E-FILED
Tuesday, 15 February, 2022 09:26:56 AM
Clerk, U.S. District Court, ILCD

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
PEORIA DIVISION

ASHLEY HIATT, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	No. 22-cv-1044
v.	)	
KOSE AMERICA, INC.,	)	JURY DEMANDED
Defendants.	)	

CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff Ashley Hiatt ("Plaintiff"), individually and on behalf of all other similarly situated individuals, brings this Class Action Complaint against Defendant Kose America, Inc. ("Defendant") for violations of the Illinois Biometric Information Privacy Act ("BIPA" or "the Act"), 740 ILCS 14/1 *et seq*. Plaintiff alleges as follows upon personal knowledge as to herself and her own acts and experiences and, as to all other matters, upon information and belief including investigation conducted by her attorneys:

NATURE OF THE ACTION

1. Decorté is a luxury cosmetics brand whose products are sold in retail stores and online.

2. Defendant sells and distributes Decorté products on its website https://decortecosmetics.com.

3. In approximately March 2021, Defendant launched a "Virtual Services" tool on its website that contains two artificial intelligence-driven features: a Virtual Try-On feature for cosmetics and a Skin Diagnostics feature.

4. Defendant's Virtual Try-On tool enables consumers to see how beauty products will look on them via Defendant and its Virtual Try-On technology accessing the camera on the consumer's device, such as a mobile phone, or having the consumer upload their picture from a file, and then collecting, capturing and obtaining the consumer's facial biometric data and identifiers in order to show the consumer how the product will look on their face.

5. Defendant's Skin Diagnostics feature measures overall skin health, moisture, texture, wrinkles, dark spots, and dark circles. The virtual skin diagnostic tool provides scores for these categories and will recommend products using the scores.

6. To use Defendant's Skin Diagnostics feature, a consumer snaps or takes a photo of themselves on their mobile phone which Defendant then uses to perform its analysis.

7. As set forth below, Defendant's Virtual Services utilize facial detection and facial recognition technology. Through both of its virtual features, Defendant collects, captures, possesses, or otherwise obtains consumers' facial biometric information and identifiers to analyze consumers' face and skin to show how each consumer how the beauty products will look on their face and to recommend beauty products.

8. In doing so—and in demonstrating to consumers what beauty products may look like on them—Defendant's Virtual Services' face-scanning technology extracts, collects, captures, possesses, obtains and uses consumers' unique facial geometry and landmark data as well as their biometric information and biometric identifiers, as defined by the Illinois Biometric Information Privy Act ("BIPA"), 740 ILCS 14/1 *et seq*.

9. Defendant is violating BIPA by, among other things, failing to inform consumers that Defendant is collecting, capturing, possessing, obtaining and using their biometric information and identifiers, failing to inform consumers about how and where their biometric data is being

collected, captured, obtained or retained, and failing to obtain informed written consent from consumers to capture, collect, possess or otherwise obtain their biometric information and identifiers.

10. Defendant is depriving consumers of any meaningful opportunity to make an informed decision about the collection and use of their own biometrics, in direct violation of BIPA.

PARTIES, JURISDICTION, AND VENUE

11. Plaintiff Ashley Hiatt is an individual citizen of the State of Illinois who resides in the Central District of Illinois.

12. Defendant Kose America, Inc. is a corporation organized under the laws of the State of Delaware.

13. Defendant's principal place of business is New York, New York.

14. Defendant does business throughout the United States of America, in Illinois, and as it is related to Plaintiff, in this district.

15. Defendant engages in online beauty and cosmetic product retailing. Defendant sells products via its website https://decortecosmetics.com, including in Illinois to Illinois residents, and ships Decorté products into Illinois on a regular basis.

16. Defendant purposely directs marketing and sales of Decorté products into the State of Illinois and to Illinois citizens through its website https://decortecosmetics.com and the "Virtual Services" feature on its website.

17. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §1332 in that plaintiff and defendant are citizens of different states and the amount in controversy exceeds $75,000, exclusive of interests and costs.

18. Jurisdiction is also proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d) ("CAFA"), because: (i) the proposed class consists of well over 100 members; (ii) the parties are minimally diverse, as members of the proposed class, including plaintiff, are citizens of a state different from defendant's home states; and (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs. The estimated number of Illinois residents impacted by Defendant's conduct in Illinois is at least 4,000.

19. This Court has personal jurisdiction over Defendant because, inter alia, the alleged tortious acts and conduct that are the subject of this action occurred in Illinois and Defendant does business in Illinois, targets business activity in Illinois, ships its products into Illinois, and purposefully avails itself of the laws, protections, and advantages of doing business in Illinois with Illinois consumers like Plaintiff.

20. Defendant's "Virtual Services" feature is offered directly to Illinois citizens. Defendant targets and uses its "Virtual Services" feature to help it sell Decorté products to Illinois citizens, and Defendant does in fact sell, ship and deliver Decorté products to Illinois citizens who use Defendant's "Virtual Services" feature.

21. Venue is proper in this District because Defendant conducts business transactions in this District, Defendant resides in this District within the meaning of 28 U.S.C. § 1391(c)(2) and the causes of action arose, in substantial part, in this District. Venue is additionally proper because plaintiff resides in this District.

DEFENDANT'S BIOMETRIC FACIAL-SCANNING OF ILLINOIS CONSUMERS

22. Defendant is a subsidiary of Kose Corporation, a Japanese multinational personal care company whose products include cosmetics, skin care, and hair products.

23. Kose Corporation owns the Decorté brand.

24. Defendant sells and distributes Decorté branded products in the United States, State of Illinois and this District.

25. Defendant uses a website https://decortecosmetics.com/ to sell Decorté cosmetic products in the United States and in this District, including makeup, lip stick, and skin care products.

