FEDO Tracker, *Browse Botnet C&Cs* (last accessed Sept. 9, 2021), https://feodotracker.abuse.ch/browse/trickbot/ (linked to in Joint Cybersecurity Advisory as "an open source tracker for Trickbot C2 servers).

13. Beyond this dire warning from federal agencies, the fact that hackers were targeting hospitals received extensive coverage in national news media prior to December 18, 2020, when hackers first accessed SJ/C's system, and well prior to these cyber criminals holding SJ/C's IT hostage.

14. On September 28, 2020, USA Today covered a "nationwide cyberattack [that] has crippled operations at Universal Health Services, one of the nation's largest health care providers."[13]

15. A CNN reporter warned on October 11, 2020, that, "[i]n 2019 alone, there have been 140 reported attacks targeting state and local governments and health care providers, according to the cybersecurity firm Recorded Future. That's an average of almost three attacks each week—a 65% increase from last year, when 85 attacks were recorded."[14]

16. Forbes journalists reported on December 9, 2020, that "[r]ansomware attacks have doubled in just the past three months. And hospitals in particular have become the new soft targets, with more than 80 publicly reported ransomware attacks thus far in 2020."[15]

---

[13] Mark Snider, *Ransomware Hack Cripples Universal Health Services Hospitals, Facilities Across the US*, USA Today (Sept. 28, 2020 at 1:28 PM), https://www.usatoday.com/story/tech/2020/09/28/health-care-provider-united-health-services-hit-cyberattack/3565533001/.

[14] Dakin Andone, *Three Alabama Hospitals Are Accepting Patients Again After a Ransomware Attack on Its Computers*, CNN (Oct. 11, 2010 at 10:41 AM), https://www.cnn.com/2019/10/11/us/alabama-hospital-ransomware-attack/index.html.

[15] Peter J. Beshar and Jane Holl Lute, *The Hacker 'Ceasefire' with Hospitals Is Over—and That Should Terrify Us*, Forbes (Dec. 9, 2020 at 3:00 PM), https://fortune.com/2020/12/09/covid-hospitals-hackers-ransomware/.

17. Warnings that healthcare providers were vulnerable to cyber-attack have dated back *years*, giving SJ/C ample notice and opportunity to take the necessary steps to secure and monitor their IT systems. In 2014, the FBI issued a notice warning that "[c]yber actors will likely increase cyber intrusions against health care systems—to include medical devices—due to mandatory transition from paper to electronic health records ("EHR"), ***lax cybersecurity standards***, and a high financial payout for medical records in the black market."[16]

18. Healthcare industry publications also were sounding the alarm and warning that many hospitals had woefully inadequate IT security measures:

> Healthcare organizations are lagging in critical security protocols. Only 50 % of organizations are conducting comprehensive end-to-end security risk assessments. While this number has grown from 37% in 2019, it still represents an alarming trend [Rod Piechowski, vice president of thought advisory at the Healthcare Information and Management Systems Society] said.
>
> "If you think about how many healthcare organizations there are in the world, even if only 1% don't have a firewall, that is a lot of opportunity for someone to attack," he said. [17]

19. A statement by SJ/C CEO and President Paul Hinchey in an August 18, 2021, Savannah Morning News article announcing that SJ/C was "fully

[16] FBI Cyber Division: Private Industry Notification, Pin #: 140409-009 (Apr. 8, 2014), *available at* https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (emphasis added).

[17] Heather Landi, *Could Patients Be at Risk During a Hospital Cyberattack? It Depends on how Far Hackers Are Willing to Go, Expert Says*, Fierce Healthcare (Nov. 23, 2020 at 7:07 AM), https://www.fiercehealthcare.com/tech/could-patients-be-at-risk-during-a-hospital-cyber-attack-it-depends-how-far-hackers-are.

operational," except for "a few hotspots where we have to change out computers," indicates that SJ/C was one of the eleven percent of hospital systems that failed to invest in basic firewall protections before the attack:

> "These entities, they reinvent themselves at warp speed," said Hinchey. "So we've hired several national companies, one who does all the security for Amazon, and we put in all these firewalls to make sure we mitigate that as best we can from ever happening again because once is enough."[18]

20. Despite repeated, explicit, detailed notices of the risks faced by hospital systems storing sensitive patient data, Defendant recklessly stored Class Members' PII and PHI in an unsafe manner.

21. Despite repeated, explicit, detailed warnings as to the manner in which hackers were targeting hospitals' IT systems and how to prevent such attacks, Defendant maintained an IT system vulnerable to attack from those very same cyber criminals.

22. The Data Breach was a direct and proximate result of Defendant's failure to implement adequate, reasonable IT security protocols.

23. Further, Defendant failed to implement reasonable and necessary measures to monitor its IT and data systems to detect cyber criminals' intrusion into its network—despite concrete and specific instructions from federal agencies and cyber security experts as to how to detect such an intrusion.

