IN THE CIRCUIT COURT OF THE FIRST JUDICIAL CIRCUIT
JACKSON COUNTY, ILLINOIS

SHARON J. MCFARLAND, individually and on behalf of all similarly situated individuals, *Plaintiff*, v. SIU PHYSICIANS & SURGEONS, INC., an Illinois corporation, *Defendant.*	)	Case No. 2021L64

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Sharon McFarland ("Plaintiff"), individually and on behalf of a class of similarly situated persons, brings this First Amended Class Action Complaint against Defendant SIU Physicians & Surgeons, Inc. ("SIU" or "Defendant") as a result of Defendant's actions and inactions concerning a recent data breach ("Data Breach") that compromised the personally identifiable information ("PII") of Plaintiff and other members of the putative class. Plaintiff alleges as follows based on personal knowledge as to her own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by her attorneys.

INTRODUCTION

1. In or about December 23, 2020, SIU Medicine (a/k/a SIU Physicians & Surgeons, Inc.) announced that sensitive patient data – including but not limited to names, dates of birth, Social Security numbers, medical record numbers, health insurance information, and medical treatment or diagnosis information – of many Illinois individuals was compromised in a data security breach of its file transfer software vendor, Accellion, USA, LLC ("Accellion").

2. Accellion is a major cloud-based software company that provides third-party file transfer platforms and services to thousands of entities in both the public and private sector, including in the government, healthcare, financial, legal, and education sectors.

3. Defendant utilized one of Accellion's products known as the File Transfer Appliance ("FTA") that enabled the transfer of large files through a purpose-built application.[1]

4. Accellion referred to its FTA service as a 20-year-old, obsolete, "legacy product" that was "nearing end-of-life," making it increasingly vulnerable to data security issues and the compromise of sensitive information.[2]

5. In fact, Accellion had "encouraged all FTA customers to migrate to kiteworks for the last three years[.]"[3]

6. However, despite Accellion's warnings, Defendant continued to utilize Accellion's FTA service.

7. Not surprisingly, beginning as early as December 2020, and continuing through the end of January 2021, Accellion's customers, including Defendant, became the target of a concerted cyberattack during which hackers and unauthorized third parties exploited the data security vulnerabilities in the FTA software to gain unauthorized access to files that were being transferred or shared across the platform and were able to gain access to Defendant's medical files and the PII of Plaintiff and Class members.

---

[1] ACCELLION, *Accellion Responds to Recent FTA Security Incident* (Jan. 12, 2021) http://www.accellion.com/company/press-releases/accellion-provides-responds-to-recent-fta-security-incident/.

[2] ACCELLION, Press Release, *Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), http://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/.

[3] *Id.*

8. The Data Breach was carried out by individuals associated with the notorious financially-motivated extortion hacker gangs known as FIN11 and Clop, which have bene linked to numerous high-profile breaches.[4]

9. True to their hacking model, these gangs have already engaged with numerous users of Accellion's FTA service, and posted individuals' personal data on the dark web. For instance, Clop published University of Colorado community members' sensitive data on the dark web, and after the University of Colorado refused to pay a ransom, Clop published more.[5] In addition, Clop has posted financial records such as tax documents and passport information associated with the University of Maryland and the University of California.[6]

10. Moreover, Clop's publications of sensitive personal data have not been limited to just financial records and student data. It has posted the demographic information and medical records – the same data breached with respect to Defendant's patients – of patients from the University of Miami healthcare system.[7]

11. Importantly, following the Data Breach cybersecurity exports have noted that sophisticated hacking groups like Clop looking for maximum monetary profit do not usually exploit all of the data they obtain from a breach at once, but rather release data slowly over time.[8]