26. Defendant enters into a contractual relationship with each Illinois resident who makes a purchase from Defendant.

27. Defendant's website requires consumers who make a purchase to enter a shipping address, including the state and zip code. Illinois is one of the ship-to options from which consumers must choose.

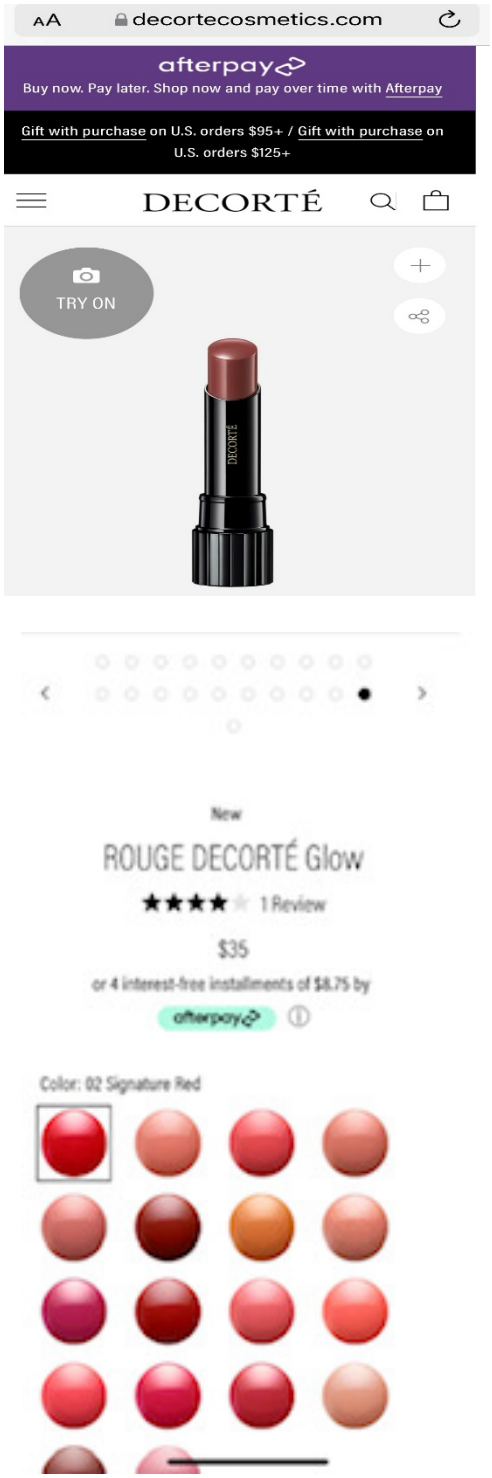
28. Defendant's website offers free shipping to Illinois citizens and their Illinois mailing addresses for orders exceeding a certain dollar amount.

29. Defendant knowingly and intentionally sells and ships products into Illinois on a regular basis.

30. As part of Defendant's sales pitch on its website to consumers in Illinois like Plaintiff, and through the use of facial detection, facial recognition, augmented reality and artificial intelligence technology, Defendant offers a "Virtual Services" feature that allows consumers to virtually try on makeup and other products and to help select and buy beauty and cosmetics products.

31. As illustrated below, if a consumer uses their mobile phone to view a Decorté lipstick webpage (https://decortecosmetics.com/collections/lips/products/rouge-decorte-glow), Defendant provides a link to its Virtual Try-On so that the consumer can virtually try on the various

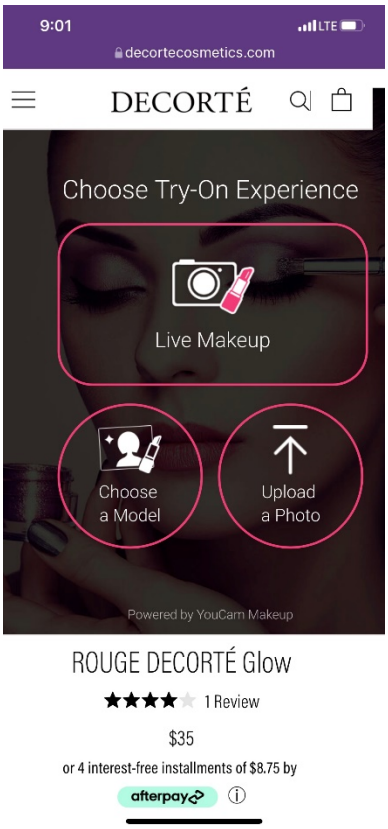
colors offered in the particular lipstick product, as illustrated here on the left side and just above the lipstick:



(Image captured from Defendant's mobile website (https://decortecosmetics.com/collections/lips/products/rouge-decorte-glow),

last visited January 24, 2022)

32. By clicking on the "TRY-ON" hyperlink, users of Defendant's webpage are prompted with the following:



(Image captured from Defendant's mobile website (https://decortecosmetics.com/collections/lips/products/rouge-decorte-glow), last visited January 24, 2022)

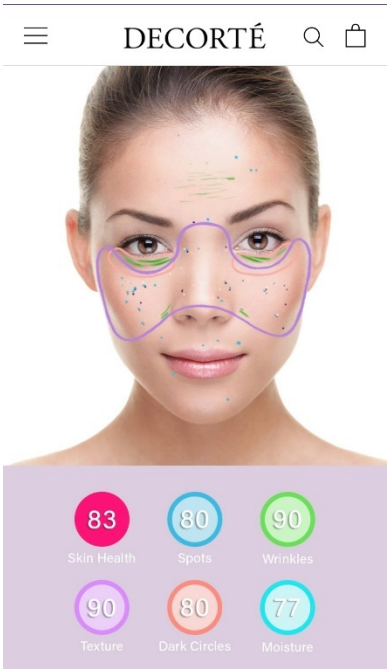
33. Defendant's Virtual Try-On feature is offered for various products such as eye shadow and lipstick.