[18] Nancy Guan, *St. Joseph's/Candler Ransomware Investigation Ongoing, Patients Offered Identity Protection*, Savannah Morning News (Aug. 18, 2021 at 6:00 AM), https://www.savannahnow.com/story/news/2021/08/18/st-josephs-candler-hospital-cyberattack-investigation-ongoing-patients-experian-security-savannah-ga/8159487002/.

24. On May 20, 2021, as cyber criminals continued to roam freely and undetected in SJ/C's network, the FBI issued another alert.[19] This time, the warning regarded the Conti Ransomware. Again, the FBI warned as to specific methods of ransomware delivery and methods for detection and mitigation.

25. On information and belief, the Maze, TrickBot, BazarLoader, BazarBackdoor, KEGTAP, BEERBOT, SINGLEMALT, Ryuk, or Conti malware/ransomware/cyber-criminal collective (or a combination thereof) that were warned of by federal agencies was the mechanism criminals used to infiltrate and attack SJ/C's IT system.

26. Alternatively, another form of malware and/or ransomware that was or should have been known to SJ/C was deployed by hackers.[20]

27. Defendant failed to notify its patients that their PII and PHI had been compromised until August 10, 2021, almost *two full months* after the Data Breach was discovered.

28. Defendant disregarded Plaintiff's and Class Members' rights as to their PII and PHI by (i) intentionally, willfully, recklessly, or negligently failing

[19] FBI Flash, *Conti Ransomware Attacks Impact Healthcare and First Responder Networks* (May 20, 2021), *available at* https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf.

[20] For examples of other types of ransomware/malware warned of before the SJ/C attack began, *see* Broadcom, *Sodinokibi: Ransomware Attackers Also Scanning for PoS Software, Leveraging Cobalt Strike* (Jun. 23, 2020), https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos, *and* Trend Micro, *Nefilim Ransomware Threatens to Expose Stolen Data* (Mar. 23, 2020), https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data.

to take reasonable measures protect the SJ/C IT and data systems from unauthorized intrusion; (ii) failing to disclose to patients that SJ/C's IT and data systems were vulnerable to intrusion before patients entrusted their PII and PHI to Defendant; (iii) failing to take reasonable and necessary steps to detect cyber criminals roaming freely in SJ/C's system for six months; and (iv) failing to timely notify patients of the Data Breach.

29. As a result of the Data Breach, Plaintiff and the Class suffered injury and ascertainable losses as described fully below.

30. Plaintiff, on behalf of herself and all other Class Members, asserts claims for negligence; negligence *per se*; violation of the Georgia Fair Businesses Practices Act, O.C.G.A. § 10-1-319 *et seq*.; breach of contract; breach of fiduciary duty; and unjust enrichment.

31. Plaintiff seeks remedies including, but not limited to, declaratory relief, monetary damages, statutory damages, punitive damages, and injunctive relief including, but not limited to, improvements to and auditing of Defendant's IT and data security systems, an equitable accounting of recipients of patients' data, and adequate credit monitoring services funded by Defendant.

PARTIES

32. Plaintiff Heather Erica Betz is, and at all times mentioned herein was, a resident of the State of South Carolina residing in the City of Bluffton and the County of Beaufort. Plaintiff was notified of Defendant's Data Breach and her

PII/PHI being compromised upon receiving a notice letter dated August 10, 2021.

33. Defendant St. Joseph's/Candler Health System, Inc. is a health system incorporated in Georgia and headquartered in Savannah, Georgia. Defendant is a domestic nonprofit corporation with its principal office located at 5353 Reynolds Street, Savannah, Chatham County, Georgia 31405. Service of process may be perfected upon Defendant by serving its registered agent Melissa Alvarez at 5353 Reynolds Street, Savannah, Chatham County, Georgia 31405.

JURISDICTION AND VENUE

34. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d)(2) because this is a class action involving common questions of law or fact in which the aggregate amount in controversy exceeds $5,000,000, there are more than 100 members of the Class, and at least one member of the putative Class is a resident of a state different from that of the Defendant. This Court has supplemental jurisdiction over Plaintiff's and the Class' state law claims pursuant to 28 U.S.C. § 1367.

35. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because Defendant resides in this District, and a substantial part of the unlawful conduct giving rise to this Complaint occurred within the Southern District of Georgia.

FACTUAL ALLEGATIONS

SJ/C Obtains PII/PHI of Plaintiff and Class Members

36. SJ/C "offers healthcare services across the entire continuum, including local and regional primary care, specialized inpatient and outpatient services in the 714 patient beds in [their] two anchor hospitals, home healthcare services, as well as a wide variety of community outreach and education efforts throughout the region."[21]

37. SJ/C operates two hospitals in Savannah, Chatham County, Georgia: St. Joseph's Hospital and Candler Hospital. SJ/C has additional medical facility locations in Chatham County, Georgia, as well as facilities in the following Georgia Counties: Effingham, Bryan, Liberty, Long, Bulloch, Wayne, Toombs, Evans, Candler, and Appling.

38. Because a large number of individuals in these Georgia counties are military members, college students with permanent residence outside of Georgia, or tourists, a large percentage of SJ/C's patients in its Georgia locations are non-Georgia residents.

