□ YES ☑ NO

EXHIBITS

CASE NO. 2021 CH 3119

DATE: 6/25/2021

CASE TYPE: Class Action

PAGE COUNT: 34

CASE NOTE

____

____

____

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

DAVID BARNETT, ETHEL BURR, and)
MICHAEL HENDERSON, on behalf of)
themselves and all others similarly situated,)
)
Plaintiffs,) No. 2021CH03119
v.)
)
APPLE, INC.,)
)
Defendant.

Plaintiffs David Barnett, Ethel Burr, and Michael Henderson, on behalf of themselves and all other persons similarly situated, by their undersigned attorneys, as and for their Class Action Complaint for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq*., against Defendant Apple, Inc. ("Defendant"), allege on personal knowledge, due investigation of their counsel, and, where indicated, on information and belief as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in capturing and collecting their and other similarly situated individuals' biometric identifiers[1] and biometric information[2] (referred to collectively at times as "biometrics") without obtaining informed written consent.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/15(c). "For example, social security numbers, when compromised, can be changed. Biometrics,

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and "face geometry", among others.

[2] "Biometric information" is any information captured, converted, stored or shared based on a person's biometric identifier used to identify an individual.

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." *Id.*

3. Prompted by these concerns, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Defendant may not obtain an individual's biometrics unless it informs that person in writing that biometric identifiers or information will be collected. *See* 740 ILCS 14/15(b).

4. BIPA requires that entities collecting biometrics must inform those persons in writing of the specific purpose and length of term for which such biometric identifiers or biometric information are being captured, collected, or otherwise obtained. *See id.*

5. BIPA further requires that entities possessing biometrics must develop and make public a written policy containing a retention schedule and guidelines for destroying the biometric data. *See* 740 ILCS 14/15(a).

6. Defendant manufactures and sells iPhones, iPads, and MacBooks that use "Touch ID" (the "Touch ID Products"),[3] which is an electronic fingerprint recognition feature that extracts the biometric fingerprint of Touch ID users.

7. Defendant also manufactures and sells iPhones and iPads that use "Face ID" (the "Face ID Products"),[4] which is a facial recognition feature that extracts the biometric facial geometry of Face ID users.

[3] These include the following iPhone models: 6S, 6S Plus, 7, 7 Plus, 8, 8 Plus, SE (2nd Generation). These also include MacBook Pros produced from 2016-2020, MacBook Airs produced from 2018-2020, and the iPad Pro 10.5" and 12.9" (2nd generation).

[4] These include the following iPhone models: X, XR, XS, XS Max, 11, 11 Pro, 11 Pro Max. These also include the iPad Pro (11-inch) and iPad Pro (12.9-inch, 2018 model).

8. Using Touch ID, Defendant captures, collects, and possesses Touch ID users' fingerprints.

9. Using Face ID, Defendant captures, collects, and possesses Face ID users' facial geometry.

10. BIPA confers on Plaintiffs and all other similarly situated Illinois residents a right to know of the risks inherently present when Defendant captures and collects their biometric identifiers and information and a right to know how long such risks will persist.

11. Despite this, Defendant has never adequately informed Plaintiffs and the Classes of its biometrics collection practices, nor has Defendant obtained the requisite written consent from Plaintiffs and the Classes regarding its biometric practices.

12. Defendant has also failed to develop a written policy establishing a retention schedule or guidelines for permanently destroying Plaintiffs' biometrics.

13. Plaintiffs bring this action to prevent Defendant from further violating the privacy rights of Illinois residents and to recover statutory damages for Defendant's unauthorized possession, capture, and collection of these individuals' biometrics in violation of BIPA.

JURISDICTION AND VENUE

14. This Court has personal jurisdiction over Defendant because the biometrics that give rise to this lawsuit were captured from Plaintiff Barnett while he was residing and physically present in Cook County, Illinois.

15. Cook County is an appropriate venue for this litigation because defendant does business in Cook County, and is therefore a resident of Cook County. 735 ILCS 5/2-102.

16. In addition, the transactions and occurrences out of which the causes of action pleaded herein arose or occurred, in part, in Cook County.

PARTIES

17. Plaintiff Barnett is, and has been at all relevant times, a resident and citizen of Illinois.

18. Plaintiff Burr is, and has been at all relevant times, a resident and citizen of Illinois.

19. Plaintiff Henderson is, and has been at all relevant times, a resident and citizen of Illinois.

20. Defendant Apple, Inc. is a California Corporation with its principal place of business in Cupertino, California. Defendant sells and/or distributes the Touch ID and Face ID Products throughout Illinois.

FACTUAL BACKGROUND

I. Illinois' Biometric Information Privacy Act

21. In 2008, Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA"), which regulates how a private entity may possess and collect biometric identifiers and information. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA's regulatory requirements differentiate between private entities that possess, and private entities that collect, biometrics.

22. 740 ILCS 14/15(a), for example, regulates a private entity's "possession" of biometrics. When a private entity is in possession of biometrics, BIPA requires that it publish a "written retention schedule, made available to the public, establishing a retention schedule and guidelines" for destroying biometrics. *See* 740 ILCS 14/15(a).

23. As with 740 ILCS 14/15(a), sections (c), (d), and (e) regulate private entities "in possession" of biometrics.

24. 740 ILCS 14/15(b), on the other hand, regulates a private entity's ability to "collect,

capture, purchase, receive through trade, or otherwise obtain" a person's biometrics. *See* 740 ILCS 14/15(b). A private entity is prohibited from doing so unless it:

> (1) informs the subject … in writing 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 or the subject's legally authorized representative.
>
> 740 ILCS 14/15 (b).

25. BIPA thus separates and distinguishes between possession and collection. *See also* 740 ILCS 14/15(b)(1) (using a disjunctive when mandating that private entities must receive consent in writing whenever biometrics are "collected *or* stored") (emphasis added).

26. The Illinois legislature listed the concerns that prompted BIPA's passage in 740 ILCS 14/5.

27. The legislature observed that "[t]he use of biometrics is growing in the business and security screening sectors and appears to promise *streamlined financial transactions and security screenings*." 740 ILCS 14/5(a) (emphasis added).

28. These financial transactions include "finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(b).

29. Left unchecked, the legislature concluded, the proliferation of biometrics could create an unprecedented security risk:

> 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.

740 ILCS 14/5(c).

30. The Illinois legislature also observed that biometric technologies were, at the time, nascent innovations, recognizing that "[t]he full ramifications of biometric technology are not fully known." 740 ILCS 14/5(f).

II. Factual Context

31. As the Illinois legislature anticipated, the popularity of biometric technologies has exploded. From test proctoring[5] to doorbells[6] to employee time-keeping devices,[7] biometric technologies are ubiquitous.[8]

32. This ubiquity dovetails with a much larger economic movement; one that profits from extracting individuals' personal data by, among other tactics, leveraging information asymmetries between consumers and corporations.[9] Defendant is an active participant in leveraging information asymmetries for profit.[10] BIPA's notice and consent provisions seek to

[5] *See* Nero Caplan-Bricker, *Is Online Test-Monitoring Here to Stay?*, New Yorker (May 27, 2021), *accessible at* https://www.newyorker.com/tech/annals-of-technology/is-online-test-monitoring-here-to-stay.

[6] *See* Tim Bradshaw, *Google facial recognition technology brings privacy debate into the home*, L.A. Times (May 7, 2019), *accessible at* https://www.latimes.com/business/la-fi-tn-google-face-match-20190507-story.html.

[7] *See* Lauren Kaori Gurley, *Amazon Delivery Drivers Forced to Sign 'Biometric Consent' Form or Lose Job*, Vice (Mar. 23, 2021), *accessible at* https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job.

[8] *See also* Alessandro Mascellino, *Facebook plans smartwatch with biometrics, Apple Watch to upgrade health app*, Biometric Update (June 11, 2021), *accessible at* https://www.biometricupdate.com/202106/facebook-plans-smartwatch-with-biometrics-apple-watch-to-upgrade-health-app ("Facebook is considering an innovative design for its upcoming smartwatch with a biometric heart rate monitor and two detachable cameras[.]").

[9] *See generally* Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for the Human Future at the New Frontier of Power (2019).