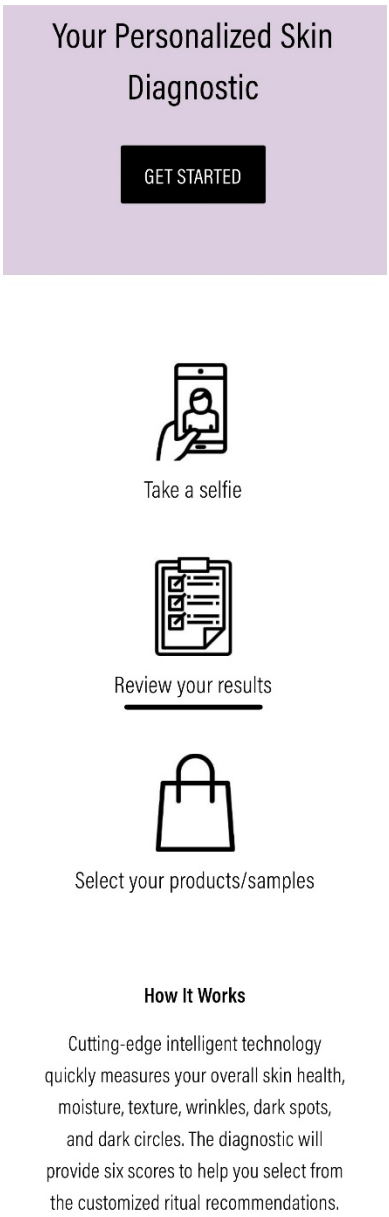
34. The hyperlink to the Virtual Try-On feature is located on several of Defendant's mobile webpages for various cosmetics and beauty products.

35. When a visitor "Allows" Defendant to access the camera on their device when using the "Live Makeup" option or when a visitor uses the "Upload a Photo" option, Defendant collects,

captures, possesses, or otherwise obtains a consumer's image and facial biometric data and identifiers in order to show the visitor how the product will look on his or her face.

36. If a consumer uses their mobile phone to view Defendant's virtual skincare diagnostics webpage (https://decortecosmetics.com/pages/skin-diagnostics-start), Defendant provides a link to its skin diagnostics webpage where the consumer can virtually try on the various colors offered in the particular lipstick product:





(Image captured from Defendant's mobile website https://decortecosmetics.com/pages/skin-diagnostics-start, last visited January 24, 2022)

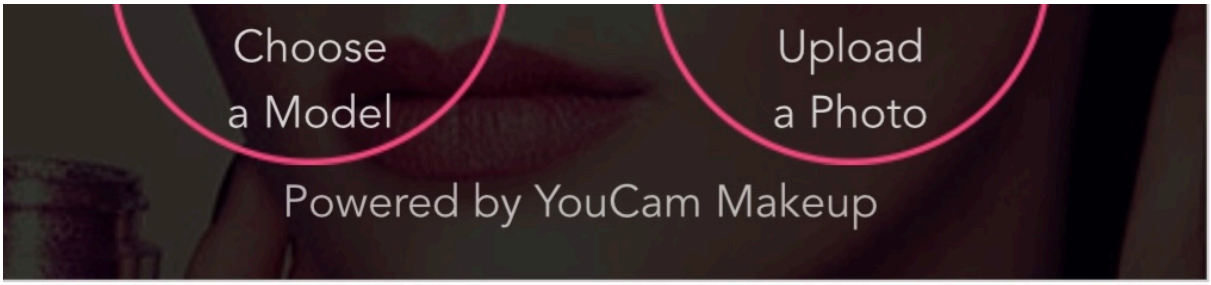
37. A consumer may start the skin diagnostics tool by clicking the "Get Started" option and submitting a "selfie" or photo of themselves.

38. Defendant's Virtual Services feature and technology uses an algorithm that scans the face in the consumer's photo, image or video to detect facial features or landmarks and

calculates a unique digital map of the face (*i.e.*, a face template) based on geometric attributes such as the distance between various facial features.

39. In performing its function, Defendant's Virtual Services feature employs facial recognition and facial detection technology.

40. As shown on Defendant's webpage, at Defendant's choice in developing its Virtual Services tools, Defendant's Virtual Try-On tool and Skin Diagnostic tool is "powered" by YouCam Makeup:



41. On or about March 2, 2021, Defendant announced the launching of its virtual Skin Diagnostics feature and tool that used Perfect Corporation's YouCam technology.[1]

42. In other words, in developing its Virtual Services, Defendant incorporated YouCam Makeup and YouCam software ("YouCam Makeup") into its Virtual Services try-on and skin diagnostic feature.