39. SJ/C additionally maintains facilities in the two following South Carolina Counties: Beaufort and Jasper.

40. SJ/C requires patients to provide PII and PHI as a condition of treatment at its facilities, including, among other things, full legal name, address,

[21] St. Joseph's/Candler, *About Us*, https://www.sjchs.org/home/about-us (last accessed Sept. 9, 2021).

phone number, date of birth, Social Security number, driver's license number, marital status, health history, family members' health history, emergency contact information, marital status, employment information, financial information, and individual medical history.

41. Additionally, SJ/C may receive private and personal information from other individuals and/or organizations such as family members, friends, referring physicians, patients' other doctors, patients' health plan(s), laboratories, and imaging centers.

42. SJ/C also keeps digital copies of patients' medical records, which patients may access through a web portal.

43. Patients are provided with a Privacy Policy when they receive treatment from SJ/C. The Privacy Policy includes a list of instances in which SJ/C may use or disclose patients' PII/PHI without written authorization, including: (i) for treatment; (ii) for payment; (iii) for health care operations; (iv) for customer services; (v) for appointments; (vi) for fundraising; (vii) for public health concerns; (viii) to funeral directors or coroners; (ix) for organ or tissue donation; (x) for research purposes; (xi) for health and safety purposes; (xii) to execute government functions; and (xiii) for workers' compensation claims.

44. The Privacy Policy further reads as follows: "[o]ther uses and disclosures will be made only with your written authorization[,] and you may

revoke the authorization except to the extent St. Joseph's Hospital or Candler Hospital has taken action in reliance on such."[22]

45. The Privacy Policy further outlines the following "Rights to Privacy":

- You have the right to request a restriction on certain uses and disclosures of your information. However, the organizations listed above are not required to agree to a requested restriction.
- You have the right to obtain a paper copy of the Notice of Privacy Practices upon request to the Privacy Official or a member of the organization.
- You have the right to inspect and obtain a copy of your health record as allowed by state and federal regulations.
- You may also request an amendment to your health record as allowed by state and federal regulations.
- You may also request communications of your health information by alternative means or at alternative locations. For example, by sending information to a P.O. Box instead of your home address.
- You may revoke your Authorization to use or disclose health information except to the extent that action has already been taken by providing written notice to the Health Information Management Department at St. Joseph's/Candler Health System, Inc., 5353 Reynolds Street, Savannah, Georgia 31405.
- You may also receive an accounting of disclosures made of your health information as provided by federal regulations by sending a written request to the Health Information Management Department at the address listed above.[23]

[22] St. Joseph's Candler, *Notice of Privacy Practices*, https://www.sjchs.org/patient-privacy/policy (last accessed Sept. 10, 2021).

[23] *Id.*

46. The Privacy Policy further reads as follows: "For reasons other than those stated above or as allowed by law, we will obtain your written authorization to use or disclose your health information."[24]

47. The Privacy Policy became effective "as of April 14, 2003. Revised: 2016, 2020."[25]

48. Plaintiff and Class Members are, or were, patients of SJ/C or received health-related services from SJ/C, and entrusted SJ/C with their PII/PHI.

SJ/C Knew Customers' PII/PHI Was at Risk

49. SJ/C knew or should have known prior to the Data Breach that Plaintiff's and other Class Members' PII/PHI were targets for malicious actors.[26] Defendant knew the nature of the risk, the steps that could be taken to mitigate the risk, and methods for detecting the Data Breach.[27]

50. In its Breach Barometer 2020 report, released prior to cyber criminals' hack of the SJ/C system, the healthcare compliance company Protenus analyzed

---

[24] *Id.*

[25] *Id.*

[26] Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector, AA20-302A (Oct. 28, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa20-302a; FireEye, *Threat Research Blog: Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser* (Oct. 28, 2020), https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html (blog linked in Joint Cybersecurity Advisory "[f]or a comprehensive list of indicators of compromise regarding the BazarLocker malware"); FEDO Tracker, *Browse Botnet C&Cs* (last accessed Sept. 9, 2021), https://feodotracker.abuse.ch/browse/trickbot/ (linked to in Joint Cybersecurity Advisory as "an open source tracker for Trickbot C2 servers").

[27] *Id.*

healthcare breaches occurring in 2019 and found that public reports of healthcare hacking incidents had increased 48.6 percent over the prior year. "This staggering number of reported hacking incidents reminds us how vulnerable patient data remains."[28]

51. In its 2021 Breach Barometer report, released while cyber criminals roamed freely in SJ/C's system, Protenus warned that hacking incidents in 2020 increased 42 percent over the already inflated number of incidents seen in 2019.[29]

52. Despite this knowledge, SJ/C failed to implement and maintain reasonable, necessary, and appropriate security protocols to protect Plaintiff's and other Class Members' PII/PHI from cyber-attacks that SJ/C should have anticipated and guarded against.

53. SJ/C collected and derived benefit from Plaintiff's and Class Members' PII/PHI. Defendant assumed both legal and equitable duties to protect that PII/PHI from unauthorized disclosure.