[10] *See* Geoffrey A. Fowler, *It's the middle of the night. Do you know who your iPhone is talking to?*, Wash. Post (May 28, 2019) ("And your iPhone doesn't only feed data trackers while you sleep. In a single week, I encountered over 5,400 trackers, mostly in apps … those unwanted trackers would have spewed out 1.5 gigabytes of data over the span of a month. That's half of an entire basic wireless service plan from AT&T."); Ian Bogost, *Apple's Empty Grandstanding About Privacy*, The Atlantic (Jan. 31, 2019) ("If Apple really cared about personal data, the company could take any number of actions to keep privacy violators off its platforms and away from its customers. Until it does, it's time to stop letting Apple off the hook as a more moral company than Google or Facebook."); *see also* Patrick McGee, *Apple under pressure to close loopholes in new privacy rules*, Fin. Times (June 8, 2021) ("Apple has come under pressure to tighten its new privacy rules ahead of its annual developers' conference on Monday, after experts warned that thousands of apps were continuing to collect data from users who had opted out of tracking.").

ameliorate information asymmetries for biometrics.

33. Also characteristic of this larger economic movement is the routine failure to properly secure that personal information—whether stored locally or on a server.[11] This too implicates the principles animating BIPA.

34. Proving the point are security concerns over newly manufactured vehicles. Like Defendant, these data-consuming vehicles locally store and collect reams of intimate, personal data from drivers. As a recent NBC investigation explained, these vehicles now "reveal everything from location, speed and acceleration to when doors were opened and closed, whether texts and calls were made while the cellphone was plugged into the infotainment system, as well as voice commands and web histories."[12] This locally stored data, however, is easily accessible, with "vehicle forensic kits" openly available for private purchase.[13] Thus, whether locally stored or stored on a server, the security concerns for personal information—or, in this case, immutable information—remain the same. Like data-consuming vehicles, Defendant's products contain a plethora of ultra-sensitive, personal information[14]—principal among them, biometrics.[15] And like

[11] *See, e.g.*, Christopher Mele, *Data Breaches Keep Happening. So Why Don't You Do Something?*, N.Y. TIMES (Aug. 1, 2018), *accessible at* https://www.nytimes.com/2018/08/01/technology/data-breaches.html ("Last year was a banner year for the exposure of personal information, and so far this year there has been a steady drumbeat of data breaches, so many that experts worry that people are just throwing up their hands in defeat.").

[12] Olivia Solon, *Insecure wheels: Police turn to data to destroy suspects' alibis*, NBC NEWS (Dec. 28, 2020), *accessible at* https://www.nbcnews.com/tech/tech-news/snitches-wheels-police-turn-car-data-destroy-suspects-alibis-n1251939.

[13] *See, e.g.*, Sam Biddle, *Your Car Is Spying On You, and A CBP Contract Shows The Risks*, THE INTERCEPT (May 3, 2021), *accessible at* https://theintercept.com/2021/05/03/car-surveillance-berla-msab-cbp/?utm_medium=email&utm_source=The%20Intercept%20Newsletter.

[14] This appetite for data only continues to grow, as do the stakes if Defendant's device security is compromised. Defendant recently announced that "it is trying to move government identification onto the devices" and to "replace physical keys … [by] making it easier to use digital keys to unlock doors at homes, offices and hotels." *See* Jack Nicas, Brian X. Chen, *Apple unveils new privacy features, digital IDs and changes to FaceTime*, N.Y. TIMES (June 7, 2021), *accessible at* https://www.nytimes.com/2021/06/07/technology/apple-wwdc-facetime.html.

[15] *See, e.g.*, Kate O'Falherty, *Apple To Kill Passwords With Game-Changing New Face ID Move*, FORBES (June 11, 2021), *accessible at* https://www.forbes.com/sites/kateoflahertyuk/2021/06/11/apple-to-kill-passwords-with-game-changing-new-face-id-move/?sh=4e00c3104708 ("Apple has become the latest big tech company to take game-changing steps towards removing passwords altogether, in favor of biometrics via its Face ID and Touch ID features.").

data-consuming vehicles, Defendant's biometric storage is vulnerable to hacking.[16]

35. Unlike other data-consuming products, however, Defendant's relationship with users is profoundly unique. Defendant has a 1) direct and 2) ongoing relationship with users, and 3) its biometric collection practice is inextricably intertwined with other services it provides.

36. Apple sells its products directly to consumers.[17] In 2019, direct-to-consumer sales accounted for 31% of Defendant's total revenue.[18]

37. Apple regularly updates and patches the software used on a user's device.[19] In just over the last four years, Defendant has released more than 200 updates to its software.[20]

38. Apple singularly regulates and controls the App Store,[21] which in 2020 generated gross sales of roughly $64 billion.[22] Indeed, Apple's control over the App Store has recently drawn antitrust scrutiny from European Union regulators, charging Apple with unfair rules and fees.[23] The App Store uses Touch ID and Face ID as authorization methods for purchases and downloads.[24]

[16] *See, e.g.*, Filipe Esposito, *New 'unpatchable' exploit allegedly found on Apple's Secure Enclave chip, here's what it could mean*, 9 TO 5 MAC (Aug. 1, 2020) ("Last month … hackers claimed they found a permanent vulnerability in the Secure Enclave, which could put data from iPhone, iPad, and even Mac users at risk.").

[17] *See, e.g*, APPLE SUPPORT, MACBOOK PRO ALL SYSTEMS PRO, *accessible at* https://www.apple.com/macbook-pro-13/.

[18] Malcolm Owen, *Apple Store revenue grows to 31% of Apple's income for 2019*, APPLE INSIDER (Nov. 6, 2019), *accessible at* https://appleinsider.com/articles/19/11/06/apple-store-revenue-grows-to-31-of-apples-income-for-2019.

[19] *See* APPLE SUPPORT, UPDATE IOS ON IPHONE, *accessible at* https://support.apple.com/en-gb/guide/iphone/iph3e504502/ios.

[20] *See* APPLE SUPPORT, APPLE SECURITY UPDATES, *accessible at* https://support.apple.com/en-us/HT201222.

[21] *See* APPLE SUPPORT, IPHONE USER GUIDE, *accessible at* https://support.apple.com/en-gb/guide/iphone/iph3dfd91de/ios.

[22] Kif Leswing, *Apple's App Store had gross sales around $64 billion last year and it's growing strongly again*, CNBC (Jan. 8, 2021), *accessible at* https://www.cnbc.com/2021/01/08/apples-app-store-had-gross-sales-around-64-billion-in-2020.html.

[23] Adam Satariano, *Apple's App Store Draws E.U. Antitrust Charge*, N.Y. TIMES (May 17, 2021), *accessible at* https://www.nytimes.com/2021/04/30/technology/apple-antitrust-eu-app-store.html; *see also* Complaint, *Epic Games Inc. v. Apple, Inc.*, 4:20-cv-05640 (N.D. Cal. Oct. 13, 2020)

[24] *See* APPLE SUPPORT, USE TOUCH ID ON IPHONE AND IPAD, *accessible at* https://support.apple.com/en-us/HT201371#:~:text=Use%20Touch%20ID%20for%20Apple%20Pay&text=You%20can%20also%20use%20Touch,and%20on%20websites%20in%20Safari.

39. Touch ID and Face ID are also used for Defendant's Apple Pay, which authorizes physical purchases.[25] Apple Pay comprises 5% of all global card transactions, with forecasts projecting that share to double by 2025.[26] *See also* 740 ILCS 14/5(a) ("The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined transactions and security screenings.").

40. Both Touch ID and Face ID are used to access traditional passwords stored on the device.[27] Apple even allows developers to utilize Touch ID and Face ID as direct log-in methods for their applications.[28]

41. Apple also collects diagnostic data from users, like how many are using Touch ID and how often they unlock their device.[29]

42. Following initial enrollment, subsequent log-in attempts are used to augment Apple's fingerprint and facial recognition technology.[30]

43. Apple solely owns, operates, maintains, and updates its proprietary software; users are only licensees. In Apple's iOS and iPadOS Software License Agreement, for example, Apple states that:

> The software (including Boot ROM code, embedded software and third party software), documentation, interfaces, content, fonts and any data that came with

[25] *See* APPLE SUPPORT, HOW TO USE APPLE PAY, *accessible at* https://support.apple.com/en-us/HT201239#stores.