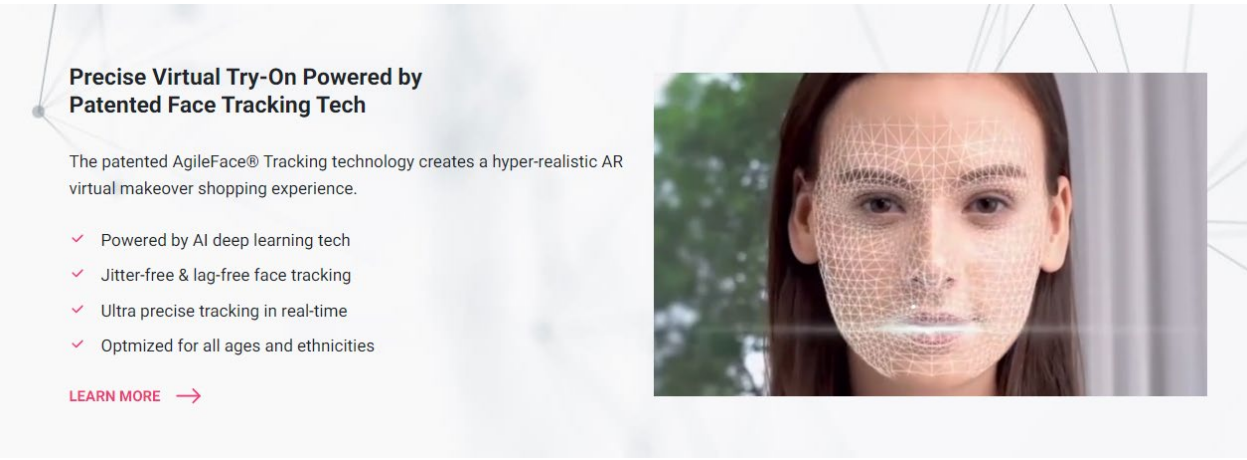
43. The YouCam Makeup application is owned by a Taiwanese artificial intelligence and augmented reality beauty tech solutions company (i.e., Perfect Corporation) that provides facial mapping and virtual try-on technology services for beauty brands, including Decorté.

[1] https://www.prnewswire.com/news-releases/decorte-partners-with-perfect-corp-to-launch-youcams-new-artificial-intelligence-driven-skincare-diagnostic-technology-that-debuted-at-ces-2021-301238229.html

44. Defendant's Virtual Services feature uses software that utilizes facial geometry data, facial detection, and facial recognition technology to digitally apply cosmetic products to the images and real-time videos of consumers' faces.

45. For example, the Virtual Services feature conducts a facial geometry scan of live camera images and photos and collects, captures or otherwise obtains datapoints from reading the geometry of the consumer's face, e.g., the distance between eyes, the distance from forehead to chin, etc. The Virtual Services also identifies and records data and identifiers regarding facial landmarks on a consumer's face. The Virtual Services technology collects, captures, obtains and uses this data and these datapoints and identifiers in the process of digitally applying the beauty products to a customer's face in the image.

46. The YouCam Makeup application and technology operates by collecting, capturing, obtaining and recording the facial landmarks and facial geometry of faces in the Virtual Services users' photos and images, regardless of whether the photo or image is taken by web or phone camera while using the Virtual Services feature, uploaded to the feature, or captured via a live web or phone camera feed. These facial-geometry scans are used to identify the shape and features of the user's face in order to accurately overlay the virtual makeup product onto the image provided. This technology is illustrated by the website of the YouCam Makeup developer:



(Image captured from https://www.perfectcorp.com/business/products/virtual-makeup, last visited on January 19, 2022)

47. According to the developer of YouCam Makeup, the application uses "proprietary AgileFace technology to deliver ultra-accurate face tracking" and "precise makeup product application that stays in the correct position with head movements, allowing them to examine the look and see the tutorials form multiple angles."[2]

48. According to one article, the YouCam Makeup application previously "use[d] 100 points to tracking on the face for facial recognition and skin-tone matching. Its technology can recognize the role of lighting and recommend products for users' specific skin types and concerns."[3]

49. Currently, as stated on the YouCam developer's website, the YouCam Makeup application now uses "Over 200+ facial landmark tracking points in real-time" to detect, track, collect, capture and obtain unique facial landmarks and facial geometry of consumers:

(Image captured on Perfect Corporation's website

[2] Perfect Corp., YouCam Tutorial, https://www.perfectcorp.com/business/products/youcam-tutorial (last visited January 18, 2022).
[3] Leah Prinzivalli, How YouCam Makeup is building a beauty AR empire, Glossy (July 5, 2018), https://www.glossy.co/new-face-of-beauty/how-youcam-makeup-is-building-a-beauty-ar-empire/.

https://www.perfectcorp.com/business/technologies/agile-face-tracking, last visited January 18, 2022)

50. The developer of the YouCam Makeup application markets its product and service in part on YouCam Makeup's ability to capture, obtain, and use consumers' unique facial landmarks, geometry and identifiers of consumers to market products to them.

51. As the developer of the YouCam Makeup application states on its website, the YouCam Makeup technology uses AgileFace face tracking technology and "AgileFace is a patent-pending face tracking technology that enables an ultra-accurate virtual makeover with extreme performance." (https://www.perfectcorp.com/business/technologies/agile-face-tracking, last visited January 18, 2022).

52. The January 21, 2020 trademark application for the mark "AgileFace," filed with the United States Patent and Trade Office, describes the YouCam Makeup software program associated with the AgileFace mark as follows: "Computer software, downloadable computer software, mobile application software and software development kit for image capturing, tracking, recognition and post-processing" and "Software as a service for image capturing, tracking, recognition and post-processing; computer and mobile device software application design for image capturing, tracking, recognition and post-processing."[4]

53. The YouCam Makeup application uses facial recognition and facial detection technology to detect, capture, obtain and track unique facial data and facial identifiers of individuals who use the application.

[4] https://uspto.report/TM/90195994/APP20200924103041/)

54. Defendant and its Virtual Tester use facial recognition and facial detection technology to detect, capture, obtain and track unique facial data and facial identifiers of the individuals who use the Virtual Tester feature.

55. The facial data and identifiers that Defendant and its Virtual Tester detects, captures, collects, tracks or obtains is Biometric Information and Biometric Data as defined by BIPA.