---

[4] *Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware*, THREATPOST (Feb. 22, 2021), https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/.
[5] *Cyberattack Update July 2, 2021*, UNIVERSITY OF COLORADO, https://www.cu.edu/accellion-cyberattack (last visited Jan. 21, 2022).
[6] *Ransomware Group Targets Universities in Maryland, California in New Data Leaks*, ZDNET (Mar. 30, 2021), https://www.zdnet.com/article/ransomware-group-targets-universities-of-maryland-california-in-new-data-leaks/.
[7] *Clop Ransomware Gang Leaks Data Stolen From Colorado, Miami Universities*, CYBERINTEL (Mar. 24, 2021), https://cyberintelmag.com/attacks-data-breaches/clop-ransomware-gang-leaks-data-stolen-from-colorado-miami-universities/.
[8] *The Accellion Breach Keeps Getting Worse—and More Expensive*, WIRED (Mar. 8, 2021), https://www.wired.com/story/accellion-breach-victims-extortion/.

12. Even though Defendant knew that it was transferring the sensitive PII of hundreds of its medical patients through its FTA service, Defendant failed to take basic security precautions, such as updating its FTA service that its own vendor, Accellion, told it to update, which could have prevented, and certainly at least mitigated, the ramifications of the vulnerabilities with the FTA service that led to the Data Breach and the unauthorized disclosure of Plaintiff's and Class members' PII.

13. Defendant's cybersecurity practices and procedures fell below the industry standard, jeopardized the PII of Plaintiff and members of the proposed Class, and exposed Plaintiff and Class members to imminent risk of harm, including identity theft and fraud, by sophisticated and financially-motivated criminal groups.

14. Furthermore, despite Illinois law mandating expedient disclosures without unreasonable delay, despite Defendant's knowledge that it has breach notification obligations and representation that it would provide patients with notice of any data breach within 60 days,[9] and Accellion's notification to its FTA clients, including Defendant, of the cyber breach on December 23, 2020,[10] Defendant failed to issue any notification of the breach to Plaintiff and the other Class members until April 6, 2021, *104 days* later.

15. To this day, Plaintiff continues to rely on her own time, efforts, and expense to monitor and assess the extent to which her valuable PII was compromised and will continually monitor her accounts into the foreseeable future.

---

[9] *Notice of Privacy Practices*, SIU HEALTHCARE, https://www.siumed.edu/notice-privacy-practices.html (last visited Jan. 21, 2022) ("You have the right to be told when a breach of your protected health information has occurred. We will notify you as soon as sufficient information about the breach is available, but not to delay past 60 days").

[10] ACCELLION, Press Release, *Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), http://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ ("All FTA customers were promptly notified of the attack on December 23, 2020").

16. On behalf of herself and the proposed Class defined below, Plaintiff seeks equitable and money damages, together with costs and reasonable attorneys' fees.

PARTIES

17. At all relevant times, Plaintiff Sharon McFarland has been a resident and a citizen of the state of Illinois.

18. Defendant SIU Physicians & Surgeons, Inc. is an Illinois corporation with its headquarters located in Springfield, Illinois. Defendant conducts business throughout Illinois, including in Jackson County.

JURISDICTION AND VENUE

19. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant is doing business within this State and because Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Defendant came into possession of Plaintiff's PII in this state, and Defendant failed to take reasonable precautions to guard against, respond to, and detect cyberattacks in this State.

20. Venue is proper in Jackson County pursuant to 735 ILCS 5/2-101, because Defendant is doing business in Jackson County and thus resides there under § 2-102.

FACTS SPECIFIC TO PLAINTIFF

21. Defendant operates SIU Medicine, a network of medical providers, outpatient treatment centers, and a hospital, located throughout the southern Illinois region.

22. Plaintiff was a patient treated by Defendant. As part of receiving treatment from Defendant Plaintiff had to provide Defendant with her PII, including her name, date of birth, and health insurance information. In addition, Defendant also entered Plaintiff's medical treatment and

diagnosis information into its digital records system in the course of providing Plaintiff medical services.

23. Plaintiff provided her PII to Defendant with the understanding and belief that her PII would be secured and that she would be immediately and directly notified of any security issues concerning her PII.

