IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BENJAMIN CHEN and RORY KESSLER, individually and on behalf of all others similarly situated, Plaintiffs, v. TARGET CORPORATION and TARGET BRANDS, INC., Defendants.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Benjamin Chen and Plaintiff Rory Kessler ("Plaintiffs"), by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves and their counsel, which are based on personal knowledge, against Defendants Target Corporation and Target Brands, Inc. ("Defendants" or "Target").

NATURE OF THE ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendants in collecting, retaining, and storing theirs and other similarly situated individuals' biometric identifier information[1] (referred to at times as "biometrics") without properly disclosing or notifying Plaintiffs and Class Members in direct violation of the New York City Biometric Identifier Information Law ("NYC BIIL" or "BIIL"), New York City, N.Y., Code § 22-1201, *et seq*.

[1] "The Term 'biometric identifier information' means a physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic." New York City, N.Y., Code § 22-1201

2. The New York City Council has found that "[d]evelopments in facial recognition and other biometric technology pose new consumer protection challenges in an atmosphere where there are already growing concerns about privacy and personal data."[2] The City Council passed the NYC BIIL in response to these challenges, which include, *inter alia*, the technological limitations, privacy-related issues, and cyber security hazards associated with the collection and use of biometrics.[3] Turning to the first of these, technological limitations, the City Council has remarked extensively on how the use of biometric technology raises "significant concerns about accuracy, especially for women, children, African Americans, and Asians for whom . . . algorithms are known to be less accurate."[4] The Council noted that "AI systems learn what they are taught. If they are not taught with robust and diverse data sets, accuracy and fairness could be at risk[]"[5] because "systems that are trained within only a narrow context of a specific data set will inevitably acquire bias that skews its learning towards the specific characteristics of that data set."[6] The BIIL evinces the City Council's recognition of how "[s]uch errors can be particularly damaging for individuals[,]" including those "who are mistakenly entered into a criminal database, for example, of supposed shoplifters."[7] One such error that the City Council found to be instructive was "the alleged case for student Ousmane Bah," who claimed "his name was mistakenly linked to the face

[2] https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3704369&GUID=070402C0-43F0-47AE-AA6E-DEF06CDF702A&Options=ID%7cText%7c&Search=, Hearing Transcript 12/10/20, p. 4-5.
[3] https://legistar.council.nyc.gov/View.ashx?M=F&ID=9004887&GUID=B0996283-26E6-4083-ACFC-830AE3AED308, Committee Report 12/10/20, p. 9, 12, 13.
[4] https://legistar.council.nyc.gov/View.ashx?M=F&ID=7761013&GUID=CAC07AB4-200A-46FC-8F2D-4D0B72E9D9E2, Committee Report 10/7/19, p. 7.
[5] *Id.* at p. 8.
[6] *Id.*
[7] https://legistar.council.nyc.gov/View.ashx?M=F&ID=9168703&GUID=A11149B9-F476-462B-B902-95153CEDC7D2, Minutes of the Stated Meeting – December 10, 2020, p. 2482.

of a thief who stole products from an Apple store. The flawed facial recognition hit resulted in the NYPD arriving at Bah's home to arrest him for crimes he had no part in."[8]

3. While working on the BIIL, the City Council also expressed apprehension about the privacy-related issues that have accompanied the advent of biometric technology. Namely, the Council wrote and spoke at length about how, in "New York City, as well as many other municipalities, establishments frequently do not inform customers"[9] that biometric technology is being utilized and "companies developing this type of software sometimes resort to shady or deceitful tactics to expand their databases or improve their product."[10] Of particular note to the City was how, "in Atlanta, Google was hiring contractors to deliberately target people of color encouraging them to scan their faces in exchange for a $5.00 gift card so that they could improve its new pixel device."[11] The Council was also distressed at how companies have been known to "conceal the fact that people's faces were being recorded and even lie to maximize their data collections[]"[12] and noted that "[t]hese kinds of deceptive practices are simply not acceptable."[13]

4. Likewise, the City Council sought to address how individuals' biometrics often come to be stored in "numerous private and public databases of information, which may be sold, shared, or used in ways that the consumer does not necessarily understand or consent to."[14] The legislative history of the BIIL mentions how "data from consumer-based surveillance software

