Attorney No. 12453

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT – CHANCERY DIVISION

Sterile Technology, LLC *Plaintiff*, vs. Medefil, Inc., Pradeep Aggarwal, Sandeep Aggarwal, and Praveen Aggarwal, *Defendants*.	Case No. 17 L 716 Judge: Honorable Michael T. Mullen
Medefil, Inc., *Counter/Third-Party Plaintiff*, vs. Sterile Technology, LLC and Austin McDonald *Counter/Third-Party Defendants*.	
Austin McDonald, individually, and on behalf of himself and all others similarly situated, *Counter-Plaintiff*, vs. Medefil, Inc., *Counter-Defendant*.	

AUSTIN McDONALD'S SECOND
AMENDED COUNTERCLAIM AGAINST MEDEFIL, INC.

Austin McDonald ("McDonald"), by and through his attorneys, complains against Medefil, Inc. ("Medefil"), and alleges as follows:

Introduction

1. This action arises from Medefil's unlawful use of a fingerprint timeclock system for its employees and contractors.

2. Medefil required its employees and contractors to clock in and out of work with a timeclock that scanned and recognized their fingerprints without developing or providing its employees or contractors with a written policy regarding retention and destruction of their fingerprints; providing the proper authorization form or disclosures to its employees and contractors; informing its employees and contractors of the reason or length of time their fingerprints will be stored; obtaining its employees' and contractors' consent to disseminate their fingerprints to third parties; using reasonable care to store, transmit, or protect its employees' and contractors' fingerprints; providing the same or more-protective means to store, transmit, or protect its employees' and contractors' fingerprints that it uses for other confidential or sensitive information; and permanently destroying employees' and contractors' fingerprint data within three years of their last interaction with Medefil.

3. The Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq*., established in 2008, regulates the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g).

4. A fingerprint is a "biometric identifier," and information gathered from a fingerprint is "biometric information" pursuant to BIPA. 740 ILCS 14/10.

5. Medefil collected and retained McDonald's (and other contractors' and employees') biometric information as part of its timekeeping system.

6. Medefil disregards its employees' and contractors' statutorily protected privacy rights and unlawfully collects, stores, disseminates, and uses their biometric data in violation of BIPA. Specifically, Medefil violated and continues to violate BIPA because it did not and continues not to:

a. Provide a publicly available written retention schedule and guidelines for permanently destroying McDonald's fingerprints as required by BIPA;

b. Properly inform McDonald in writing that it collected and stored his fingerprints or of the specific purpose and length of time for which his fingerprints were being collected, stored, and used, as required by BIPA;

c. Receive a written release from McDonald to collect, store, or otherwise use his fingerprints, as required by BIPA;

d. Obtain consent from McDonald to disclose, redisclose, or otherwise disseminate his fingerprints to a third party, as required by BIPA;

e. Use reasonable care to store, transmit, and protect McDonald's fingerprints, as required by BIPA; and

f. Permanently destroy McDonald's fingerprints when his biometric data when the initial purpose for collecting his fingerprints was satisfied or within three years of his last interaction with Medefil.

7. Accordingly, McDonald seeks, the following relief: (1) an order declaring that Medefil's conduct violates BIPA; (2) a declaration that Medefil must cease the unlawful activities described herein; and (3) an order awarding damages to McDonald.

The Parties

8. McDonald is a resident of Newcastle County, Delaware and resides in Wilmington, Delaware.

9. Medefil is an Illinois corporation that is headquartered in Oakbrook and Glendale Heights, Illinois, and conducts business in the State of Illinois.

Jurisdiction

10. This Court has personal jurisdiction over the parties.

11. The amount in controversy meets or exceeds this Court's jurisdictional threshold.

Factual Allegations

I. The Biometric Information Privacy Act

12. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b).

13. Because "an overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information," the Illinois legislature passed BIPA in 2008 to regulate the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(d), (g).