54. Plaintiff and Class Members relied on SJ/C to protect their PII/PHI in accordance with Defendant's published Privacy Policy.

55. PII/PHI is a property right with tangible monetary value.[30]

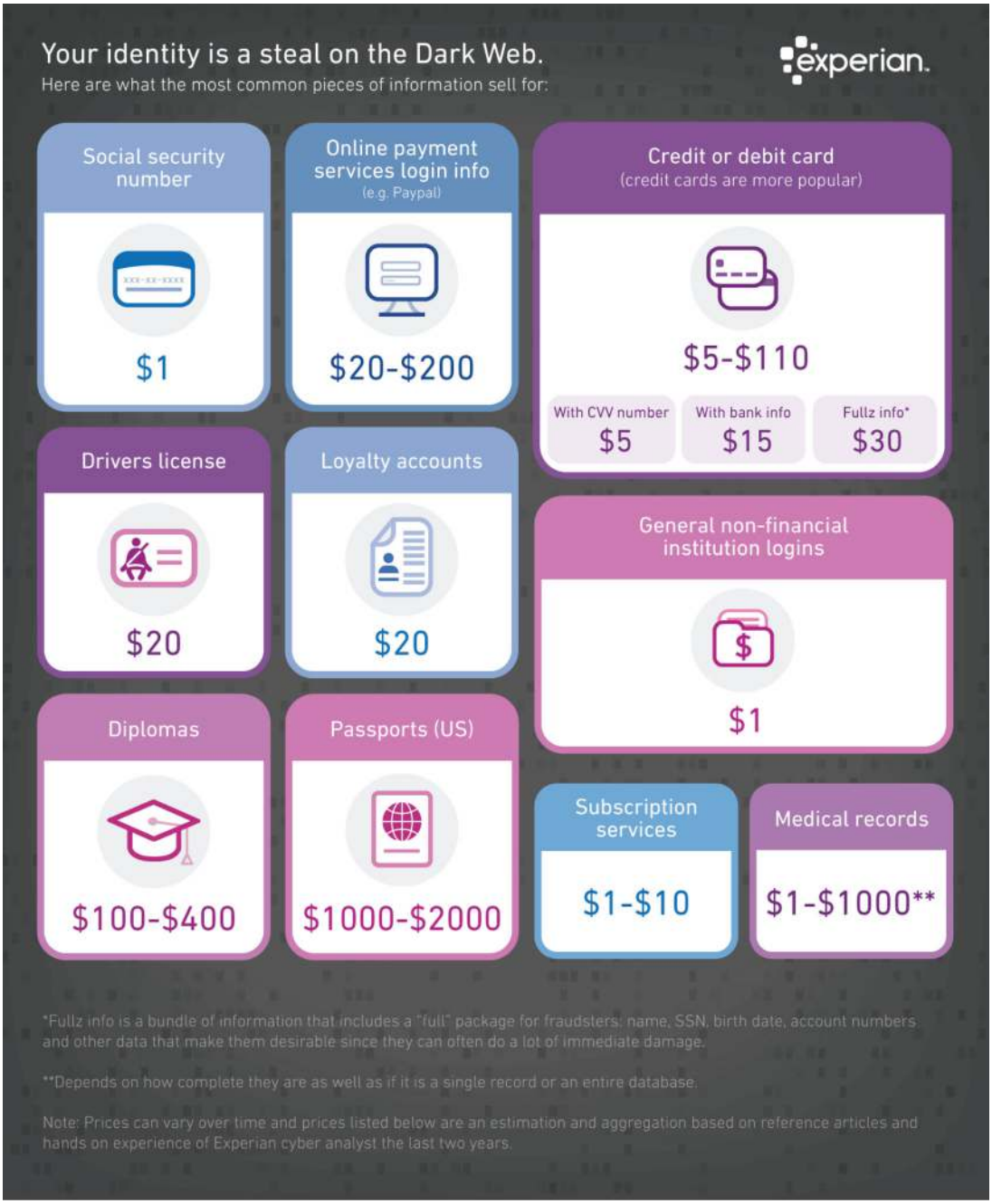
---

[28] Protenus, *2020 Breach Barometer*, *available at* https://www.protenus.com/resources/2020-breach-barometer (last accessed Sept. 10, 2021).

[29] Protenus, *2021 Breach Barometer*, *available at* https://www.protenus.com/resources/2021-breach-barometer (last accessed Sept. 10, 2021)

[30] *See* John T. Soma, et al, *Corporate Privacy Trend: The "Value of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at 1, 2 (2009) ("PII is now a commodity that

56. Personal Health Information (PHI) is gold to cyber criminals. In 2017, the credit reporting company Experian valued PII/PHI items as follows:[31]



companies trade and sell… There is a catch, however: companies benefiting from the value of PII bear the burden of protecting the privacy interests attached to the PII.") (citations omitted).