[26] *See* Bryan Pietsch, *1 in 10 card transactions could be done with Apple Pay by 2025, providing Apple a revenue boost amid iPhone sales slump*, BUSINESS INSIDER (Feb. 12, 2020), *accessible at* https://www.businessinsider.com/apple-bet-apple-pay-shows-results-transactions-market-share-increases-2020-2.

[27] *See* APPLE SUPPORT, HOW TO FIND SAVED PASSWORDS ON YOUR IPHONE, *accessible at* https://support.apple.com/en-us/HT211146.

[28] *See* APPLE DEVELOPER, LOGGING A USER INTO YOUR APP WITH FACE ID OR TOUCH ID, *accessible at* https://developer.apple.com/documentation/localauthentication/logging_a_user_into_your_app_with_face_id_or_touch_id.

[29] *See* Mikey Campbell, *Average iPhone user unlocks device 80 times per day, 89% use Touch ID, Apple Says*, APPLE INSIDER (Apr. 19, 2016), *accessible at* https://appleinsider.com/articles/16/04/19/average-iphone-user-unlocks-device-80-times-per-day-89-use-touch-id-apple-says.

[30] *See* APPLE, FACE ID SECURITY 4 (2017), *accessible at* https://www.apple.com/ca/business-docs/FaceID_Security_Guide.pdf ("The following Face ID data is saved … during normal operation: … [t]he mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching.").

> your Device ("Original Apple Software"), as may be updated or replaced by feature enhancements, software updates or system restore software provided by Apple ("Apple Software Updates"), whether in read only memory, on any other media or in any other form … are licensed, not sold, to you by Apple Inc.[31]

44. Apple's ownership rights encompass the software used to capture, collect, and analyze a user's biometrics.

45. Upon information and belief, users are unable to access their own biometrics collected or stored on their devices without violating Apple's Software License Agreement. Thus, Apple possesses the "'right to exclude,' so universally held to be a fundamental element of the property rights," over a user's biometrics.[32]

46. Apple possesses complete control over what to include in a software update and, more importantly, what to disclose to its users.[33] Upon information and belief, Apple—like Microsoft and other software manufacturers[34]—has the capability to force updates on a device. In this way, Apple possesses almost omnipotent power over how a device functions.[35]

III. Defendant Violates Illinois' Biometric Information Privacy Act

1. Touch ID

47. In direct violation of § 15(a) of BIPA, Defendant failed to develop a written policy,

[31] *See* iOS AND iPadOS SOFTWARE LICENSE AGREEMENT, *accessible at* https://www.apple.com/legal/sla/docs/iOS14_iPadOS14.pdf.

[32] *See Kaiser Aetna v. United States*, 444 U.S. 164, 180-81 (1979) ("In this case, we hold that the 'right to exclude,' so universally held to be a fundamental element of the property right, falls within the category of interests that the Government cannot take without compensation.").

[33] *See* Jacob Siegal, *iOS 14.6 has a secret new feature that Apple didn't announce*, YAHOO (May 26, 2021), *accessible at* https://www.yahoo.com/entertainment/ios-14-6-secret-feature-222215251.html ("Apple usually highlights all of the biggest changes in the release notes for its software updates, but for whatever reason, faster shortcuts didn't make the cut for the iOS 14.6 release notes.").

[34] *See* Sergiu Gatlan, *Microsoft starts force installing Windows 10 20H2 on more devices*, BLEEPING COMPUTER (Mar. 3, 2021), *accessible at* https://www.bleepingcomputer.com/news/microsoft/microsoft-starts-force-installing-windows-10-20h2-on-more-devices/.

[35] *See* Alisha Ebrahimji, *Apple warns some iPhone users: Update your phone or lose internet*, CNN (Oct. 30, 2019) ("If it ain't broke, don't fix it – right? Well, some of you Apple product users may not have a choice this weekend."), *accessible at* https://www.cnn.com/2019/10/30/tech/old-apple-product-update-trnd/index.html; *see also* Geoffrey A. Fowler, *iTrapped: All the things Apple won't let you do with your iPhone*, WASH. POST (May 27, 2021) ("When you buy an iPhone, it isn't really yours.").

made available to the public, establishing a retention schedule and guidelines for permanently destroying a user's biometrics.

48. In direct violation of § 15(b)(2) of BIPA, Defendant failed to inform Touch ID users of the specific purpose and length of time for which their biometrics were collected or stored.

49. In direct violation of § 15(b)(3) of BIPA, Defendant failed to obtain a written release from Touch ID users.

50. Defendant's Touch ID scans and collects a user's fingerprints, which is then used to create a unique mathematical representation. If a user is enrolling in Touch ID, this representation is stored on a user's device. If a user is already enrolled, then the representation is compared with the saved representation.

51. Defendant's website elaborates on the Touch ID process:

> The [Touch ID] sensor uses advanced capacitive touch to take a high-resolution image from small sections of your fingerprint from the subepidermal layers of your skin. Touch ID then intelligently analyzes this information with a remarkable degree of detail and precision. It categorizes your fingerprint as one of three basic types—arch, loop, or whorl. It also maps out individual details in the ridges that are smaller than the human eye can see, and even inspects minor variations in ridge direction caused by pores and edge structures. … It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device.[36]

//

//

//

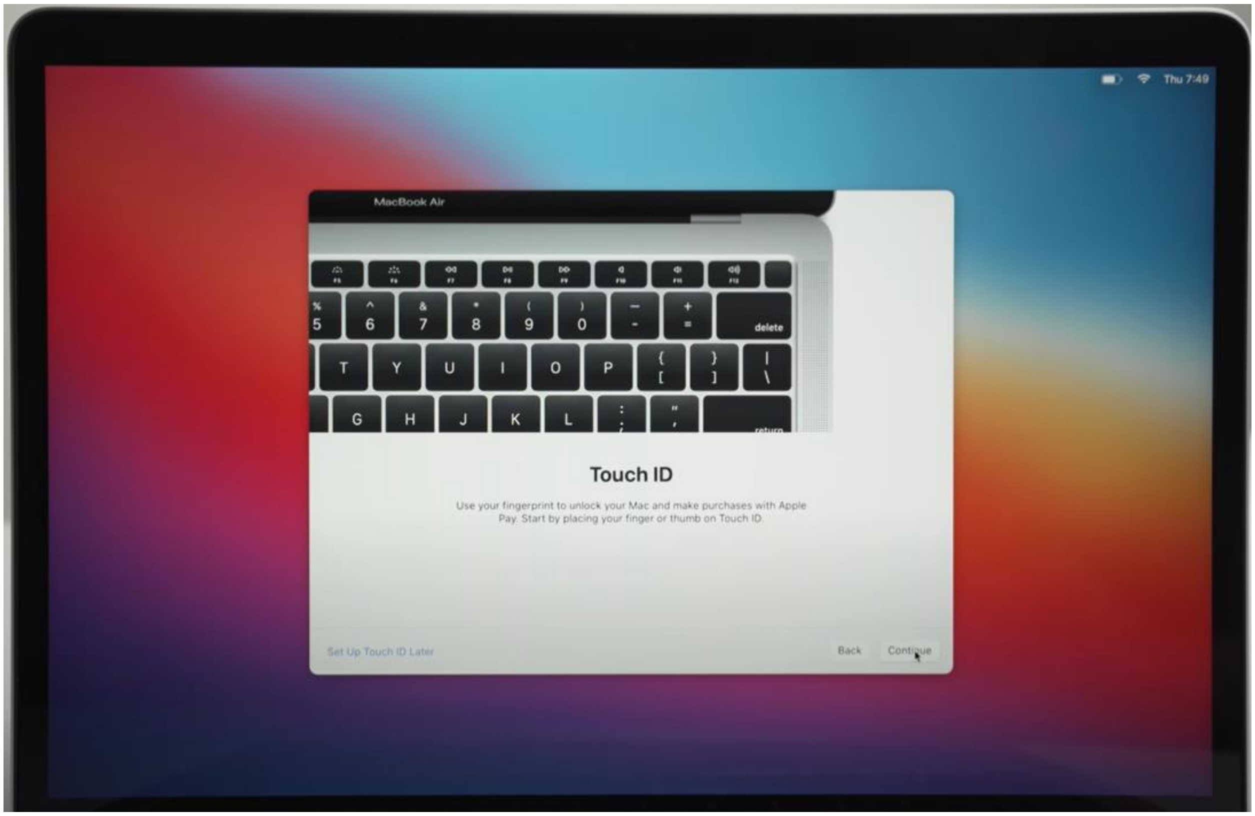
//

//

//

[36] *See* APPLE SUPPORT, ABOUT TOUCH ID ADVANCED SECURITY TECHNOLOGY, *accessible at* https://support.apple.com/en-us/HT204587#:~:text=Touch%20ID%20can%20be%20used,be%20enrolled%20across%20the%20system.