14. To ensure compliance, BIPA provides individuals a private right of action. For each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations, and $5,000 or actual damages, whichever is greater, for intentional or reckless violations. *See* 740 ILCS 14/20. BIPA strictly regulates the manner in which entities collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

15. BIPA makes it unlawful for a company to, among other things, possess, collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information, unless it first:

a. Develops and complies with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first;

b. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used; the specific purpose and length of time the biometric identifier or biometric information is being collected, stored, and used; and receives a written release executed by the subject of the biometric identifier or biometric information;

c. Prohibits selling, leasing, trading, or otherwise profiting from an individuals' biometric identifiers or information.

d. Obtains the subject's consent to disclose, redisclose, or otherwise disseminate the subject's biometric identifiers and biometric information.

e. Establishes reasonable standards to store, transmit, and protect individuals' biometric identifiers and biometric information, including providing the same or more-protection to biometric identifiers and biometric information that it provides for other sensitive and confidential information.

740 ILCS § 14/15.

16. BIPA specifically applies to companies like Medefil, as a "private entity," defined as "any individual, partnership, corporation, limited liability company, association, or other group, however organized." 740 ILCS 14/10.

17. Further, a person's fingerprint is specifically included in BIPA's definition of "biometric identifier." *Id.* BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

18. The Illinois legislature, in passing BIPA, clearly recognized the imperative of keeping biometric information safe and secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Medefil's Violations of BIPA

19. Medefil is a sterile syringe and vial manufacturer. Medefil regularly employed a host of full-time employees, and regularly hired independent contractors or consultants for assistance on specific matters.

20. At some point during 2010 to 2013, Medefil began using one or more timeclocks that identify a user by scanning the user's fingerprint.

21. On information and belief, Medefil uses and has used hardware—*i.e.*, the fingerprint-operated timeclock—and software supplied by a third party that requires employees and contractors to use their fingerprint as a means of authentication.

22. Medefil requires its employees and contractors to clock-in and clock-out for attendance using their fingerprint. As such, when Medefil began using the fingerprint-operated timeclock, it required all employees and contractors, as a condition of working for Medefil, to have a fingerprint scanned.

23. Upon information and belief, Medefil failed and continues to fail to inform its employees and contractors that it disclosed or discloses their fingerprint data to at least one third-party vendor, and potentially others, that hosts the biometric data in its data centers; and to obtain written releases from employees before collecting and/or disseminating their fingerprints to third parties.

24. Additionally, Medefil fails to provide employees and contractors with a written, publicly available policy identifying its retention schedule and guidelines for permanently destroying fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by BIPA.

25. Medefil employees and contractors are aware that they have provided their fingerprint, but have not consented to do so and are not told exactly who is collecting their biometric data, the specific purpose of collecting their biometric data, where their biometric data will be transmitted and for what purposes, or for how long their biometric data will be retained. Medefil disregards its obligations and its employees' and contractors' statutory rights and, instead, unlawfully collects, stores, uses, and disseminates Medefil's employees' and contractors' biometric identifiers and information, without ever receiving the individuals' informed written consent as required by BIPA.

26. Medefil lacks retention schedules and guidelines for permanently destroying McDonald's biometric data. Upon information and belief, Medefil has not and will not destroy McDonald's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of McDonald's last interaction with the company.

27. Medefil did not tell its employees, contractors, or McDonald what might happen to their biometric data if and when Medefil merges with another company or worse, if and when Medefil's business folds or ceases operating, or when the other third parties that have received their biometric data fold or cease to operate.

28. Since Medefil neither publishes a BIPA-mandated data retention policy nor discloses the full purposes for their collection and use of biometric data, Medefil's employees and contractors do not know to whom Medefil sells, discloses, re-discloses, or otherwise disseminates their biometric data. Nor were McDonald and Medefil's employees and contractors told to whom Medefil currently discloses their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy or simply, if Medefil ceases to use the fingerprint timeclock.

29. By failing to promulgate and abide by a written, publicly available policy regarding the retention, transmission, and destruction of biometric identifiers and biometric information, and failing to inform and obtain consent, in writing, from employees and contractors to store, retain, or disseminate their biometric data, Medefil failed, and continues to fail, to use reasonable industry care to store, transmit, and protect biometric identifiers and/or biometric information.

30. On information and belief Medefil, failed and continues to fail to protect biometric identifiers and biometric information in the same or more protective manner than other confidential or sensitive information.

31. These violations have raised a material risk that McDonald's and other employees' and contractors' biometric data will be unlawfully accessed by third parties.

32. Through the actions detailed above, Medefil has violated McDonald's legal rights in violation of BIPA.

III. McDonald's Experiences at Medefil

33. McDonald began working with Medefil in 2010 and did so until March 2014. He provided sterile process consulting services to Medefil through Sterile Technology, LLC.