---

[8] *Id.*
[9] https://legistar.council.nyc.gov/View.ashx?M=F&ID=9004887&GUID=B0996283-26E6-4083-ACFC-830AE3AED308, Committee Report 12/10/20, p. 14.
[10] https://legistar.council.nyc.gov/View.ashx?M=F&ID=7786279&GUID=16F7F4CE-9E1B-4629-A11F-232A2BCC31DF, Hearing Transcript 10/7/19, p. 10.
[11] *Id.*
[12] *Id.* at p. 10-11.
[13] *Id.* at 11.
[14] https://legistar.council.nyc.gov/View.ashx?M=F&ID=7761013&GUID=CAC07AB4-200A-46FC-8F2D-4D0B72E9D9E2, Committee Report 10/7/19, p. 9.

such as Ring (which uses cameras to monitor a person's doorbell and/or entryway), is also being shared with law enforcement[,]"[15] and how "[g]overnment agencies have [] been accused of mining personal biometric data[]" such as when "Immigration and Customs Enforcement ('ICE') used facial recognition software to mine state driver's license databases."[16]

5. Relatedly, the Council remarked on the ways in which biometrics may be paired with "multiple tracking technologies" to "manipulate the availability, cost, and appeal of an item."[17] It noted that companies already draw upon "customer information to determine the ideal cost at which a shopper will purchase a particular product"[18] by using, *inter alia*, "the data obtained by social media platforms, such as shoppers' e-mail addresses and other personal information."[19] This information is voluminous and "enables retailers 'to develop a broad picture about a consumer, such as identifying that the individual owns a house, runs marathons, eats healthy food, has a premium bank card, and is good in financial health.'"[20] The BIIL marks the City's trepidation about how "[c]onnecting such data to a customers' faceprint [or other biometrics] would allow retailers to inflate the price of a product to consumers in the store willing and able to pay more, while offering the same product to other consumers for less money."[21] The City found it especially egregious that "this information[is] mostly collected without consumers' knowledge or consent[.]"[22]

---

[15] *Id.* at p. 14.
[16] *Id.* at p. 13-14.
[17] https://legistar.council.nyc.gov/View.ashx?M=F&ID=7761013&GUID=CAC07AB4-200A-46FC-8F2D-4D0B72E9D9E2, Committee Report 10/7/19, p. 17.
[18] *Id.*
[19] *Id.* at p. 18.
[20] *Id.*
[21] *Id.*
[22] *Id.*

6. Finally, the BIIL was enacted as a means of confronting the problem that "[b]iometric data is often collected and stored in large databases that, if not properly protected, are susceptible to hacking."[23] The Law's legislative history notes that, "[t]hese databases will likely be exposed to security failures and breaches, information leaks by careless or corrupt employees, hackers, or even foreign intelligence agency break-ins."[24] The Council was especially perturbed by how "researchers discovered a severe vulnerability in the biometric databases of a company called Suprema, which contained the fingerprints of over one million people, as well as facial recognition information, unencrypted usernames and passwords, and personal information of employees of various clients of the company."[25]

7. The BIIL seeks to prevent incidents like this, which, the City noted, "could result in grave consequences for those affected[]"[26] because "[b]iometric information is based on a unique physiological characteristic making it naturally stable and hard to artificially alter."[27] That is, the BIIL embodies the notions that "[b]iometric information is part of a person's identity." [28] "Unlike a password, this information cannot be changed." [29] "When cybercriminals access biometric data — fingerprints, retina, facial, or voice — they gain information that can be linked

[23] https://legistar.council.nyc.gov/View.ashx?M=F&ID=9168703&GUID=A11149B9-F476-462B-B902-95153CEDC7D2, Minutes of the Stated Meeting - December 10, 2020, p. 2483.
[24] https://legistar.council.nyc.gov/View.ashx?M=F&ID=7761013&GUID=CAC07AB4-200A-46FC-8F2D-4D0B72E9D9E2, Committee Report 10/7/19, p. 9.
[25] https://legistar.council.nyc.gov/View.ashx?M=F&ID=9168703&GUID=A11149B9-F476-462B-B902-95153CEDC7D2, Minutes of the Stated Meeting - December 10, 2020, p. 2483.
[26] https://legistar.council.nyc.gov/View.ashx?M=F&ID=7786279&GUID=16F7F4CE-9E1B-4629-A11F-232A2BCC31DF, Hearing Transcript 10/7/19, p. 7.
[27] https://legistar.council.nyc.gov/View.ashx?M=F&ID=7761013&GUID=CAC07AB4-200A-46FC-8F2D-4D0B72E9D9E2, Committee Report 10/7/19, p. 9.
[28] *Id.*
[29] *Id.*

to the identity forever." [30] "The potential damage is irreversible, creating a constant fear of information or identity theft." [31]