24. Beginning as early as December 2020, and continuing through the end of January 2021, Defendant was the target of a concerted cyberattack during which sophisticated and financially-motivated third-party hackers exploited the data security vulnerabilities in the outdated Accellion FTA software that Defendant had been utilizing to gain u access to Defendant's medical files and the PII of Plaintiff and Class members.

25. As a result of the cyberattack, the PII of thousands of Defendant's patients was accessed by unauthorized third-party hackers in order to use it for financial extortion.

26. Importantly, Defendant had been made aware of the security vulnerabilities in the Accellion FTA service that it utilized, having been informed by Accellion for at least three years prior to the cyberattack that the FTA service that Defendant was using was obsolete and that Defendant should upgrade to a more secure file transfer service. Nonetheless, Defendant failed to take reasonable measures to mitigate the vulnerabilities or switch to a different file transfer service.

27. On December 23, 2020, Accellion notified all of its FTA clients of the attach, but it was not until April 6, 2021 that Defendant notified patients that their sensitive patient data – including but not limited to names, dates of birth, Social Security numbers, medical record numbers, health insurance information, and medical treatment or diagnosis information – was compromised in a data security breach.

28. Despite the severity of the data breach and requirements under state law to inform victims of data breaches without undue delay (and Defendant's own representations that it would inform patients within 60 days that it would notify them of a breach), Plaintiff did not receive any notice about the Data Breach and that her PII had been exposed in the cyberattack until more than a month later, on or about April 13, 2021.

29. Due to the highly sensitive nature of the information provided by Plaintiff that was compromised in the Data Breach, including her personal medical information, Plaintiff has had to expend a substantial amount of time and effort monitoring her personal accounts.

30. The Data Breach here was particularly damaging given the nature of the FTA service that Defendant was utilizing "because in a normal case an attacker has to hunt to find your sensitive files, and it's a bit of a guessing game, but in this case the work is already done . . . By definition everything sent through Accellion was pre-identified as sensitive by a user."[11]

31. Defendant's failure to implement a reasonable cybersecurity protocol and upgrade the file transfer service that it was using for highly sensitive PII allowed unauthorized third-party hackers to access Plaintiff's and other Class members' PII.

32. Given the current prevalence of cybersecurity awareness, especially in light of constant, high profile data breaches, Defendant knew of the risks inherent in capturing, storing, and using the PII of Plaintiff and the other Class members, and the consequences of the exposure of such PII to unauthorized third parties, as well as the importance of promptly notifying affected parties in the event of a breach incident.

[11] *The Accellion Breach Keeps Getting Worse—and More Expensive*,WIRED (Mar. 8, 2021), https://www.wired.com/story/accellion-breach-victims-extortion/ (quoting Jake Williams, founder of the security firm Rendition Infosec).

33. These types of data breaches harm consumers beyond increasing the likelihood of identity and financial theft—they are harmed by the fact that their personal information, such as emails, addresses, phone numbers, and, more importantly, their medical information are connected with their names..

34. As security experts now know, and as the behavior of the hackers following the Data Breach confirms, the release of data breach victims' personal information to the black market not only increases the likelihood of identity theft and financial extortion, but also makes them an easy target for spammers.

35. Thus, Plaintiff and the Class members are subject to and imminent risk of ongoing and targeted financial extortion and spam and phishing attacks for an unknown period of time since the financially-motivated hackers their criminal partners are not only armed with Plaintiff's and the Class member's PII, but also armed with the knowledge that such PII is associated with real people.

36. Indeed, as discussed above, the hackers responsible for the breach are using this connection between the breached sensitive medical data and contact information as leverage for their ransom threats.

37. Defendant had a duty to keep Plaintiff's and Class members' PII secure and to protect it from unauthorized disclosures. Plaintiff and the other Class members provided PII to Defendant with the understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized disclosures.

38. Defendant's failure to comply with reasonable data security standards and to update its file transfer service provided Defendant a benefit in the form of saving on the costs of compliance, but at the expense and severe detriment of Defendant's patients, including Plaintiff

and the other Class members, whose PII has been exposed in the data breach or otherwise placed at serious and ongoing risk of imminent misuse, fraudulent charges, and identity theft.