34. As a condition of his work for Medefil, McDonald was required to have his fingerprint scanned so that Medefil could use it as an authorization method to track his time and attendance.

35. Medefil required McDonald to scan his fingerprint each time he clocked in and out of work, like all other Medefil employees and contractors. McDonald was required to use the fingerprint timeclock during his time at Medefil, beginning when Medefil instituted the use of the fingerprint timeclock, and until McDonald stopped performing work for Medefil in 2014.

36. McDonald was required to scan his fingerprint using the fingerprint timeclock on, including but not limited to, the following dates: 8/19/2010; 8/20/2010, 8/23/2010, 9/7/2010, 9/8/2010, 9/9/2010, 9/10/2010, 9/14/2010, 9/15/2010, 9/16/2010, 9/17/2010, 9/20/2010, 9/21/2010, 9/24/2010, 9/30/2010, 10/6/2010, 10/7/2010, 10/8/2010, 10/12/2010, 10/16/2010, 12/2/2010, 12/21/2010, 12/28/2010, 12/29/2010, 12/30/2010, 1/3/2011, 1/5/2011, 1/6/2011, 1/7/2011, 1/8/2011, 1/10/2011, 1/11/2011, 1/12/2011, 1/14/2011, 1/18/2011, 1/19/2011, 1/20/2011, 1/21/2011, 1/26/2011, 1/27/2011, 2/1/2011, 2/7/2011, 2/25/2011, 2/28/2011, 3/2/2011, 3/10/2011, 4/18/2011, 4/19/2011, 4/20/2011, 4/21/2011, 5/3/2011, 5/4/2011, 5/6/2011, 5/9/2011, 5/11/2011, **after May 22, 2011:** 5/31/2011, 6/16/2011, 6/23/2011, 8/19/2011, **after August 19, 2011:** 8/20/2011, 8/22/2011, 8/23/2011, 8/24/2011, 8/30/2011, 8/31/2011, 9/1/2011, 9/2/2011, 9/6/2011, 9/12/2011, 9/13/2011, 9/14/2011, 9/20/2011, 9/23/2011, 9/26/2011, 9/29/2011, 9/30/2011, 10/11/2011, **after October 29, 2011:** 12/6/2011, 12/7/2011, 12/15/2011, 12/16/2011, 12/19/2011, 12/20/2011, 1/6/2012, 7/16/2012, 7/17/2012,

7/18/2012, 7/19/2012, 7/21/2012, 7/23/2012, 7/24/2012, 7/25/2012, 7/26/2012, 7/27/2012, 8/1/2012, 8/2/2012, 8/3/2012, 8/4/2012, 8/6/2012, 8/7/2012, 8/10/2012, 8/13/2012, 8/14/2012, 8/16/2012, 8/17/2012, 8/18/2012, 8/20/2012, 8/21/2012, 8/22/2012, 9/5/2012, 9/6/2012, 9/7/2012, 9/8/2012, 9/10/2012, 9/11/2012, 9/12/2012, 9/13/2012, 9/14/2012, 9/15/2012, 9/20/2012, 9/21/2012, 9/22/2012, 9/24/2012, 9/25/2012, 9/26/2012, 9/27/2012, 9/28/2012, 9/29/2012, 10/9/2012, 10/10/2012, 10/11/2012, 10/12/2012, 10/22/2012, 10/23/2012, 10/24/2012, 10/25/2012, 10/26/2012, 10/27/2012, 10/31/2012, 11/12/2012, 11/13/2012, 11/26/2012, 11/27/2012, 11/29/2012, 11/30/2012, 12/1/2012, 12/4/2012, 12/5/2012, 12/6/2012, 12/7/2012, 12/10/2012, 12/11/2012, 12/12/2012, 12/13/2012, 12/14/2012, 12/17/2012, 12/18/2012, **after January 2, 2013:** 1/4/2013, 1/7/2013, 1/8/2013, 1/9/2013, 1/15/2013, 1/16/2013, 1/17/2013, 1/18/2013, 1/19/2013, 1/22/2013, 1/23/2013, 1/24/2013, 1/29/2013, 1/30/2013, 1/31/2013, 2/1/2013, 2/2/2013, 2/4/2013, 2/5/2013, 2/6/2013, 2/7/2013, 2/12/2013, 2/13/2013, 2/14/2013, 2/15/2013, 2/27/2013, 2/28/2013, 3/1/2013, 3/4/2013, 3/5/2013, 3/6/2013, 3/7/2013, 3/15/2013, 3/18/2013, 3/21/2013, 3/25/2013, 3/26/2013, 4/1/2013, 4/2/2013, 4/5/2013, 4/8/2013, 4/9/2013, 4/10/2013, 4/16/2013, 4/17/2013, 4/18/2013, 4/19/2013, 4/20/2013, 4/22/2013, 4/23/2013, 4/29/2013, 5/1/2013, 5/2/2013, 5/3/2013, 5/8/2013, 5/9/2013, 5/13/2013, 5/15/2013, 5/16/2013, 5/21/2013, 5/22/2013, 5/24/2013, 5/31/2013, 6/3/2013, 6/6/2013, 6/10/2013, 6/11/2013, and 7/13/2013. At no point prior to any of those dates did Medefil comply with the notice, safeguards, or other requirements of BIPA.