52. When a user first purchases an Apple Touch ID Product, they are prompted with a series of steps to complete. This includes setting up fingerprint authentication, which is functionally identical for every device equipped with Touch ID. The initial page describes the capabilities of Touch ID: “Use your fingerprint to unlock your [device] and make purchases with Apply Pay. Start by placing your finger or thumb on Touch ID.”



Touch ID

Use your fingerprint to unlock your Mac and make purchases with Apple Pay. Start by placing your finger or thumb on Touch ID.

//

//

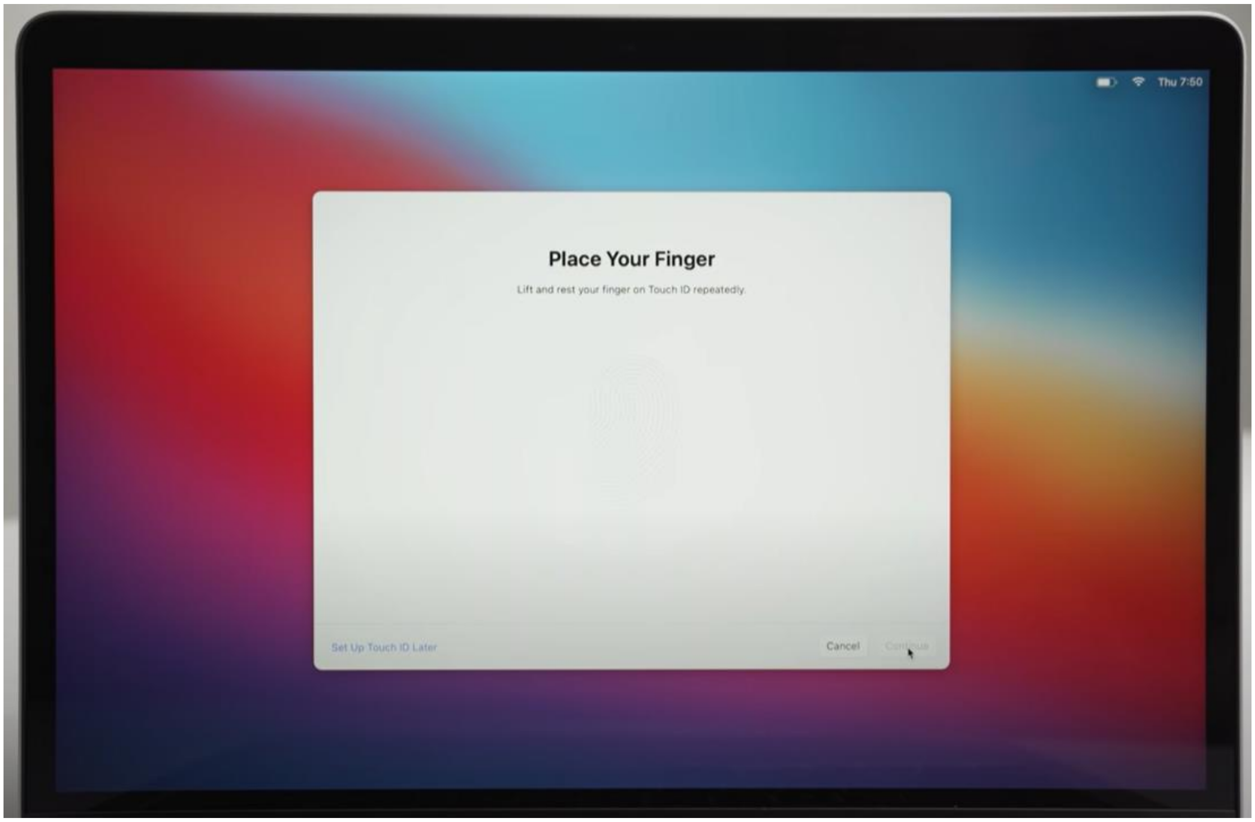
//

//

//

//

53. Once a user clicks "Continue," a new window appears asking the user to "[l]ift and rest your finger on Touch ID repeatedly":



Place Your Finger

Lift and rest your finger on Touch ID repeatedly.

//

//

//

//

//

//

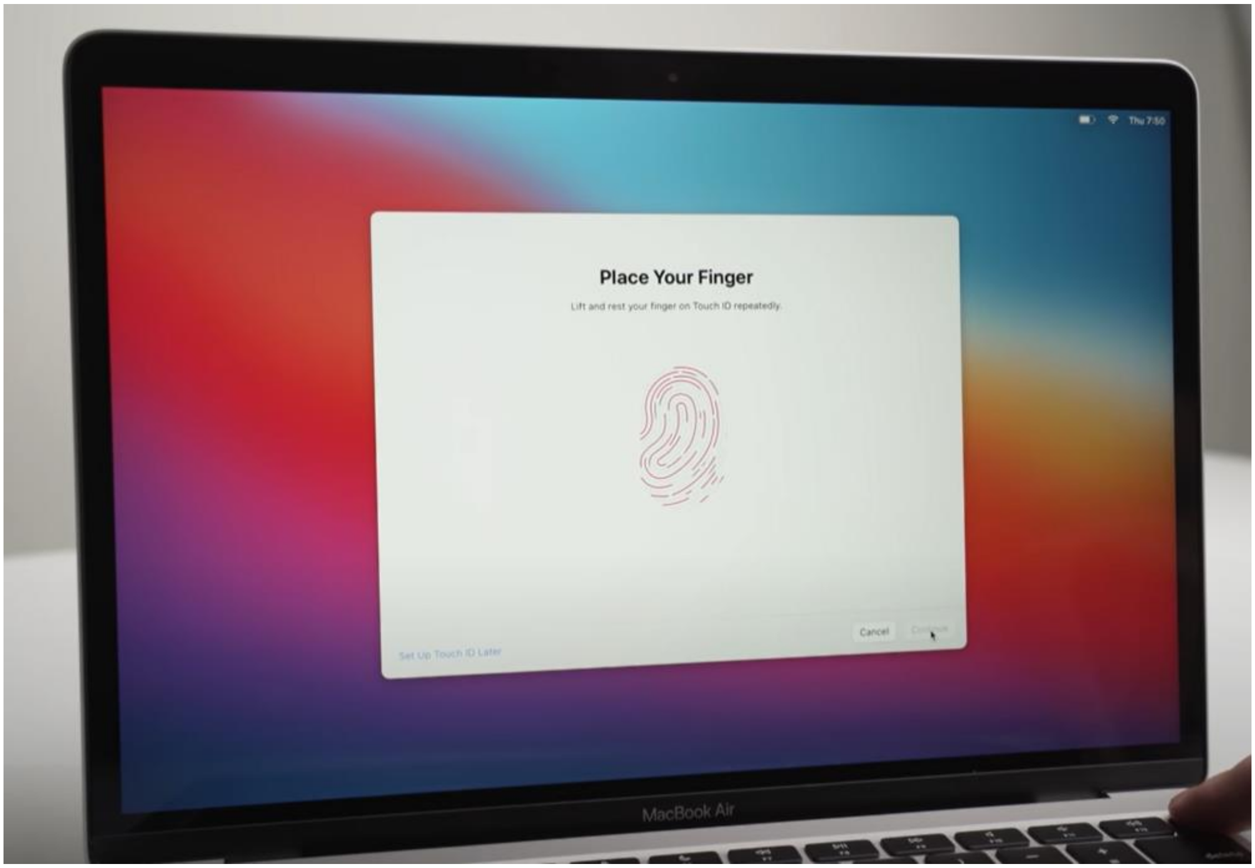
//

//

//

//

54. A user then rolls their finger onto the scanner until a complete fingerprint is captured:



Place Your Finger

Lift and rest your finger on Touch ID repeatedly.