56. The YouCam App developer even states in its privacy policy that the technology and application "collects, processes, and stores your Biometric Information through our mobile applications…For example, our YouCam Makeup application allows users to undergo a true-to-life virtual makeover using our world-class facial mapping technology. Specifically, for the processing of facial characteristics information, we will only detect your facial feature vectors in order to apply real-time virtual try-on effects thereon, upon your usage of our Apps." (https://www.youcamapps.com/info/privacy.action, last visited January 19, 2022.[5]

57. Defendant, however, does not inform or provide written notice to consumers who use its Virtual Services feature that it is collecting, capturing, tracking or obtaining unique facial geometry and facial landmark data and information or the specific purpose and length of term for which Defendant's Virtual Services platform is capturing, collecting, tracking, possessing, obtaining or using such data and information. Nor does Defendant obtain consumers' informed written consent before capturing, collecting, tracking or otherwise obtaining such data and information.

[5] The Youcamapps website and privacy policy webpage are not part of or hyperlinked to Defendant's https://decortecosmetics.com webpages.

58. Companies that collect, capture, possess, or otherwise obtain the biometric information and identifiers of online visitors are required to inform them and then obtain sufficient consent before collecting, capturing, possessing, or otherwise obtaining such personal data.

59. Moreover, companies generally need to notify such individuals about the specific purpose and length of time that the data will be collected, stored, used, or otherwise obtained. As set forth herein, Defendant did not undertake any of these practices.

SUBSTANTIVE ALLEGATIONS

60. Much like fingerprints, voiceprints, and retinal patterns, facial geometry, facial identifiers and each face template is unique to, and can be used to identify, a particular person.

61. BIPA expressly obligates Defendant to obtain an executed, written release from an individual, prior to capturing, collecting, obtaining and/or storing of an individual's biometric identifiers or biometric information, especially a facial geometry scan and biometric information and identifiers derived from it.

62. BIPA obligates Defendant to inform its Virtual Services users in writing that a biometric identifier or biometric information is being collected, captured and/or obtained; to tell its potential customers in writing how long it will use and/or store their biometric data or information and any purposes for which biometric information is being captured, collected, obtained or used; and to make available a written policy disclosing when it will permanently destroy such information.

63. BIPA makes all of these requirements a *precondition* to the collection or recording of face geometry scans or other associated biometric information.

64. Under the Act, no biometric identifiers or biometric information may be captured, collected, purchased, obtained, or used if these pre-capture, pre-collection, pre-storage, or pre-obtainment requirements are not met.

65. There is no realistic way, absent surgery, to reassign someone's facial biometric data.

66. A person can obtain a new social security number, but not a new face, which makes the protection of, and control over, biometric identifiers and biometric information critical.

67. In direct violation of BIPA, Defendant captured, collected, received through trade, and/or otherwise obtained biometric identifiers or biometric information of their Illinois customers or potential customers, like Plaintiff, without properly obtaining the required informed written consent, and without making the required disclosures concerning the collection, storage, use, or destruction of biometric identifiers or information.

68. Moreover, Defendant caused these biometrics to be associated with consumers, along with other consumer information.

69. The Virtual Services feature on Defendant's website captures, collects and/or otherwise obtains the facial geometry and related biometric information and identifiers of users without proper consent and in direct violation of BIPA.

70. Each facial geometry scan and face template, as described above, constitutes a "biometric identifier" and "biometric information" under BIPA. See 740 ILCS 14/10.

71. Defendant has no written policy, made available to the public, which discloses its retention schedule and/or guidelines for retaining and then permanently destroying consumer biometric identifiers and information that complies with the requirements of BIPA.

72. Plaintiff and the putative Class are aggrieved by Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the consumers' last interactions with the company, whichever occurs first.

73. Plaintiff seeks damages and injunctive relief for Defendant's BIPA violations, for herself and all those similarly situated.

PLAINTIFF SPECIFIC ALLEGATIONS

74. Plaintiff has, at relevant times, had her facial geometry data, biometric information and biometric identifiers collected, captured, obtained, tracked and used by Defendant.

75. On January 6, 2022, Plaintiff used Defendant's Virtual Service feature on Defendant's website.

76. When visiting Defendant's mobile website on January 6, 2022, Plaintiff used the Virtual Try-On feature to virtually try on Decorté lipstick. Plaintiff used the "Take a selfie" option (as illustrated in paragraph 36 above) and took a "selfie" of her face which Defendant's Virtual Try-On feature accessed and processed.

77. When Plaintiff used the Virtual Services feature, Defendant unlawfully obtained and used her biometrics when Defendant scanned Plaintiff's facial geometry and used her facial geometry and landmarks, detected from her image, to apply the product to her face.

78. When Plaintiff used Defendant's Virtual Services feature, Defendant never asked her to consent to Defendant capturing, collecting, tracking, obtaining, using, storing and/or sharing her facial geometry, biometric identifiers or biometric information.

79. Defendant has never informed Plaintiff of the specific purposes or length of time for which Defendant captured, collected, tracked, obtained, stored and/or used her facial geometry and landmark data, biometric identifiers or biometric information.

80. Defendant has never informed Plaintiff of any specific biometric data retention policy developed by Defendant, nor has she ever been informed of whether Defendant will ever permanently delete her facial geometry and landmark data, biometric identifiers or biometric information.

81. Defendant has never provided Plaintiff with, nor did she ever sign, a written release allowing Defendant to collect, capture, track or otherwise obtain her facial geometry, biometric identifiers or biometric information.

82. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA as alleged herein.