37. For example, after May 22, 2011, on the dates included above, Medefil: 1) captured, stored, and retained McDonald's biometric data; 2) possessed McDonald's biometric data without developing or making publicly available a written policy with retention schedules and destruction guidelines for biometric data; 3) collected, captured, and obtained McDonald's biometric data without

informing him in writing that his biometric data was being collected or stored, informing him of the specific purpose and length of term it would collect, store, and use his biometric data, or obtaining his signed consent; 4) disclosed McDonald's biometric data without obtaining his consent; 5) possessed McDonald's biometric data without using reasonable care to store, transmit, or protect his biometric data, or provide the same or more protection for McDonald's biometric information that it provides to other sensitive or confidential information; and 6) failed to permanently destroy McDonald's biometric data when the initial purpose for obtaining his biometric identifiers or information has been satisfied or within three years of his last interaction with Medefil.

38. After August 19, 2011, on the dates included above, Medefil: 1) captured, stored, and retained McDonald's biometric data; 2) possessed McDonald's biometric data without developing or making publicly available a written policy with retention schedules and destruction guidelines for biometric data; 3) collected, captured, and obtained McDonald's biometric data without informing him in writing that his biometric data was being collected or stored, informing him of the specific purpose and length of term it would collect, store, and use his biometric data, or obtaining his signed consent; 4) disclosed McDonald's biometric data without obtaining his consent; 5) possessed McDonald's biometric data without using reasonable care to store, transmit, or protect his biometric data, or provide the same or more protection for McDonald's biometric information that it provides to other sensitive or confidential information; and 6) failed to permanently destroy McDonald's biometric data when the initial purpose for obtaining his biometric identifiers or information has been satisfied or within three years of his last interaction with Medefil.

39. After October 29, 2011, on the dates included above, Medefil: 1) captured, stored, and retained McDonald's biometric data; 2) possessed McDonald's biometric data without developing or making publicly available a written policy with retention schedules and destruction guidelines for biometric data; 3) collected, captured, and obtained McDonald's biometric data without informing

him in writing that his biometric data was being collected or stored, informing him of the specific purpose and length of term it would collect, store, and use his biometric data, or obtaining his signed consent; 4) disclosed McDonald's biometric data without obtaining his consent; 5) possessed McDonald's biometric data without using reasonable care to store, transmit, or protect his biometric data, or provide the same or more protection for McDonald's biometric information that it provides to other sensitive or confidential information; and 6) failed to permanently destroy McDonald's biometric data when the initial purpose for obtaining his biometric identifiers or information has been satisfied or within three years of his last interaction with Medefil.

40. After January 2, 2013, on the dates included above, Medefil: 1) captured, stored, and retained McDonald's biometric data; 2) possessed McDonald's biometric data without developing or making publicly available a written policy with retention schedules and destruction guidelines for biometric data; 3) collected, captured, and obtained McDonald's biometric data without informing him in writing that his biometric data was being collected or stored, informing him of the specific purpose and length of term it would collect, store, and use his biometric data, or obtaining his signed consent; 4) disclosed McDonald's biometric data without obtaining his consent; 5) possessed McDonald's biometric data without using reasonable care to store, transmit, or protect his biometric data, or provide the same or more protection for McDonald's biometric information that it provides to other sensitive or confidential information; and 6) failed to permanently destroy McDonald's biometric data when the initial purpose for obtaining his biometric identifiers or information has been satisfied or within three years of his last interaction with Medefil.