//

//

//

//

//

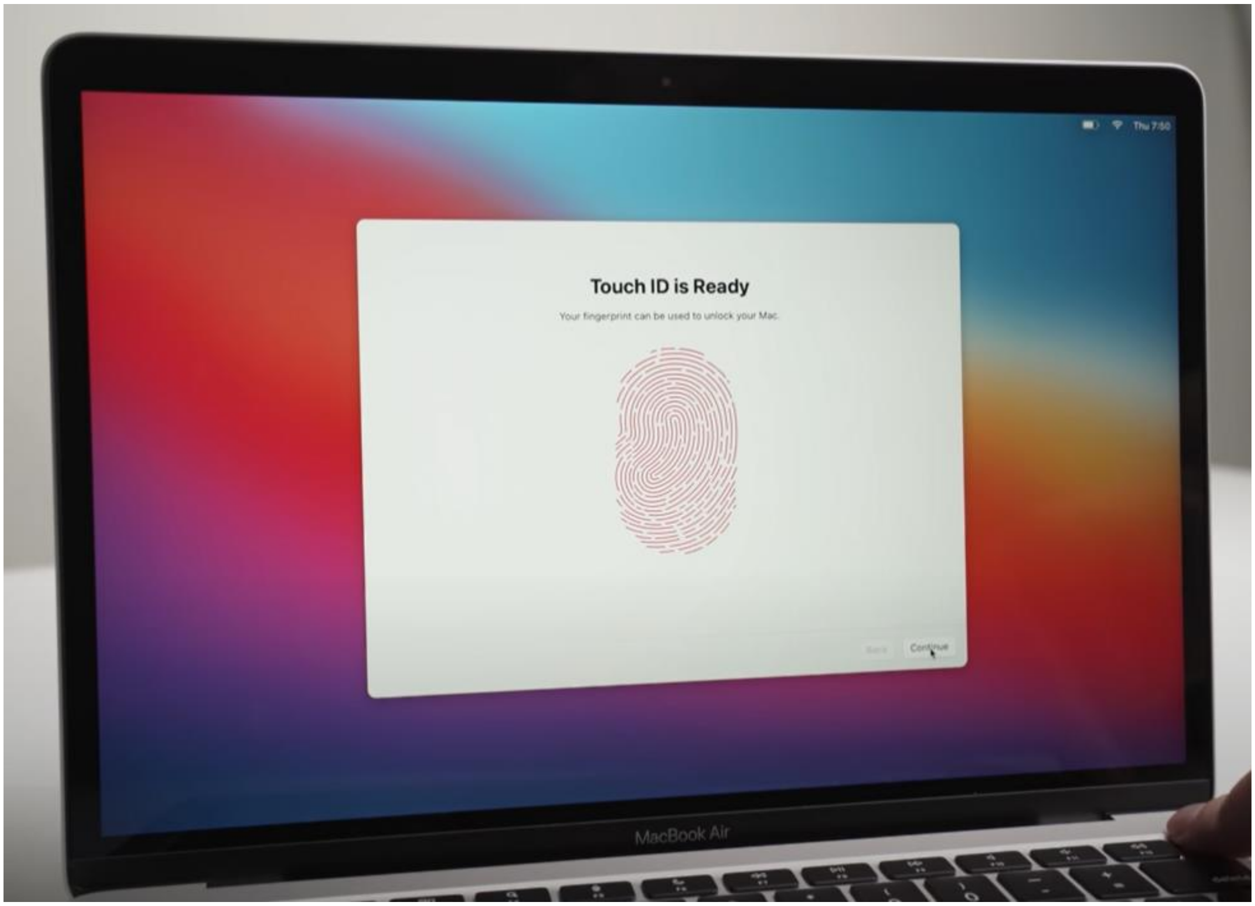
//

//

//

//

55. After the fingerprint is captured, the “continue” dialog box is activated and the user moves onto the next step in the set-up process:



Touch ID is Ready

Your fingerprint can be used to unlock your Mac.

56. This is the full extent of Defendant’s representations during the enrollment process. All Apple Products equipped with Touch ID employ the same process for set-up and use of Touch ID.[37]

57. This enrollment process fails to inform a user of “the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used[.]” *See* 740 ILCS 14/15(b)(2).

[37] *See* Apple Support, Use Touch ID on iPhone and iPad, *accessible at* https://support.apple.com/en-us/HT201371.

58. During this process, Defendant also fails to receive "a written release executed by" the users. *See* 740 ILCS 14/15(b)(3).

59. Thus, Defendant violates 740 ILCS 14/15(b)(2) and (3).

2. Face ID

60. In direct violation of § 15(a) of BIPA, Defendant failed to develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying a user's biometrics.

61. In direct violation of § 15(b)(2) of BIPA, Defendant failed to inform Face ID users of the specific purpose and length of time for which their biometrics were collected or stored.

62. In direct violation of § 15(b)(3) of BIPA, Defendant failed to obtain a written release from Face ID users.

63. Defendant's Face ID scans and collects a user's facial geometry, which is then used to create a unique mathematical representation. If a user is enrolling in Face ID, this representation is stored on a user's device. If a user is already enrolled, the representation is compared with the saved representation.

64. Defendant's website elaborates on the Face ID process:

> The [Face ID] TrueDepth camera captures accurate face data by projecting and analyzing over 30,000 invisible dots to create a depth map of your face and also captures an infrared image of your face. A portion of the neural engine of the A11, A12 Bionic, A12X Bionic, and A13 Bionic chip — protected within the Secure Enclave — transforms the depth map and infrared image into a mathematical representation and compares that representation to the enrolled facial data.[38]

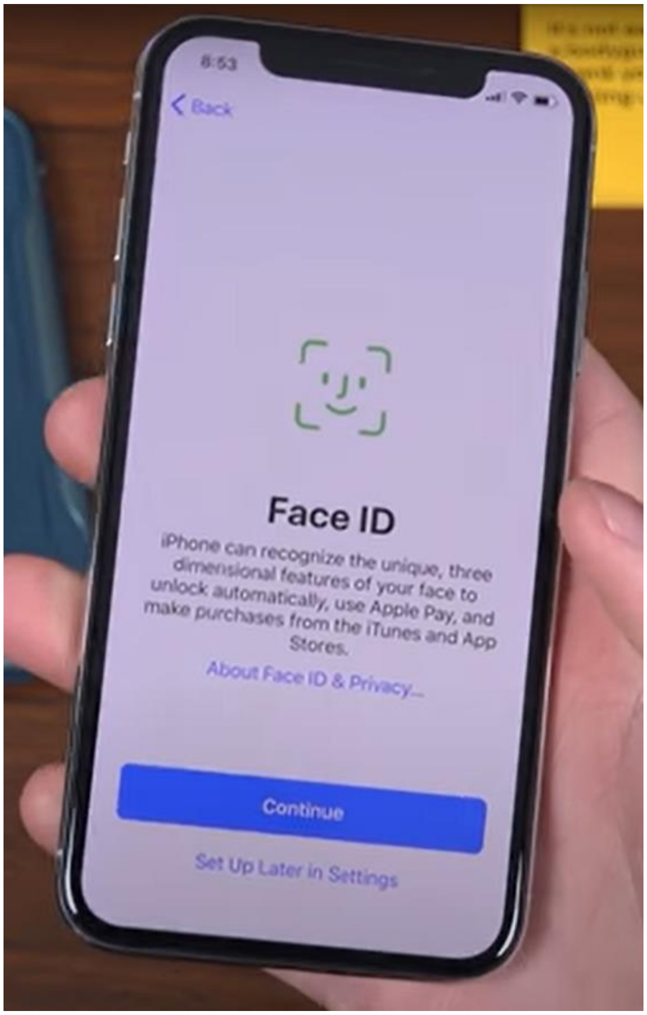
//

//

//

[38] *See* APPLE SUPPORT, ABOUT FACE ID ADVANCED TECHNOLOGY, *accessible at* https://support.apple.com/en-us/HT208108.

65. When a user first purchases an Apple Face ID Product, they are prompted with a series of steps to complete. This includes setting up facial recognition authentication, which is functionally identical for every device equipped with Face ID. The initial page describes the capabilities of Face ID: “iPhone can recognize the unique, three dimensional features of your face to unlock automatically, use Apple Pay, and make purchases from the iTunes and App Store.”