39. Since recently becoming aware of the Data Breach, Plaintiff has taken substantial time and effort to mitigate her risk of identity theft and fraud, monitoring her virtual accounts to guard against fraudulent attempts to open accounts in her respective name.

40. Plaintiff has also been harmed by having her sensitive PII compromised and faces the imminent and impending threat of future additional harm from the increased threat of financial extortion, identity theft and fraud by the sophisticated hackers themselves or from having her PII sold, misappropriated, or otherwise misused by other unknown parties.

41. Plaintiff has also experienced mental anguish as a result of the Data Breach. For example, she experiences anxiety and anguish when thinking about what would happen if her identity is stolen as a result of the Data Breach; when contemplating that her PII will be used as a means to extort her; and when considering that her PII has likely been sold to unknown criminals.

CLASS ALLEGATIONS

42. Plaintiff brings this action as a class action on behalf of herself and a Class of similarly situated individuals pursuant to 735 ILCS § 5/2-801. The Class is defined as follows:

> **Class:** All Illinois residents whose PII was in the possession of Defendant, or any of its subsidiaries or agents, at any time beginning in December 2020 through the end of January 2021.

43. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

44. Upon information and belief, there are thousands of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the

exact number of Class members is currently unknown to Plaintiff, the precise size of the Class may easily be ascertained through Defendant's records.

45. Plaintiff's claims are typical of the claims of the Class members she seeks to represent because the factual and legal bases of Defendant's liability to Plaintiff and the other Class members are the same and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class members. As alleged herein, Plaintiff and the other Class members have all suffered damages as a result of Defendant's failure to maintain reasonable security safeguards with respect to the FTA vulnerabilities and its handling and storage of its patients' sensitive PII.

46. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant adequately safeguarded Plaintiff's and the Class members' PII;

b. Whether Defendant failed to implement adequate technical, administrative, and physical safeguards to protect Plaintiff's and the Class members' PII by not upgrading or replacing its FTA product;

c. Whether Defendant's patients were notified of the Data Breach within a reasonable period of time;

d. Whether Defendant willfully, recklessly, and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class members' PII;

e. Whether there was an unauthorized disclosure of the Class members' PII;

f. Whether Plaintiff and the Class members sustained damages as a result of Defendant's failure to adequately safeguard their PII;

g. Whether Defendant's PII storage and protection protocols and procedures were reasonable under industry standards;

h. Whether Defendant's cybersecurity prevention, detection, and notification protocols were reasonable under industry standards;

i. Whether Defendant misrepresented the safety and security of the Class members' PII maintained by Defendant;

j. When Defendant became aware of the unauthorized access to Plaintiff's and the Class members' PII; and

k. Whether Defendant's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*.

47. Absent a class action, most Class members would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

48. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class she seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the other Class members and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

49. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other Class members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

50. Plaintiff realleges the foregoing allegations as if fully set forth herein.

51. At all relevant times, Defendant had a duty, including a statutory duty under 815 ILCS 530/45), or undertook/assumed a duty, to implement a reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to safeguard the PII of the Plaintiff and the Class members, *i.e.* to utilize a secure file transfer process, keep any file transfer process up to date, and to prevent the unauthorized access to and disclosures of the same.

52. Upon storing and handling Plaintiff's and Class members' PII, Defendant also undertook and owed a duty to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so. This duty included, among other things, designing, implementing, maintaining, and testing Defendant's cybersecurity systems to ensure that Plaintiff's and the Class members' PII was reasonably secured and protected.

53. Finally, due to Defendant's position of exclusive control, knowledge, and discretion regarding its cybersecurity and data breach notification practices compared to its clients' and Plaintiff's relative lack of power concerning the same, a duty arose due to such special relationship that required Defendant to implement industry standard cybersecurity protocols regarding its technical, administrative, and physical controls, and its data breach notification procedures.