41. Medefil stored McDonald's fingerprint data in its databases or the databases of the third party vendor running the timeclock, and, upon information and belief, continues to do so.

42. Medefil never informed McDonald of the specific limited purposes or length of time for which Medefil collected, stored, used and/or disseminated his biometric data.

43. Medefil never informed McDonald of any biometric data retention policy developed by Medefil, nor has he ever been informed of whether Medefil will ever permanently delete his biometric data or has deleted his biometric data.

44. McDonald never signed a written release allowing Medefil to collect, store, use or disseminate his biometric data.

45. Upon information and belief, Medefil failed to permanently destroy McDonald's fingerprints when the initial purpose for Medefil collecting or obtaining his fingerprint data was satisfied or within three years of McDonald's last interaction with Medefil, whichever came first.

46. McDonald has continuously and repeatedly been exposed to the risks and harmful conditions created by Medefil's multiple violations of BIPA, as alleged herein.

47. No amount of time or money can compensate McDonald if his biometric data is compromised by the lax procedure through which Medefil captured, stored, used, and disseminated his biometrics.

48. McDonald would not have provided his fingerprint and biometric data to Medefil if he had known that it would retain such information for an indefinite period of time without his consent or that this information was being shared to third parties.

49. McDonald has suffered and continues to suffer an injury-in-fact based on Medefil's violations of his legal rights. Medefil intentionally interfered with McDonald's ability and right to possess and control his own sensitive biometric data. Additionally, McDonald suffered an invasion of a legally protected interest when Medefil secured his personal and private biometric data at a time when it had no right to do so, a gross invasion of his right to privacy. BIPA protects individuals like McDonald from this precise conduct. Medefil had no lawful right to secure his data or share it with third parties absent a specific legislative license to do so.

50. McDonald also suffered and continues to suffer an informational injury because Medefil failed and continues to fail to provide him with information to which he was entitled by statute. Through BIPA, the Illinois legislature has created a right: a person's right to receive certain information prior to another person or entity securing their highly personal, private, and proprietary biometric data; and an injury—not receiving this extremely critical information.

51. On information and belief, McDonald also suffered and continues to suffer an injury-in-fact because Medefil improperly disseminated his biometric identifiers and/or biometric information to one or more third parties that hosted the biometric data in their data centers, in violation of BIPA.

52. McDonald also suffered and continues to suffer an injury-in-fact because Medefil failed and continues to fail to use reasonable care regarding the storage, transmission, and protection of his biometric identifiers and/or biometric information, and failed and continues to fail to protect his biometric identifiers and/or biometric information in the same or more-protective manner than other confidential and sensitive information.

53. McDonald has suffered actual and ongoing harm in the form of monetary damages for the value of the collection and retention of his biometric data; in the form of unauthorized disclosure of his confidential biometric data to third parties; in the form of interference with his right to control and possess his confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

54. As McDonald is not required to allege or prove actual damages in order to state a claim under BIPA, he seeks statutory damages under BIPA as compensation for the injuries cause by Medefil.

55. McDonald brings this action, individually, on behalf of a Class defined as: All employees, vendors, and contractors of Medefil who used a hand geometry scanner for timekeeping

purposes. The Proposed Class meets the requirements for class certification under 735 ILCS 5/2-801, *et seq.*:

A. **Numerosity**: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identity of individual members of the Class is unknown at this time, such information being in the sole possession of Medefil and obtainable by McDonald only though the discovery process, McDonald believes, and on that basis alleges, that the Class consists of more than 50 individuals. The exact number of Class members can be determined based on Medefil's records;

B. **Commonality and Predominance**: Common questions of law and fact exist as to all members of the Class. These questions predominate over questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

1. whether Medefil collected, captured, or otherwise obtained McDonald's and Class members' biometric identifiers or biometric information;

2. whether Defendant used McDonald's and the Class's fingerprints to identify them;

3. whether Medefil informed McDonald and Class members in writing of Medefil's purposes for collecting, using, and storing their biometric identifiers or biometric information;