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

57. As the above graphic indicates, the value of medical records "[d]epends on how complete they are as well as if it is a single file or an entire database."[32]

58. As criminals had unfettered access to SJ/C's entire IT system and database for six months—including the records of patients of the 28 primary care physicians practicing with SJ/C—it is reasonable to believe that the records these criminals possess are complete, substantial, and highly valuable.[33]

59. The value of medical information to hackers, which can reach into the thousands of dollars, has been well documented by journalists and cyber-security experts.

> "Your EHR [Electronic Health Record] contains all of your demographic information—names, historical relevant information of where you live, where you worked, the names and ages of your relatives, financial information like credit cards and bank numbers," [Healthcare Cyber-Security Expert Robert Lord] explains. If that isn't scary enough, there's also data about your past medical history, including every doctor's visit you've made and diagnosis you've received. "***The medical record is the most comprehensive record about the identity of a person that exists today,***" Lord emphasizes.[34]

PII/PHI Theft Has Serious and Long-Term Consequences for Victims

---

[32] *Id.*

[33] St. Joseph's/Candler, *St. Joseph's Candler Primary Care*, https://www.sjchs.org/a-z-services-list/primary-care-physicians (last accessed Sept. 10, 2021).

[34] Mariya Yao, *Your Electronic Medical Records Could Be Worth $1000 to Hackers*, Forbes (Apr. 14, 2017), https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/?sh=25b72b8150cf.

60. Theft of PII and PHI has serious, long-term consequences for victims.

61. Plaintiff and Class Members' injury and damages include, but are not limited to: (i) improper disclosure of PII/PHI now in the custody of cyber criminals; (ii) increased risk of identity theft and medical identity theft; (iii) time, money, and energy expended mitigating the risk of identity theft and medical identity theft; (iv) mental and emotional damages associated with unauthorized parties being privy to and possessing sensitive medical information; (v) and being deprived of valuable PII/PHI, for which there is a well-established international market.

62. Theft of PII and PHI in combination presents particularly serious consequences.

> With traditional identity theft, banks and the Social Security Administration are able to contain some instances by changing details, such as account or social security numbers. However, because health data can't be changed, identity theft can have long-term ramifications that go beyond the typical hazards.[35]

63. In one instance, a young Marine had his wallet and medical identity stolen, with the thief stealing vehicles and having multiple medical procedures done, which the Marine learned of when he was presented with a $20,000.00 hospital bill.[36]

---

[35] Andrew Stenger, *What Happens to Stolen Healthcare Data?*, Health Tech Magazine (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[36] *Hackers Are Stealing Millions of Medical Records—And Selling Them on the Dark Web*, CBS News (Feb. 14, 2019 at 7:37 AM), https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/.

64. On the Dark Web, a criminal offered for sale a file called "USA KIDS FULLZ," data from a pediatrician from the years 2000 to 2014.[37]

65. The Georgia Attorney General's Office's Consumer Protection Division warns that stolen PII and PHI resulting in medical identity theft can allow criminals to get medical treatment using the victim's identity and/or insurance information, commit further crimes using the victim's identity, and obtain government benefits using the victim's information.[38]

66. Criminals also can use sensitive health information to blackmail patients regarding sensitive health information, such as sexually transmitted diseases, mental/behavioral health struggles, plastic surgery, or terminal illness.[39]

67. Armed with PII/PHI thieves can commit "more serious and heinous identity theft, like tax fraud and home equity loan fraud, which is growing dramatically in the U.S."[40]

---

[37] *Id.*

[38] Georgia Attorney General's Office Consumer Protection Division, *Identity Theft: Medical Identity Theft*, https://consumer.georgia.gov/consumer-topics/identity-theft-medical-identity-theft (last accessed Sept. 12, 2021).

[39] Robert Lord, *The Real Threat of Identity Theft Is in Your Medical Records, Not Credit Cards*, Forbes (Dec. 15, 2017 at 7:30 AM), https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/?sh=25c4627a1b59.

[40] Andrew Stenger, *What Happens to Stolen Healthcare Data?*, Health Tech Magazine (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellerman, chief cybersecurity officer of Carbon Black) (internal quotations omitted).

68. Identity theft can further lead to damaged credit. "Not only can this impact your ability to get credit, but it can also hurt your job prospects and increase your auto and homeowners insurance premiums."[41]

69. Resolving identity theft takes victims, on average, about 200 hours of work over the course of six months to resolve identity theft.[42]

70. A 2017 study by the Federal Trade Commission ("FTC") on the aftermath of identity theft found as follows:

- Victims' actions following identity theft included selling possession to pay for expenses and closing financial and online accounts.
- We continue to see significant negative financial impact on victims as a result of this crime. Victims' relationships with others continue to be impacted by this crime.
- Three-quarters of survey respondents expressed they were severely distressed over the misuse or attempted misuse of their personal information.
- Victims expressed a number of strong emotions and feelings as a result of their victimization.
- The majority of victim respondents indicated they have yet to clear up their issue and their cases are not resolved.[43]

CLASS ALLEGATIONS

[41] Ben Luthi, *What to Know About the Effects of Identity Theft*, Experian (Jul. 23, 2021), https://www.experian.com/blogs/ask-experian/how-long-can-the-effects-of-identity-theft-last/.