54. Defendant negligently failed to change or upgrade its outdated FTA platform for securely transferring files containing confidential information even though Defendant was made

aware of the vulnerabilities concerning its FTA program, placing Defendant at a heightened risk of security breaches.

55. Defendant breached the aforementioned duties in, including but not limited to, one or more of the following ways:

a. Failing to implement reasonable data privacy and cybersecurity measures to secure Plaintiff's and Class members' PII;

b. Failing to implement a reasonable data privacy and cybersecurity protocol, including adequate procedures for preventing cybersecurity threats and/or detecting such threats in a timely manner;

c. Failing to implement industry standard data privacy and cybersecurity protocols including failing to promptly notify its patients who were impacted by the Data Breach.

d. Failing to reasonably comply with applicable state and federal law concerning its data privacy and cybersecurity protocol, including the manner of its notification to its patients concerning the Data Breach; and

e. Otherwise failing to act reasonably under the circumstances and being negligent with regards to its conduct in preventing, detecting, and disclosing the subject Data Breach.

56. Defendant knew, or should have known, of the risks inherent to storing Plaintiff and Class members' PII, and of not ensuring that its FTA platform was secure. The risk of compromised data and a data breach were reasonably foreseeable to Defendant as Defendant was informed of the need to upgrade its FTA platform due to the program's dated nature and the increased susceptibility to data security incidents three years prior to the Data Breach.

57. Defendant knew, or should have known, that its data privacy and cybersecurity protocol failed to reasonably protect Plaintiff and the Class members' PII and that its lack of an adequate data breach notification protocol was insufficient to enable its patients such as Plaintiff to mitigate the impact of the Data Breach.

58. As a direct result of Defendant's aforesaid negligent acts and omissions, Plaintiff and the Class members suffered actual injury and damages as expressed herein, including foreseeable anxiety and mental anguish due to the exposure of their sensitive PII to malicious, financially-motivated hackers, pecuniary injury in the form of time and expense to mitigate the disclosure and/or significantly increased risk of exposure of PII to still other nefarious third parties.

59. Further, Plaintiff and the Class members face privacy and economic injuries from the imminent risk of misuse of other online accounts secured by the same PII exposed in the Data Breach.

60. Wherefore, Plaintiff prays for the relief set forth below.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

61. Plaintiff realleges the foregoing allegations as if fully set forth herein.

62. Plaintiff and the Class members are parties to a contract implied-in-fact with Defendant whereby Defendant offered to perform medical services and associated data security services for Plaintiff and the Class members in exchange for monetary consideration. The amount of such consideration included Defendant's provision of reasonable and adequate cybersecurity protections to prevent the unauthorized disclosure of Plaintiff's and the Class members' sensitive personal data.

63. As part of receiving medical services from Defendant, Plaintiff and the Class members were required to provide their PII to Defendant, which Defendant accepted, received, stored, and otherwise handled in order to, *inter alia*, provide them medical services for monetary consideration.

64. By accepting, receiving, storing, and handling Plaintiff's and the Class members' PII in order to provide them medical services in exchange for money, and by virtue of Plaintiff providing such PII in accordance with the same, a contract implied-in-fact was created by the aforementioned conduct of Plaintiff and Defendant with regard to the handling and management of such PII.

65. As part of these agreements, Plaintiff and the other Class members paid for, and Defendant was obligated to implement, reasonable cybersecurity standards in order to safeguard and prevent the unauthorized disclosure of Plaintiff's and Class members' PII.

66. Defendant's failure to implement adequate and reasonable data privacy and cybersecurity protocols which included ensuring that its file transfer service was up to date and secure, constitutes a breach of the contract implied-in-fact.

67. Plaintiff and the other Class members would not have provided and entrusted their PII to Defendant or would have sought other alternative care from Defendant's competitors, in the absence of an agreement with Defendant to reasonably safeguard their PII and to promptly notify them of security issues, including unauthorized disclosures of their PII.