4. whether Medefil informed McDonald and Class members in writing of the length of time that their biometric identifiers or biometric information would be stored, collected and used;

5. whether Medefil informed McDonald and Class members in writing of the purpose and length of time their biometric identifiers or biometric information would be stored, collected, and used prior to obtaining their biometric identifiers or biometric information;

6. whether Medefil obtained a signed written release from McDonald and Class members to collect, use, and store their biometric identifiers or biometric information;

7. whether Medefil has disclosed or re-disclosed McDonald's and Class members' biometric identifiers or biometric information;

8. whether Medefil obtained McDonald's and Class members' consent to disclose or re-disclose their biometric identifiers or biometric information;

9. whether Medefil has sold, leased, traded, or otherwise profited from McDonald's and the Class's biometric identifiers or biometric information;

10. whether Medefil developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction, whichever occurs first;

11. whether Medefil complied with any such written policy (if one existed);

12. whether Medefil's violations of BIPA were committed negligently; and

13. whether Medefil's violations of BIPA were committed recklessly or willfully.

C. **Typicality:** McDonald has the same interest in this matter as all Class members, and McDonald's claims arise out of the same set of facts and conduct as the claims of all Class members. McDonald's and Class members' claims all arise out of the uniform conduct of Medefil's failure to develop and adhere to a publicly available policy, securing written consent prior to the collection of biometric identifiers and/or information, and obtaining consent prior to the disclosure of biometric identifiers to a third-party;

D. **Adequacy:** McDonald has no interest that conflicts with the interests of the Class and is committed to pursuing this action vigorously. McDonald has retained counsel

competent and experienced in complex class action litigation. Accordingly, McDonald and his counsel will fairly and adequately protect the interests of the Class.

E. **Superiority:** A class action is superior to all other available means of fair and efficient adjudication of the claims of McDonald and members of the Class. The injury suffered by each individual Class member is relatively small compared to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by McDonald's conduct. It would be virtually impossible for individual Class members to effectively redress the wrongs done to them. Even if Class members could afford individualized litigation, the court system could not. Individualized litigation would increase delay and expense to all parties, and to the court system, because of the complex legal and factual issues of this case. Individualized rulings and judgments could result in inconsistent relief for similarly-situated individuals. 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; and

F. Medefil has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief and corresponding declaratory relief with respect to the Class as a whole.

Count I
Violations of the Illinois Biometric Information Privacy Act[1]
740 ILCS § 14/1, *et seq.*

56. McDonald re-alleges paragraphs 1-54 as if set forth fully in this Count I.

[1] The Court's March 4, 2020 Order limited McDonald's BIPA claim to violations that occurred "post-bankruptcy petition." McDonald pleads pre-bankruptcy petition claims for the purposes of preserving the previously dismissed claims for appeal. *See Tabora v. Gottlieb Memorial Hosp.*, 279 Ill. App. 3d 108, 114 (1st Dist. 1996) ("A simple paragraph or footnote in the amended pleadings notifying defendants and the court that plaintiff [is] preserving the dismissed portions of his former complaints for appeal [is] sufficient. . . .").

57. Medefil is a "private entity" under BIPA. *See* 740 ILCS §14/10.

58. McDonald is an individual who had his "biometric identifier" collected by Medefil (in the form of fingerprints), as explained in detail above. *See* 740 ILCS §14/10.

59. McDonald biometric identifier was used to identify him and, therefore, constitutes "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

60. Medefil is required to establish and maintain a satisfactory biometric data retention—and, importantly, deletion—policy. Specifically, Medefil must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 14/15(a).

61. Medefil failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information, as required by 740 ILCS §14/15(a).

62. On information and belief, Medefil violated and continues to violate BIPA because it lacks retention schedules and guidelines for permanently destroying McDonald's biometric data and has not and will not destroy McDonald's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of his last interaction with the company.

63. Medefil must obtain informed written consent from its employees and contractors before acquiring their biometric data. Specifically, Medefil cannot "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless it first: (1) informs the subject . . . that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored,

and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information. . . ." 740 ILCS § 14/15(b).

64. Medefil has not informed McDonald that it collected or stored his biometric identifiers and biometric information; has not informed McDonald in writing of the specific purposes and length of term for which a biometric identifier or biometric information is being collected, stored, and used, as required by 740 ILCS 14/15(b)(1)-(2).