[42] Gayle Sato, *The Unexpected Costs of Identity Theft*, Experian (Sept. 30, 2020), https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft/.

[43] FTC Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, *available at* https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf (last accessed Sept. 12, 2021).

71. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

72. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

> All persons whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including but not limited to all persons who received notice of the Data Breach, during the period of December 18, 2020 to the present.

73. Excluded from the Class are the judge(s) presiding over this matter, family members of the judge(s), and clerks of the judge(s). Also excluded are SJ/C and its affiliates, parents, subsidiaries, employees, officers, agents, directors, and legal representatives.

74. Class certification of Plaintiff's claims is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

75. The members of the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable.[44] While the precise number of Class Members is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery, upon information and belief, the size

[44] Department of Health and Human Services Office of Civil Rights, *Breach Portal*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Sept. 9, 2021).

of the Class far exceeds 100 individuals. The identities of Class Members are ascertainable through Defendant's records, publication notice, self-identification, Class Members' records, and other means.

76. There are questions of law and fact common to the class that predominate over any questions affecting only individual Class Members. Common questions of law and fact include, but are not limited to, the following:

a. Whether SJ/C had legal and/or equitable duties to maintain reasonable security measures to protect Plaintiff's and Class Members' PII/PHI from unauthorized access/unauthorized disclosure;

b. Whether SJ/C exercised reasonable care to protect Plaintiff's and Class Members' PII/PHI from unauthorized access/unauthorized disclosure;

c. Whether unauthorized individuals obtained Plaintiff's and Class Members' PII/PHI;

d. Whether SJ/C's data security measures complied with security laws and regulations;

e. Whether SJ/C's data security measures complied with industry standards;

f. Whether SJ/C knew or should have known that its data security measures were insufficient;

g. Whether SJ/C breached its duties to Plaintiff and Class Members in protecting their PII/PHI;

h. Whether an implied contract existed between Plaintiff/Class Members and SJ/C that Defendant would exercise reasonable security measures to protect Plaintiff's and Class Members' PII/PHI from unauthorized access/disclosure;

i. Whether Plaintiff and Class Members are entitled to monetary damages and the measure of such damages;

j. Whether the Plaintiff and Class Members are entitled to declaratory relief; and

k. Whether the Plaintiff and Class Members are entitled to equitable relief and the nature of such relief.

77. Common sources of evidence may be used to answer the aforementioned common questions of law and fact.

78. Plaintiff and Class Members were injured by the same practices, acts, and omissions committed by Defendant and described herein. Plaintiff's claims arise from the same acts, practices, and omissions by Defendant and common to all Class Members. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised by the Data Breach.

79. Plaintiff will adequately and fairly protect the interest of all Class Members. Plaintiff has no interests adverse to or in conflict with the Class she seeks

to represent. Plaintiff's counsel are competent and experienced in the successful prosecution of complex consumer class actions of this nature.

80. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. Piecemeal litigation via multiple individual actions would create a risk of varying adjudications as to individual Class Members establishing incompatible standards of conduct for Defendant. Individual actions would substantially impair or impede Class Members' ability to protect their interests. No unusual difficulties will likely be encountered in the management of this matter as a class action. Defendant has acted or failed to act on grounds generally applicable to the class so that relief as to the Class as a whole is appropriate. Questions of law and fact in this action common to class members predominate over questions affecting individual members of the Class.

COUNT I: NEGLIGENCE

81. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

82. SJ/C knew or should have known of data breaches targeting healthcare systems.

83. Given the personal nature of the PII/PHI entrusted to Defendant, the nature of Defendant's business, and the commercial value of PII/PHI entrusted to Defendant, SJ/C should have taken reasonable steps to protect Plaintiff's and Class Members' PII/PHI.

84. Defendant had legal duties to protect Plaintiff's and Class Members' PII/PHI.

85. Defendant had equitable duties to protect Plaintiff's and Class Members' PII/PHI.

86. Defendant breached these duties by failing to exercise reasonable care to protect and safeguard Plaintiff's and Class Members' PII/PHI.

87. Defendant additionally breached these duties by failing to timely notify Plaintiff and Class members of the Data Breach.

88. As a direct and proximate result of Defendant's breach of its duties to exercise reasonable care to protect and safeguard Plaintiff's and Class Members' PII/PHI, Plaintiff's and Class Members' PII/PHI were compromised.

89. As a direct and proximate result of Defendant's breach of its duties to exercise reasonable care to protect and safeguard Plaintiff's and Class Members' PII/PHI, Plaintiff and Class Members suffered and will continue to suffer the damages complained of herein, including, but not limited to: (i) improper disclosure of PII/PHI now in the custody of cyber criminals; (ii) increased risk of identity theft and medical identity theft; (iii) time, money, and energy expended mitigating the risk of identity theft and medical identity theft; (iv) mental and emotional damages associated with unauthorized parties being privy to and possessing sensitive medical information; and (v) being deprived of valuable PII/PHI, for which there is a well-established international market.