68. Plaintiff and the other members of the Class fully performed their obligations under their implied contract to provide their PII prior to receiving medical care from Defendant.

69. Defendant's breach of its implied contracts with Plaintiff and the other class members was wanton and reckless considering that it had been informed by Accellion for years that it need to bring its FTA service up to date. Defendant knew, or had reason to know, that a breach of its duty to protect Plaintiff's and the Class members' sensitive PII from unauthorized disclosure would cause them anxiety and mental suffering.

70. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breaches of contract

71. Wherefore, Plaintiff prays for the relief set forth below.

COUNT III
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Class)
(In the alternative to Count II)

72. Plaintiff realleges the allegations contained in Paragraphs 1–60 as if fully set forth herein.

73. Plaintiff brings this Count in the alternative to Count II.

74. Plaintiff and the Class members are parties to a contract implied-in-fact with Defendant whereby Defendant offered to perform medical services and associated data security services for Plaintiff and the Class members in exchange for monetary consideration. The amount of such consideration included Defendant's provision of reasonable and adequate cybersecurity protections to prevent the unauthorized disclosure of Plaintiff's and the Class members' sensitive personal data.

75. As such, pursuant to a contract implied-in-fact, Defendant was obligated to take reasonable steps to secure and safeguard such PII and obligated to take reasonable steps following an unauthorized disclosure of the same.

76. Defendant had broad and exclusive contractual discretion to implement its cybersecurity practices in any manner of its choosing, including the timing of any data breach notifications.

77. By failing to protect Plaintiff's and the Class members' accounts in accordance with reasonable industry standards and failing to keep its FTA application up to date, Defendant abused its contractual discretion and acted in a manner inconsistent with the reasonable expectations of

the Plaintiff and the Class members. As such, Defendant breached the implied covenant of good faith and fair dealing.

78. By failing to notify Plaintiff and the Class members of the Data Breach for over three months, Defendant abused its contractual discretion and acted in a manner inconsistent with the reasonable expectations of the Plaintiff and the Class members. As such, Defendant breached the implied covenant of good faith and fair dealing.

79. Defendant's breach the implied covenant of good faith and fair dealing was wanton and reckless considering that it had been informed by Accellion for years that it need to bring its FTA service up to date. Defendant knew, or had reason to know, that a breach of the implied covenant leading to Plaintiff's and the Class members' sensitive PII being disclosed to third parties would cause them anxiety and mental suffering

80. The damages expressed herein as sustained by Plaintiff and the Class members were the direct and proximate result of Defendant's breach of the implied covenant of good faith and fair dealing and its abuse of contractual discretion.

81. Wherefore, Plaintiff prays for the relief set forth below.

COUNT IV
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*.
(On behalf of Plaintiff and the Class)

82. Plaintiff realleges the foregoing allegations as if fully set forth herein.

83. Pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*., ("PIPA"), Defendant was required to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII, and to notify them regarding any unauthorized disclosure in the most expedient time possible and without unreasonable delay.

84. Further, pursuant to Section 530/45 of PIPA, as a data collector that maintains and stores records containing the PII of Illinois residents, including Plaintiff and the other Class members, Defendant was required to implement and maintain reasonable security measures to protect their PII from the unauthorized access, acquisition, destruction, use, modification, or disclosure that resulted in the Data Breach.

85. Defendant's unlawful conduct alleged herein in failing to safeguard Plaintiff's and the Class member's PII, and subsequent failure to timely notify its patients that such PII had been compromised, is a direct violation of the Illinois Personal Information Protection Act.

86. Defendant was fully aware that its patients were necessarily relying on Defendant to follow proper industry standards in handling and securing PII in order to ensure the secure sharing of confidential sensitive information.

87. Nonetheless, Defendant failed to secure and protect Plaintiff's and the Class members' PII from the Data Breach by failing to implement industry standard practices for managing now-frequent ransomware attacks, and Defendant failed to directly notify them of the Data Breach within a reasonable period of time.