Face ID

iPhone can recognize the unique, three dimensional features of your face to unlock automatically, use Apple Pay, and make purchases from the iTunes and App Stores.

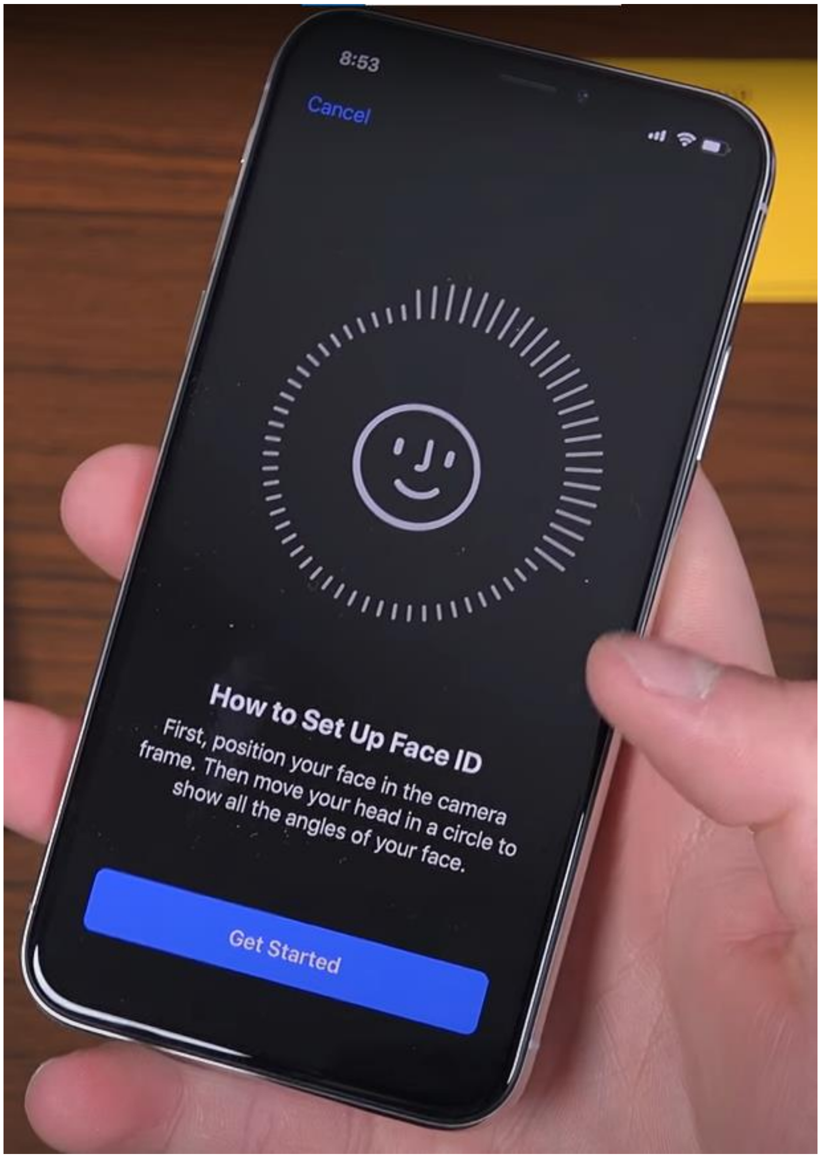
//

//

//

//

66. Once a user clicks "Continue," a new page appears that asks the user to "position your face in the camera frame. Then move your head in a circle to show all the angles of your face."



How to Set Up Face ID

First, position your face in the camera frame. Then move your head in a circle to show all the angles of your face.

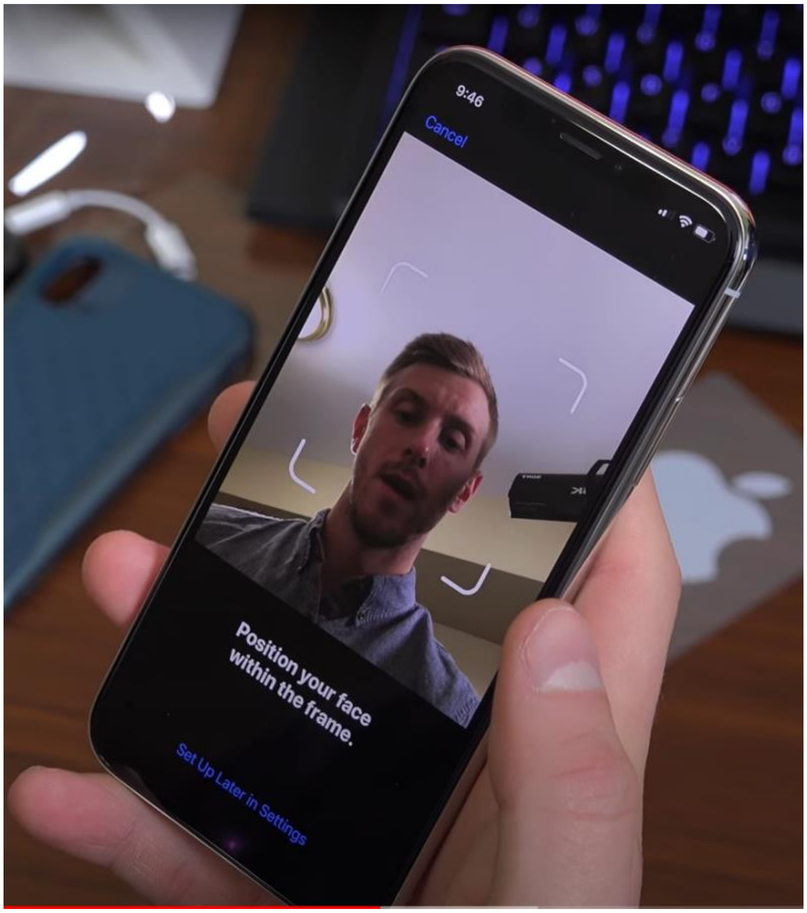
//

//

//

//

67. When a user clicks "Get Started," a new page populates, asking the user to "Position your face within the frame."



Position your face within the frame.

//

//

//

//

//

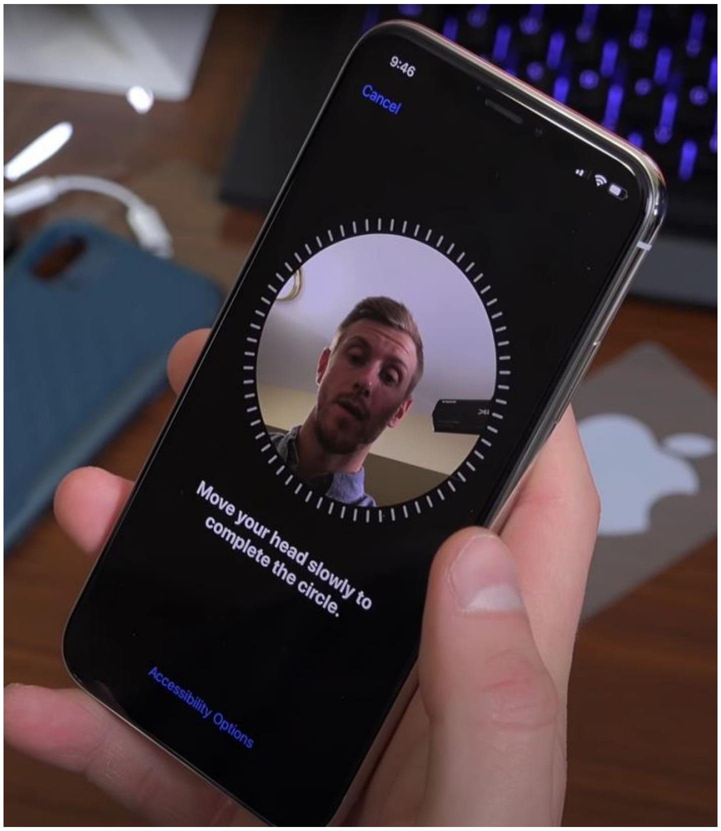
///

//

//

//

68. A user is then automatically prompted with a new page, asking the user to "Move your head slowly to complete the circle."