THE PRIVACY POLICY MAKES NO MENTION OF BIOMETRICS AND DO NOT COMPLY WITH BIPA REQUIREMENTS

83. At the bottom of the webpage for Decorté products (https://decortecosmetics.com) is a hyperlink to, inter alia, a "Terms and Conditions" webpage and a "Privacy Policy" webpage.[6]

84. The Terms and Conditions and Privacy Policy webpages fail to make any mention of biometrics or facial geometry or identifiers whatsoever.

85. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that in processing photographs, images or live viewings of a consumer's face in Defendant's Virtual Services technology, Defendant tracks, captures, collects, possesses or obtains their facial geometry data, biometric information or biometric identifiers.

86. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that Defendant tracks their facial geometry, biometric information or biometric identifiers.

[6] https://decortecosmetics.com/pages/terms-conditions, https://decortecosmetics.com/pages/privacy-policy, last visited January 24, 2022.

87. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that Defendant captures their facial geometry, biometric information or biometric identifiers.

88. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that Defendant collects their facial geometry, biometric information or biometric identifiers.

89. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that Defendant possesses via its YouCam Makeup application their facial geometry, biometric information or biometric identifiers.

90. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that Defendant obtains their facial geometry, biometric information or biometric identifiers.

91. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that Defendant stores their facial geometry, biometric information or biometric identifiers.

92. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that Defendant shares their facial geometry and biometric information or biometric identifiers.

93. Neither the Terms and Conditions nor the Privacy Policy webpage state or inform the consumer that Defendant uses their unique facial geometry data, biometric information or biometric identifiers.

94. While Defendant fails to have the BIPA required publicly-accessible retention and destruction schedules or informed written consent, the developer of the YouCam Makeup

feature—that Defendant utilizes in creating this Virtual Services tool—states on its webpage that (among other things):

> Perfect [i.e., the developer company] collects, processes, and stores your Biometric Information through our mobile applications, allowing you in real-time to engage our products and services such as, but not limited to, creating and sharing beautiful photos and selfies, trying virtual makeup looks with your favourite products, and editing videos. For example, our YouCam Makeup application allows users to undergo a true-to-life virtual makeover using our world-class facial mapping technology. Specifically, for the processing of facial characteristics information, we will only detect your facial feature vectors in order to apply real-time virtual try-on effects thereon, upon your usage of our Apps.

https://www.youcamapps.com/info/privacy.action, last visited on January 19, 2022.[7]

95. A consumer who uses Defendant's Virtual Services feature does not agree or consent to the purported terms and conditions of set forth in the Terms and Conditions or the Privacy Policy webpage, which are on a separate webpage than the webpages used by a consumer of Defendant's Virtual Services feature.

96. Plaintiff did not ever agree or accept the information on the Terms and Conditions or the Privacy Policy webpages that are hyperlinked in the small print at the bottom of a lengthy and information-packed webpage.

97. BIPA's requirement that companies obtain informed written consent before collecting biometric information and/or biometric identifiers is not satisfied by the Terms and Conditions or the Privacy Policy webpage.

98. Further, BIPA's requirements that companies have accessible retention and destructions guidelines and policies is not satisfied by the Terms and Conditions or the Privacy Policy.

[7] The Youcamapps website and privacy policy webpage are separate from and are not part of or hyperlinked to Defendant's webpages.

THE BIOMETRIC INFORMATION PRIVACY ACT AND ILLINOIS'S STRONG STANCE ON PROTECTION OF BIOMETRIC INFORMATION

99. BIPA provides valuable rights, protections, and benefits to consumers in Illinois.

100. For example, BIPA's requirements ensure that the environment for the taking of biometrics is not forced or coerced; that individuals are freely advised that, by scanning one's facial geometry and identifiers, the retailer is capturing, extracting, collecting, obtaining or recording biometrics; that individuals can keep tabs on their biometric roadmaps (*e.g.*, who has their biometrics, for long how, and how it is being used), including after one's relationship ceases, or after the retailer stops storing the consumer's biometrics if at all; that individuals can evaluate the potential consequences of providing their biometrics; that companies must give individuals the right, and opportunity, to freely consent (or decline consent) **before taking** their biometrics; and that, if the disclosure does not say so, the consumer's biometrics will not be used for any other purpose except for those approved by the consumer.

101. To this end, in passing the Biometric Information Privacy Act (hereinafter "the Act") in 2008, the Illinois general assembly found:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) 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.

…

(e) The full ramifications of biometric technology are not fully known.

(f) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

See 740 ILCS 14/5, Legislative findings; intent.

102. BIPA is specifically designed to require a company that collects biometrics to meet several conditions, **before collection**, aimed, in part, at educating and protecting the person whose biometrics it is taking for its own use, and requiring signed, written consent attesting that the individual has been properly informed and has freely consented to biometrics collection.

103. The Act defines "Biometric identifier" as:

a retina or iris scan, fingerprint, voiceprint, or scan of had or face geometry...

See 740 ILCS 14/10.

104. The Act 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. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

See 740 ILCS 14/10.

105. The Act defines "Confidential and sensitive information" as:

personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

See 740 ILCS 14/10.

106. The Act defines "Private entity" as:

> any individual, partnership, corporation, limited liability company, association, or other group, however organized...

See 740 ILCS 14/10.

107. The Act defines "Written release" as:

> informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

See 740 ILCS 14/10.

108. The Act requires:

> A private entity in possession of biometric identifiers or biometric information must develop 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 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

740 ILCS 14/15(a).

109. Additionally, the Act provides:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative 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 or the subject's legally authorized representative.

740 ILCS 14/15(b).

110. Further, the Act provides:

> No private entity in possession of a biometric information may sell, lease, trade or otherwise profit from a person's or a customer's biometric identifier or biometric information.