90. Defendant's actions and/or failure(s) to act complained of herein show willful misconduct, malice, wantonness, oppression, or that entire want of care which would raise the presumption of conscious indifference to consequences, and punitive damages are warranted.

COUNT II: NEGLIGENCE *PER SE*

91. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

92. SJ/C had and has duties arising from statutory law, including, but not limited to, the Health Information Portability and Accountability Act ("HIPAA") Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E; the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C; the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45(a)(1); and the Georgia Fair Businesses Practices Act ("GFBPA"), O.C.G.A. § 10-1-390(a)-(b).

93. Defendant breached its duties arising from statutory law, including, but not limited to, the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E; the HIPAA Security Rule, 45 at 45 C.F.R. Part 160 and Part 164, Subparts A and C; the FTCA, 15 U.S.C. § 45(a)(1); and/or the GFPBA, O.C.G.A. § 10-1-390(a)-(b).

94. Plaintiff and Class Members are among the class of persons that the statutes referenced in ¶¶ 92-93 were intended to protect.

95. Plaintiff and Class Members suffered harm occurring from the Data Breach. And the harm suffered by Plaintiff and Class Members is the type of harm that the statutes referenced in ¶¶ 92-93 were intended to guard against.

96. It was reasonably foreseeable that Plaintiff and Class Members would suffer the type of harm from the Data Breach that the statutes referenced in ¶¶ 92-93 were intended to guard against.

97. Plaintiff and Class Members suffered direct and proximate injury as a result of Defendant's violations of the statutes referenced in ¶¶ 92-93. These injuries include, but are not limited to: (i) improper disclosure of PII/PHI now in the custody of cyber criminals; (ii) increased risk of identity theft and medical identity theft; (iii) time, money, and energy expended mitigating the risk of identity theft and medical identity theft; (iv) mental and emotional damages associated with unauthorized parties being privy to and possessing sensitive medical information; and (v) being deprived of valuable PII/PHI, for which there is a well-established international market.

98. Defendant's violations of the statutes referenced in ¶¶ 92-93 constitute negligence *per se*.

COUNT III: VIOLATION OF THE GEORGIA FAIR BUSINESSES PRACTICES ACT (O.C.G.A. § 10-1390 *ET SEQ.*)

(On Behalf of Plaintiffs and all Class Members, or, Alternatively, Plaintiffs and the Georgia Statewide Class)

99. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

100. SJ/C, while operating in Georgia, engaged in unfair and deceptive consumer acts in the conduct of trade and commerce, in violation of O.C.G.A. § 10-1-390(a) and (b), including, but not limited to, the following:

a. Defendant failed to enact adequate privacy and security measures to protect Plaintiff's and Class Members' PII/PHI from unauthorized disclosure, release, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendant knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' PII/PHI from unauthorized disclosure, release, theft, and data breaches;

c. Defendant knowingly and fraudulently misrepresented that it would comply with requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PII/PHI, including, but not limited to, duties imposed by the HIPAA Security Rule at 45 C.F.R. Part 160 and Part 164, Subparts A and C and the FTCA at 15 U.S.C. § 45(a)(1); and

d. Defendant failed to maintain the privacy and security of Plaintiff's and Class Members' PII/PHI in violation of duties imposed by

applicable federal and state laws, including, but not limited to, those mentioned in the preceding paragraph, which failure was a direct and proximate cause of the Data Breach.

101. As a direct and proximate result of Defendant's practices, Plaintiff and Class Members suffered the injury and/or damages described herein, including, but not limited to: (i) improper disclosure of PII/PHI now in the custody of cyber criminals; (ii) increased risk of identity theft and medical identity theft; (iii) time, money, and energy expended mitigating the risk of identity theft and medical identity theft; (iv) mental and emotional damages associated with unauthorized parties being privy to and possessing sensitive medical information; and (v) being deprived of valuable PII/PHI, for which there is a well-established international market.

COUNT IV: BREACH OF CONTRACT

102. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

103. Plaintiff and other Class Members entered into express and/or implied contracts with SJ/C in receiving medical treatment from Defendant.

104. In reliance on Defendant's duties under these express and/or implied contracts, Plaintiff and Class Members, either through themselves or their insurers (including Medicare/Medicaid), provided SJ/C with PII/PHI. Defendant's duties under these express and/or implied contracts included but were not limited to: (i)

providing medical treatment based upon, in part or in whole, PII/PHI provided by Plaintiff and Class members; (ii) taking reasonable measures to protect Plaintiff's and Class Members' PII/PHI from unauthorized disclosure; and (iii) complying with applicable federal and state law regarding disclosure of Plaintiff's and Class Members' PII/PHI.

105. Had Plaintiff and Class Members known that Defendant would not take reasonable measures to protect their PII/PHI, Plaintiff and Class Members would not have, either through themselves or their insurers (including Medicare/Medicaid), paid money for medical services in the amount Plaintiff and Class Members paid to SJ/C.