//

//

//

//

//

//

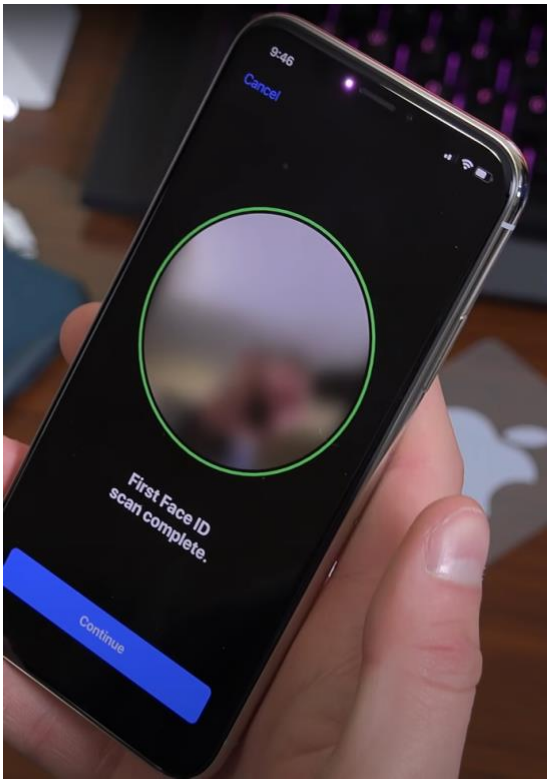
//

//

//

//

69. After a user does so, the next page states that the "First Face ID scan [is] complete."



//

//

//

//

//

//

//

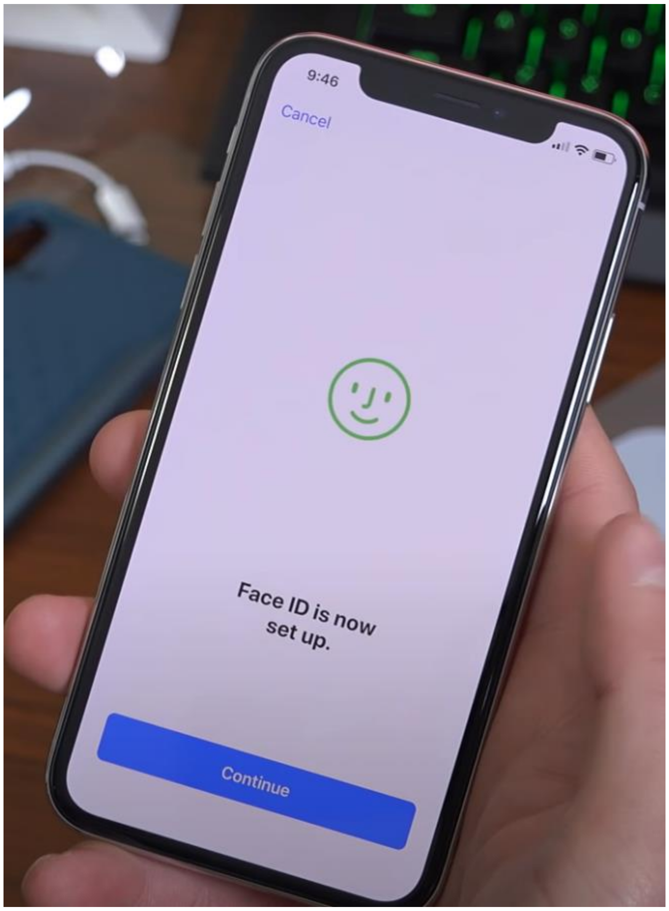
//

//

//

//

70. After a user clicks on “continue,” a second scan is completed, utilizing the same dialogs and functions as the first scan. After completing the second scan, a user is prompted with the following page. After clicking complete, the user moves to the next step in the set-up process.



9:46

Face ID is now set up.

//

//

//

//

//

//

//

71. This is the full extent of Defendant's visible representations during the enrollment process. All Apple Products equipped with Face ID employ the same process for set-up and use of Face ID.

72. This enrollment process fails to inform a user of "the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used[.]" *See* 740 ILCS 14/15(b)(2).

73. During this process, Defendant also fails to receive "a written release executed by" the users. *See* 740 ILCS 14/15(b)(3).

74. Thus, Defendant violates 740 ILCS 14/15(b)(2) and (3).

75. Altogether, Apple's Touch ID and Face ID brings together into one body or place—and thus captures and collects—a user's biometrics. Apple also controls—and thus possesses—a user's biometrics. Defendant's contractual relationship with users is direct, ongoing, and intertwined with other services Apple provides. Defendant wholly owns and exclusively controls the software used to capture, collect, and possess a user's biometrics. Defendant's enrollment process fails to inform users of the specific purpose and length of time a user's biometric identifier or information is being collected or stored. Defendant also fails to receive a written release from users. And Defendant fails to make publicly available a written retention schedule for destroying a user's biometrics. Accordingly, Defendant's Face ID and Touch ID Products violate § 15(a) and §§ 15(b)(2) and (3) of BIPA.

IV. Experience of Plaintiff David Barnett

76. In August 2020, Plaintiff purchased a MacBook equipped with Touch ID. When setting up his MacBook, Plaintiff Barnett was prompted to set up Touch ID. Plaintiff Barnett

followed the prompt as directed and provided his fingerprint pursuant to Defendant's directions. As recently as April 12, 2021, Plaintiff Barnett employed Touch ID to unlock his MacBook.

77. To employ Touch ID, Defendant required Plaintiff to place his fingers on a fingerprint scanner, at which point Defendant scanned, collected, captured, and obtained Plaintiff's fingerprints.

78. Then, upon information and belief, Defendant's proprietary software translated Plaintiff's fingerprint scans into a unique mathematical representation, which it then stored locally.

79. Upon information and belief, each time Plaintiff Barnett used Touch ID after his initial enrollment, Defendant captured and collected a scan of Plaintiff's fingerprint, translated it into a unique mathematical representation, and then compared this representation against Plaintiff Barnett's previously stored biometric information.

80. Plaintiff Barnett never received, and Defendant never provided, information about the specific purpose and length of time for which his biometric identifier or biometric information was being collected or stored as required by 740 ILCS 14/15(b)(2).

81. Plaintiff Barnett never executed, and Defendant never received, a written release as required by 740 ILCS 14/15(b)(3).

82. Plaintiff Barnett never received, nor was made aware of, any publicly available written policy establishing a retention schedule or guidelines for permanently destroying his biometrics as required by 740 ILCS 14/15(a).

83. By collecting Plaintiff Barnett's unique biometric identifiers and/or biometric information without his consent, Defendant invaded Plaintiff's statutorily protected right to privacy in his biometrics.

VI. Experience of Plaintiff Burr

84. In October 2019, Plaintiff Burr purchased an iPhone 11 equipped with Face ID. When setting up her iPhone, Plaintiff Burr was prompted to set up Face ID. Plaintiff Burr followed the prompt as directed and provided her facial geometry pursuant to Defendant's directions. As recently as May 20, 2021, Plaintiff Burr employed Face ID to unlock her iPhone 11.

85. To employ Face ID, Defendant required Plaintiff to rotate her face in view of a facial geometry scanner, at which point Defendant scanned, collected, captured, and obtained Plaintiff's facial geometry.

86. Then, upon information and belief, Defendant's proprietary software translated Plaintiff's facial geometry into a unique mathematical representation, which it then stored locally.

87. Upon information and belief, each time Plaintiff Burr used Face ID after her initial enrollment, Defendant captured and collected a scan of Plaintiff's facial geometry, translated it into a unique mathematical representation, and then compared this representation against Plaintiff's previously stored biometric information.

88. Plaintiff Burr never received, and Defendant never provided, information about the specific purpose and length of time for which her biometric identifier or biometric information was being collected or stored as required by 740 ILCS 14/15(b)(2).

89. Plaintiff Burr never executed, and Defendant never received, a written release as required by 740 ILCS 14/15(b)(3).

90. Plaintiff Burr never received, nor was made aware of, any publicly available written policy establishing a retention schedule or guidelines for permanently destroying his biometrics as required by 740 ILCS 14/15(a).

91. By collecting Plaintiff Burr's unique biometric identifiers and/or biometric information without her consent, Defendant invaded Plaintiff's statutorily protected right to privacy in her biometrics.