740 ILCS 14/15(c).

111. The Act also provides:

> No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
>
> (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

740 ILCS 14/15(d).

112. Furthermore, the Act provides:

> A private entity in possession of a biometric identifier or biometric information shall:
>
> (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
>
> (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

740 ILCS 14/15(e).

113. BIPA provides statutory damages if a private entity takes an Illinois consumer's biometrics by circumventing BIPA's preconditions and requirements.

114. The Act explicitly provides a private right of action for violations of the Act, and provides that a prevailing party "may recover for each violation:"

> (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
>
> (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;
>
> (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
>
> (4) other relief, including an injunction, as the State or federal court may deem appropriate.

740 ILCS 14/20.

115. BIPA's formalized protections enable consumers to consent to the taking of their biometrics, if they so choose, after receiving legislatively-required information.

116. As BIPA demonstrates, the State of Illinois takes the privacy of biometric data seriously.

117. BIPA is the Illinois Legislature's expression that Illinois citizens have biometric rights that BIPA is intended to protect.

118. Defendant disregarded these rights and instead unlawfully collected, stored, and used Plaintiff's and consumers' biometric identifiers and information, without ever receiving the individual's informed written consent as required by BIPA.

CLASS ALLEGATIONS

119. Plaintiff brings this action on behalf of herself and pursuant to 735 ILCS 5/2-801 on behalf of a class (hereinafter the "Class") defined as follows:

> All Illinois residents who used Defendant's Virtual Services technology in Illinois between February 15, 2017 and the present.

Excluded from the Class are Defendant's officers and directors, Plaintiff's counsel, and any member of the judiciary presiding over this action.

120. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint.

121. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but on information and belief exceeds 100, in which case, individual joinder is impracticable. Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from over 100 individuals who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendant's records.

122. **Commonality and Predominance**: There are questions of law and fact common to the claims of Plaintiff and Class, and those questions predominate over any questions that may affect individual members, and frame issues for class-wide adjudication. Common questions for the Class include, but are not necessarily limited to the following:

A. Whether Defendant captured, collected, or otherwise obtained scans of facial geometry from the Class;

B. Whether the facial scan data Defendant captures, collects or otherwise obtains qualifies as "biometric identifiers" and/or "biometric information" under BIPA;

C. Whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information when the initial purpose for collecting and obtaining such identifiers or information has been satisfied or within three years of

the individual's last interaction with Defendant, whichever occurs first;

D. Whether Defendant obtained an executed written release from face-scanned consumers, before capturing, collecting, converting, sharing, storing, obtaining or using their biometrics;

E. Whether, in order to collect biometrics, Defendant provided a writing disclosing to face-scanned consumers the specific purposes for which their biometrics are being collected, captured, obtained, stored and/or used;

F. Whether, in order to collect biometrics, Defendant provided a writing disclosing to face-scanned consumers the length of time for which their biometrics are being collected, captured, obtained, stored and/or used;

G. Whether Defendant's conduct violates BIPA;

H. Whether Defendant's conduct was negligent, reckless or willful;

I. Whether Plaintiff and the Class are entitled to damages, and what is the proper measure thereof; and

J. Whether Plaintiff and the Class are entitled to injunctive relief.

123. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interest of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, 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.

124. **Appropriateness**: This class action is appropriate for certification because class

proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economics of time, effort and expense will be fostered and uniformity of decisions will be ensured.

COUNT I
VIOLATIONS OF ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT
(Damages)

125. Plaintiff, individually and on behalf of all others similarly situated, repeats and re-alleges the preceding allegations as though fully set forth herein.

126. BIPA is a remedial statute designed to protect consumers, by requiring consent and disclosures associated with the handling of biometrics, particularly in the context of biometric technology. 740 ILCS §§ 14/5(g), 14/10 and 14/15(b)(3).

127. The Illinois General Assembly's recognition of the importance of the public policy and benefits underpinning BIPA's enactment, and the regulation of biometrics collection, is detailed in the text of the statute itself. *E.g.,* 740 ILCS § 14/5(a), (c), (d), (f), (g).

128. Further, in a unanimous decision, the Illinois Supreme Court made clear that

"Compliance should not be difficult." *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 37 (Jan. 25, 2019). (emphasis added).

129. Additionally, the Illinois Supreme Court has made clear that the Illinois Legislature intended to "subject[] private entities who fail to follow the statute's requirement to substantial potential liability, including liquidated damages, injunctions, attorney fees, litigation expenses "'for each violation' of the law (*id.*, § 20) whether or not actual damages, beyond violation of the law's provisions, can be shown." *Id.* at ¶ 36.

130. "It is clear that the legislature intended for this provision to have substantial force." *Id.* at ¶ 37.

131. Defendant has been a "private entity" in possession of Plaintiff's and other consumers' and individuals' biometrics, and collected, captured or otherwise obtained their biometric identifiers and biometric information within the meaning of the Act.

132. As more fully set forth above, at relevant times Defendant obtained, collected, or otherwise obtained Plaintiff's and other individuals' biometric identifiers and biometric information based on those identifiers as defined by BIPA, 740 ILCS § 14/10, through Defendant's facial scanning platform.

133. In violation of Section 14/15(a), Defendant failed to make a written policy publicly available to Plaintiff and other Class members or comply with it.

134. In violation of Section 14/15(b), Defendant has collected, captured, stored or obtained Plaintiff's and other Class members' biometric identifiers and biometric information without:

a. informing Plaintiff and the Class (including, where applicable, their legal authorized representatives), in writing, that their biometric identifiers or biometric

information were being recorded, tracked, captured, collected or obtained;

b. informing Plaintiff and the Class (including, where applicable, their legal authorized representatives), in writing, of the specific purpose and length of term which the biometric identifiers or biometric information were being recorded, tracked, captured, collected or obtained; and

c. receiving an informed written release executed by Plaintiff and the Class.