106. Had Plaintiff and Class Members known that Defendant would not take reasonable measures to protect their PII/PHI, they would not have entrusted their PII/PHI to Defendant.

107. Defendant breached its obligations under the express or implied contracts it entered into with Plaintiff and Class Members by failing to take reasonable measures to protect Plaintiff's and Class Members' PII/PHI.

108. Plaintiff and Class Members fulfilled their obligations under the express or implied contract entered into with Defendant by paying for medical services—either directly or through their insurers (including Medicare/Medicaid).

109. As a direct and proximate result of Defendant's breach of its express or implied contracts with Plaintiff and Class Members, Plaintiff and Class Members suffered and continue to suffer damages, including, but not limited to: (i) improper disclosure of PII/PHI now in the custody of cyber criminals; (ii) increased risk of identity theft and medical identity theft; (iii) time, money, and energy expended mitigating the risk of identity theft and medical identity theft; (iv) mental and emotional damages associated with unauthorized parties being privy to and possessing sensitive medical information; and (v) being deprived of valuable PII/PHI, for which there is a well-established international market.

COUNT V: BREACH OF FIDUCAIRY DUTY

110. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

111. But for Plaintiff's and Class Members' belief that Defendant would take reasonable steps to protect their PII/PHI, Plaintiff and Class Members would not have provided their PII/PHI to Defendant.

112. Plaintiff and Class Members gave Defendant their PII/PHI in confidence.

113. Defendant's acceptance and retention of Plaintiff's and Class Members' PII/PHI created a fiduciary relationship.

114. To fulfill its duties pursuant to this fiduciary relationship, Defendant was required to take reasonable steps to protect Plaintiff's and Class Members' PII/PHI.

115. By acting or failing to act as complained of herein, Defendant failed to exercise its duties under this fiduciary relationship.

116. As a direct and proximate result of Defendant's breach of its duties pursuant to this fiduciary relationship, Plaintiff and Class Members suffered and continue to suffer damages, including, but not limited to: (i) improper disclosure of PII/PHI now in the custody of cyber criminals; (ii) increased risk of identity theft and medical identity theft; (iii) time, money, and energy expended mitigating the risk of identity theft and medical identity theft; (iv) mental and emotional damages associated with unauthorized parties being privy to and possessing sensitive medical information; and (v) being deprived of valuable PII/PHI, for which there is a well-established international market.

COUNT V: UNJUST ENRICHMENT

117. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

118. Plaintiff, on behalf of herself and the Class, pleads her claim of unjust enrichment in the alternative to her claim of breach of express or implied contract.

119. Plaintiff and Class Members—either through themselves or their insurers (including Medicare/Medicaid)—conferred monetary benefit on SJ/C.

120. Defendant benefitted from receiving Plaintiff's and Class Members' PII/PHI, which Defendant used to make insurance claims and facilitate payment.

121. Defendant either accepted or had knowledge of the monetary benefits conferred as a result of receiving Plaintiff's and Class Members' PII/PHI, which Defendant used to make insurance claims and facilitate payment.

122. Damages incurred by Plaintiff and Class Members equal the difference in payment made on reliance that Defendant would take reasonable steps to protect Plaintiff's and Class Members' PII/PHI and/or comply with applicable federal and/or state law and actual steps Defendant took to protect Plaintiff's and Class members' PII/PHI.

123. Defendant should be compelled to return to Plaintiff and Class Members the difference between payment made on reliance that Defendant would take reasonable steps to protect Plaintiff's and Class Members' PII/PHI and/or comply with applicable federal and/or state law and actual steps Defendant took to protect Plaintiff's and Class members' PII/PHI.

PRAYER FOR RELIEF

WHEREFORE, individually, and on behalf of all other Class Members, Plaintiff respectfully prays this Court for relief and judgment, as follows:

A. Determining that this action is a proper class action, and designating Plaintiff as class representative of the Class;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. For equitable relief compelling Defendant to adopt appropriate measures to protect Plaintiff's and Class Members' PII/PHI;

D. For an equitable accounting detailing the recipients of Plaintiff's and Class Members' PII/PHI;

E. Ordering Defendant to pay for not less than five years of credit monitoring and identity theft services for Plaintiff and Class Members;

F. Awarding of pre-judgment and post-judgment interest to the maximum extent allowable;

G. Awarding Plaintiff and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

H. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial of all claims of this action so triable.

Dated: September 13, 2021

Constance Cooper, Esq.
Ga. Bar No. 469041
HACH ROSE SCHIRRIPA & CHEVERIE LLP
1505 Washington Ave.
Savannah, GA 31404

ccooper@hrsclaw.com

Frank R. Schirripa (*pro hac vice* forthcoming)
Seth M. Pavsner (*pro hac vice* forthcoming)
HACH ROSE SCHIRRIPA & CHEVERIE LLP
112 Madison Avenue, 10th Floor
New York, New York 10016
Tel: (212) 213-8311
fschirripa@hrsclaw.com
spavsner@hrsclaw.com