65. Medefil systematically and automatically collected, used, and stored McDonald's biometric identifiers and biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

66. BIPA prohibits Medefil from disclosing McDonald's biometric identifier or biometric information without first obtaining consent from McDonald for that disclosure. *See* 740 ILCS 14/15(d)(1).

67. On information and belief, Medefil systematically and automatically disclosed, redisclosed, or otherwise disseminated McDonald's biometric identifiers and/or biometric information without first obtaining the consent, as required by 740 ILCS § 14/15(d)(1).

68. Medefil failed to store, transmit, and protect McDonald's biometric identifiers and/or biometric information using the reasonable standard of care for its industry as required by 740 ILCS § 14/15(e)(1).

69. Medefil failed to store, transmit, and protect McDonald's biometric identifiers and/or biometric information in the same or more protective manner as its stores, transmits, and protects other confidential and sensitive information, as required by 740 ILCS § 14/15(e)(2).

70. Medefil has repeatedly failed to comply with the mandates of BIPA discussed above, and did so either negligently or intentionally and recklessly.

71. By failing to develop and follow a written policy regarding the retention and destruction of biometric identifiers and/or biometric information, failing to inform McDonald in writing that his biometric identifiers and/or biometric information is being collected or stored, failing to inform McDonald in writing of the specific purposes and length of term for which his biometric identifiers and/or biometric information is being collected, stored, and used, failing to obtain a written release and consent from McDonald to collect and disclose his biometric identifiers and/or biometric information, failing to use reasonable industry standards to store, transmit, and protect McDonald's biometric identifiers and/or biometric information, and failing to protect McDonald's biometric identifiers and/or biometric information the same manner it protects other confidential and sensitive information, a separate and distinct violation of BIPA occurred at least on each instance that McDonald scanned his fingerprint with the fingerprint timeclock.

72. As set forth above, most of the violations alleged herein occurred after May 22, 2011, August 19, 2011, October 29, 2011, and January 2, 2013.

73. McDonald seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect McDonald's interests by requiring Medefil to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

Prayer for Relief

Wherefore, Austin McDonald respectfully requests that this Court enter an Order:

A. Declaring that Medefil's actions, as set forth above, violate BIPA;

B. Awarding McDonald statutory damages of $5,000 for each intentional or reckless violation of BIPA, or in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1)-(2);

C. Declaring that Medefil's actions, as described above, were intentional or reckless, or in the alternative, that Medefil's actions, as described above were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect McDonald's interests, including an Order requiring Medefil to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

E. Grant McDonald an award of reasonable attorneys' fees and costs and other ligation expenses pursuant to 740 ICLS § 14/20(3);

F. Awarding McDonald pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as this Court deems equitable, just and proper.

Dated: August 23, 2023

Respectfully Submitted,

s/ Nickolas J. Hagman

Nickolas J. Hagman
Paige L. Smith
CAFFERTY CLOBES MERIWETHER & SPRENGEL, LLP
135 S. LaSalle Street, Suite 3210
Chicago, Illinois 60603
Phone: (312) 782-4880
Facsimile: (312) 782-4485
nhagman@caffertyclobes.com
psmith@caffertyclobes.com
Attorney No. 12453

Anthony F. Fata
KIRBY MCINERNEY LLP
211 W. Wacker Dr., Suite 550
Chicago, IL 60606
Phone: (312) 767-5180
afata@kmllp.com

Attorneys for Austin McDonald

CERTIFICATE OF SERVICE

I, Nickolas J. Hagman, an attorney, hereby certify that I caused ***Austin McDonald's Second Amended Counterclaim Against Medefil, Inc.*** to be served upon the following by electronic mail:

Melissa A. Siebert
Erin Bolan Hines
Cozen O'Connor
123 N. Wacker Dr. Suite 1800
Chicago, Illinois 60606
msiebert@cozen.com
ebolanhines@cozen

Shomshon Moskowitz
Steven Ruffalo
Fuchs & Roselli, Ltd.
200 South Wacker Drive, Suite 600
Chicago, Illinois 60606
smoskowitz@frltd.com
sruffalo@frltd.com

Dated: August 23, 2023

s/Nickolas J. Hagman
Nickolas J. Hagman