88. Plaintiff and the Class members relied on Defendant to protect their PII from the Data Breach and to notify them of the same within a reasonable time frame. Otherwise, Plaintiff and the other Class members would not have provided and entrusted their PII to Defendant and would not have entered into any transactions with Defendant.

89. After gaining knowledge of the Data Breach in December 2020 and that Plaintiff's and the other Class members' PII had been exposed, Defendant failed to immediately notify them of the Data Breach as required by PIPA, 815 ILCS 530/10.

90. Pursuant to Section 530/20 of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*. ("ICFA"), a violation of the Illinois Personal Information Protection Act, as alleged herein, is itself deemed an "unlawful practice" and violation under the ICFA, and Defendant has therefore violated the ICFA.

91. Defendant's ICFA violations, including its inadequate and unlawful cybersecurity practices and data breach notification practices, resulted in Plaintiff and the other Class members paying more for their medical care – the cost of which included adequate data protection and notification services – than such care was actually worth. Accordingly, Plaintiff and Class members have been injured and suffered actual damages to be proved at trial.

92. Wherefore, Plaintiff prays for relief as set forth below.

COUNT V
Unjust Enrichment
(on behalf of Plaintiff and the Class)
(in the alternative to Counts II & III)

93. Plaintiff realleges the allegations contained in Paragraphs 1–60 as if fully set forth herein.

94. Plaintiff brings this Count in the alternative to Counts II and III.

95. Plaintiff and the Class members conferred a benefit on Defendant in the form of monetary payment for services including reasonable data transfer and security services.

96. Defendant accepted such monetary benefit but grossly failed to provide reasonable data transfer and security services by failing to keep its FTA application, which it knew to be outdated, up to date, resulting in the breach of Plaintiff's and the Class members' sensitive PII.

97. Under principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit conferred upon it for reasonable data security services that it failed to provide.

98. Accordingly, because Defendant will be unjustly enriched if it is allowed to retain such funds, Defendant must pay restitution to Plaintiff and the other Class members in the amount which Defendant were unjustly enriched.

99. Wherefore, Plaintiff prays for the relief below.

COUNT VI
Invasion of Privacy - Public Disclosure of Private Facts
(on behalf of Plaintiff and the Class)

100. Plaintiff realleges the foregoing allegations as if fully set forth herein.

101. Through the services Defendant provided to Plaintiff and the Class members, Defendant came into possession of private medical information that is among the most sensitive private data, the disclosure of which would be, and is, highly offensive to any objective or reasonable person.

102. Publicity was given to such sensitive private medical information as a result of Defendant's grossly inadequate data security practices, including its failure to update its FTA application in accordance with Accellion's recommendations.

103. Such private medical information is not public.

104. As a result, Plaintiff and the Class members have suffered injuries and damages as described herein to be proven at trial.

105. Wherefore, Plaintiff plays for the relief below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class set forth above, respectfully request the Court order relief and enter judgement against Defendant:

A. Certifying the Class identified above and appointing Plaintiff as Class representative and the undersigned counsel as Class counsel;

B. Awarding Plaintiff and the Class appropriate relief, including actual, statutory, compensatory, and/or punitive damages, and restitution;

C. Granting injunctive relief requiring Defendant to implement commercially reasonable security measures to properly guard against any and all future cyberattacks and to provide prompt, reasonable notification in the event of such an attack;

D. Requiring Defendant to pay Plaintiff and the Class members' reasonable attorneys' fees, expenses, and costs; and

E. Any such further relief as this Court deems reasonable and just.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

Dated: January 21, 2022

Respectfully submitted,

SHARON MCFARLAND, individually and on behalf of a class of similarly situated individuals

By: /s/ Timothy P. Kingsbury
One of Plaintiff's Attorneys

Eugene Y. Turin (ARDC # 6317282)
Timothy P. Kingsbury (ARDC # 6329936)
MCGUIRE LAW, P.C.
55 W. Wacker Dr., 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
eturin@mcgpc.com
tkingsbury@mcgpc.com

Attorneys for Plaintiff and the Putative Class