135. Defendant took Plaintiff's and other Class members' facial scans, and knowingly caused their biometrics to be captured, collected, stored, and/or otherwise obtained without making publicly available the required policy that explains, for example, any purpose for which the biometric identifiers and information were captured, collected or obtained; the length of time Defendant captured, collected or obtained it; a retention schedule; or guidelines for permanently destroying biometric identifiers and information.

136. As a result of Defendant's above described acts and omissions, Defendant has unlawfully taken their biometrics; it has failed to provide them with information required by BIPA; it has deprived them of benefits, rights, opportunities and decisions conferred and required by the Illinois legislature via BIPA; and it illegally recorded, tracked, collected, captured, and stored their facial scans, biometrics and property.

137. By capturing, collecting, obtaining, and/or using Plaintiff's and the Class members' biometric identifiers and biometric information as described herein, Defendant violated the BIPA rights of Plaintiff and each Class member.

138. Additionally, to the extent Defendant has disclosed Plaintiff's and the Class members' biometric information to any third parties or vendors without first obtaining Plaintiff's and the Class members' written consent, Defendant has further violated BIPA.

139. Accordingly, Defendant has violated BIPA, and Plaintiff and the Class are entitled to damages available under BIPA, including damages for each violation.

COUNT II
VIOLATIONS OF ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT
(Injunctive Relief)

140. Plaintiff, individually and on behalf of all others similarly situated, repeats and re-alleges the preceding allegations as though fully set forth herein.

141. BIPA provides for injunctive relief. 740 ILCS § 14/20(4).

142. Plaintiff and other Class members are entitled to an order requiring Defendant to make disclosures consistent with the Act and enjoining further unlawful conduct.

143. First, Plaintiff seeks an order requiring Defendant to publicly disclose a written policy establishing any specific purpose and length of term for which Plaintiff's and other consumers' biometrics have been collected, stored, and used, as well as guidelines for permanently destroying such biometrics when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first, as required by 740 ILCS § 14/15(a).

144. Second, Plaintiff seeks an order requiring Defendant to disclose whether Defendant has retained Plaintiff's and other consumers' biometrics in any fashion, and if, when, and how such biometrics were permanently destroyed, consistent with BIPA.

145. Third, Plaintiff seeks an order requiring Defendant going forward to obtain a written release from any individual, prior to the capture, collection, obtainment and/or storage of that individual's biometric identifier or biometric information, especially a facial geometry scan, and biometric information and identifiers derived from it.

146. Fourth, due to the aforementioned facts, and Defendant's failure to make publicly

available facts demonstrating BIPA compliance as BIPA requires, Defendant should be ordered to: (i) disclose the extent to which (and precisely how and to whom) it has disseminated, sold, leased, used, traded, or otherwise profited from Plaintiff's and other face scanned consumers' biometric information, which is strictly prohibited under BIPA; and (ii) disclose the standard of care that it employed to store, transmit, and protect such biometrics, as provided under BIPA. 740 ILCS § 14/15(c), (d), (e).

147. Fifth, Defendant should be enjoined from further BIPA non-compliance, and should be ordered to remedy any BIPA compliance deficiencies forthwith.

148. Plaintiff's and other Class members' legal interests are adverse to Defendant's legal interests.

149. There is substantial controversy between Plaintiff and Defendant warranting equitable relief so that Plaintiff and the Class may obtain the protections that BIPA entitles them to receive.

150. Plaintiff and the Class do not know what Defendant has done (or intends to do) with their stored biometrics. Absent injunctive relief, Defendant is likely to continue their BIPA non-compliance and Plaintiff and other Class members will continue to be uninformed on their rights under BIPA.

151. For the reasons set forth above, Plaintiff are likely to succeed on the merits of their claims.

152. BIPA establishes the importance, value, and sensitive nature of biometrics, along with the need to protect and control it; Plaintiff are entitled to know what Defendant has done with it as set forth above, and to an affirmation and verification that it has been permanently destroyed as required by 740 ILCS § 14/15(a).

153. The gravity of the harm to Plaintiff and the Class, absent equitable relief, outweighs any harm to Defendant if such relief is granted.

154. As a result, Plaintiff request commensurate injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays that the Court grant the following relief:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Ashley Hiatt as Class Representatives, and appointing Donelon, P.C. and Law Office of Thomas M. Ryan, P.C. as Class Counsel;

B. Declaring that Defendant's action, as set forth above, violate BIPA

C. Awarding statutory damages of $5,000 for each intentional 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);

D. Declaring that Defendant's actions, as set forth above, were intentional and/or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendant to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

G. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as equity and just may require.

Dated: February 15, 2022

Respectfully Submitted,

/s/ Brendan Donelon
One of Plaintiff's Attorneys

Brendan Donelon
DONELON, P.C.
4600 Madison Avenue
Kansas City, Missouri 64112
Tel: (816) 221-7100
Fax: (816) 709-1044
brendan@donelonpc.com

Daniel W. Craig
DONELON, P.C.
6642 Clayton Rd., #320
St. Louis, Missouri 63117
Tel: (314) 297-8385
Fax: (816) 709-1044
dan@donelonpc.com

Thomas M. Ryan,
LAW OFFICE OF THOMAS M. RYAN, P.C.
35 E. Wacker Drive, Suite 650
Chicago, IL 60610
Tel: (312) 726-3400
Fax: (312) 782-4519
tom@tomryanlaw.com