VI. Experience of Plaintiff Michael Henderson

92. In July 2020, Plaintiff Henderson purchased an iPhone 7 equipped with Touch ID. When setting up his iPhone 7, Plaintiff Henderson was prompted to set up Touch ID. Plaintiff Henderson followed the prompt as directed and provided his fingerprint pursuant to Defendant's directions. As recently as April 12, 2021, Plaintiff Henderson employed Touch ID to unlock his iPhone 7.

93. To employ Touch ID, Defendant required Plaintiff to place his fingers on a fingerprint scanner, at which point Defendant scanned, collected, captured, and obtained Plaintiff's fingerprints.

94. Then, upon information and belief, Defendant's proprietary software translated Plaintiff's fingerprint scans into a unique mathematical representation, which it then stored locally.

95. Upon information and belief, each time Plaintiff Henderson used Touch ID after his initial enrollment, Defendant captured and collected a scan of Plaintiff's fingerprint, translated it into a unique mathematical representation, and then compared this representation against Plaintiff's previously stored biometric data.

96. Plaintiff Henderson never received, and Defendant never provided, information about the specific purpose and length of time for which his biometric identifier or biometric information was being collected or stored as required by 740 ILCS 14/15(b)(2).

97. Plaintiff Henderson never executed, and Defendant never received, a written release as required by 740 ILCS 14/15(b)(3).

98. Plaintiff Henderson never received, nor was made aware of, any publicly available written policy establishing a retention schedule or guidelines for permanently destroying his biometrics as required by 740 ILCS 14/15(a).

99. By collecting Plaintiff Henderson's unique biometric identifiers and/or biometric information without his consent, Defendant invaded Plaintiff's statutorily protected right to privacy in his biometrics.

CLASS ALLEGATIONS

100. **Class Definition:** Plaintiffs Barnett and Henderson bring this action pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals, defined as follows (the "Touch ID Class"):

> All Illinois residents who had their fingerprints possessed, captured, collected, stored, or otherwise obtained by Defendant's Touch ID in the state of Illinois.

101. Plaintiff Burr brings this action pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals, defined as follows (the "Face ID Class"):

> All Illinois residents who had their facial geometry possessed captured, collected, stored, or otherwise obtained by Defendant's Face ID in the state of Illinois.

102. **Numerosity:** Pursuant to 735 ILCS 5/2-801(1), the number of persons within the Classes are substantial, believed to amount to hundreds of thousands, if not millions, of persons. It is, therefore, impractical to join each member of the Classes as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Classes renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Classes are ascertainable and identifiable from Defendant's records.

103. **Commonality and Predominance:** Pursuant to 735 ILCS 5/2-801(2), there are well-defined common questions of fact and law that exist as to all members of the Classes and that predominate over any questions affecting only individual members of the Classes. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member, include, but are not limited to, the following:

(a) whether Defendant collected, captured, or otherwise obtained Plaintiffs' and the Classes' biometric identifiers and/or biometric information;

(b) whether Defendant properly informed Plaintiffs and the Classes that it collected, captured, or otherwise obtained their biometric identifiers and/or biometric information;

(c) Whether Defendant received a written release from Plaintiffs to capture, collect, or otherwise obtain their biometric identifiers and/or biometric information;

(d) whether Defendant used Plaintiffs' and the Classes' biometric identifiers and/or biometric information to identify them;

(e) whether Defendant possessed Plaintiffs' and the Classes' biometric identifiers and/or biometric information without developing and following a publicly available written policy establishing a retention schedule and guidelines for permanently destroying the information; and

(f) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

104. **Adequate Representation:** Pursuant to 735 ILCS 5/2-801(3), Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiffs are able to fairly and adequately represent and protect the interests of such Classes. Neither Plaintiffs nor their counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Classes. Plaintiffs have raised

viable statutory claims or the type reasonably expected to be raised by members of the Classes, and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Classes, additional claims as may be appropriate, or to amend the Class definition to address any steps that Defendant took.

105. **Superiority:** Pursuant to 735 ILCS 5/2-801(4), a class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Classes could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Classes. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

COUNT I – FOR DAMAGES AGAINST DEFENDANTS
VIOLATION OF 740 ILCS 14/15(a) –
FAILURE TO INSTITUTE, MAINTAIN, AND ADHERE TO PUBLICLY AVAILABLE RETENTION SCHEDULE

(Both Face ID Class and Touch ID Class)

106. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

107. BIPA makes it unlawful for Defendant to possess biometric identifiers and biometric information without establishing and following certain procedures. Specifically, BIPA mandates that "[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." 740 ILCS 14/15(a).

108. Defendant has not created, and has not made publicly available, a retention schedule and guidelines for permanently destroying Plaintiffs' and the Classes' biometric identifiers and biometric information.

109. Defendant thus violated 740 ILCS 14/15(a).

110. On behalf of themselves and the Classes, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Classes by requiring Defendant to comply with BIPA's requirements for the possession, control, and use of biometric identifiers and biometric information as described herein; (3) 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); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Barnett, Plaintiff Burr, and Plaintiff Henderson, on behalf of themselves and the proposed Classes, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiffs as representatives of the Classes, and appointing their counsel as Class Counsel;
B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;
C. Awarding statutory damages of $5,000.00 for each and every intentional and/or

reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the Court finds that Defendant's violations were negligent;

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

E. Awarding Plaintiffs and the Classes their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

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

G. Awarding such other and further relief as equity and justice may require.

COUNT II – FOR DAMAGES AGAINST DEFENDANTS
VIOLATION OF 740 ILCS 14/15(b) –
FAILURE TO OBTAIN INFORMED WRITTEN CONSENT AND RELEASE BEFORE OBTAINING BIOMETRIC IDENTIFIERS OR INFORMATION

(Both Face ID Class and Touch ID Class)

111. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

112. BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject … in writing 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) (emphasis added).

113. Defendant failed to comply with these BIPA mandates.

114. Defendant is a company registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

115. Plaintiffs and the Class are individuals who have had their "biometric identifiers" collected and/or captured by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

116. Plaintiffs' and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

117. Defendant systematically and automatically collected, captured, stored, or otherwise obtained Plaintiffs' and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

118. Defendant never informed Plaintiffs, and never informed any member of the Classes at least prior to June 2021, in writing that their biometric identifiers and/or biometric information were being collected, captured, or otherwise obtained, nor did Defendant inform Plaintiffs and the Classes in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being captured, collected and stored as required by 740 ILCS 14/15(b)(2)-(3).

119. By collecting, capturing, or otherwise obtaining Plaintiffs' and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiffs' and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

120. On behalf of themselves and the Classes, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Classes by requiring Defendant to comply with BIPA's requirements for the collection, captures, storage, and use of biometric identifiers and biometric information as described herein; (3) 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); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Barnett, Plaintiff Burr, and Plaintiff Henderson, on behalf of themselves and the proposed Classes, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiffs as representatives of the Classes, and appointing their counsel as Class Counsel;
B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;
C. Awarding statutory damages of $5,000.00 for each and every intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the Court finds that Defendant's violations were negligent;
D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an Order requiring Defendant to collect, store, and use biometric identifiers and/or biometric information in compliance with BIPA;
E. Awarding Plaintiffs and the Classes their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);
F. Awarding Plaintiffs and the Classes pre- and post-judgment interest, to the extent allowable; and
G. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

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

Dated: June 25, 2021

Respectfully submitted,

/s/ William Beaumont
William H. Beaumont

BEAUMONT COSTALES LLC
William H. Beaumont (#6323256)
107 W. Van Buren, Suite 209
Chicago, IL 60605
Tel: (773) 831-8000
E-mail: whb@beaumontcostales.com
Local Counsel for Plaintiffs and the Putative Classes

BURSOR & FISHER, P.A.
Philip L. Fraietta (*Pro Hac Vice Forthcoming*)
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Brittany S. Scott (*Pro Hac Vice Forthcoming*)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: bscott@bursor.com

BURSOR & FISHER, P.A.
Rachel L. Miller (*Pro Hac Vice Forthcoming*)
Christopher R. Reilly (*Pro Hac Vice Forthcoming*)
701 Brickell Avenue, Suite 1420
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
Email: rmiller@bursor.com
creilly@bursor.com
Attorneys for Plaintiffs and the Putative Classes