8. The Council noted that:

> Alarmingly, stolen biometric identifiers could be used to impersonate consumers, gaining access to personal information and buildings. The use of biometrics for accessing sensitive personal information creates an increased risk of tangible and substantial harm when such information is stolen. The privacy risks of data breaches may also lead to potential future harm even when stolen consumer data is not yet targeted to directly harm the consumer. The heightened alert following a data breach creates uncertain[ty] and a form of lost opportunities as individuals take actions to mitigate against and reduce any potential harms or transactional losses. Although some argue that it is possible to overcome the problem of information leaks or hacks through appropriate security measures, recent sensitive data leaks, numbering hundreds of thousands of military, business, politician and public figures— suggests that nothing is safe."[32]

9. In recognition of these and other concerns related to the collection and use of individuals' biometrics, the New York City Council enacted NYC BIIL, which provides, *inter alia*, that any "commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable." New York City, N.Y., Code § 22-1202(a).

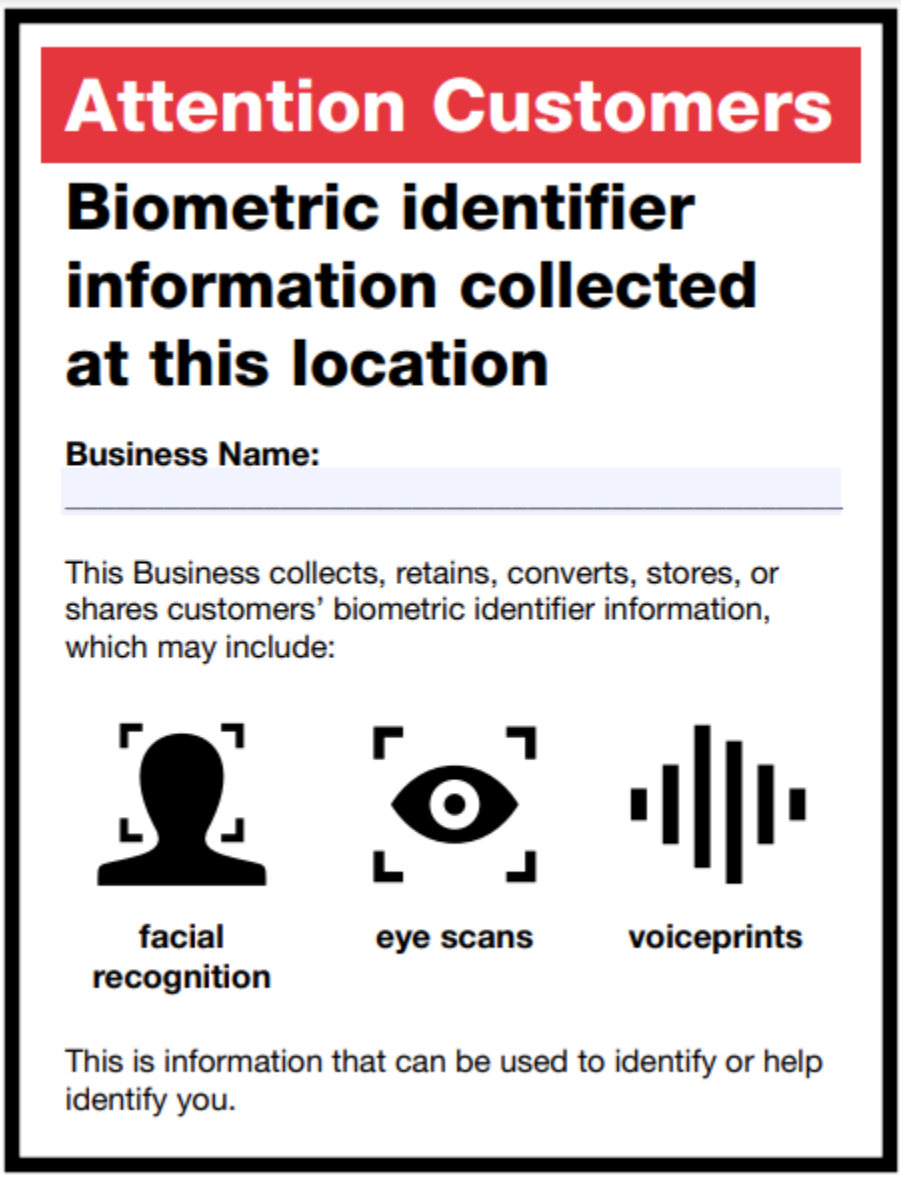
[30] *Id.*
[31] *Id.*
[32] *Id.* at p. 12.

10. The "rule" referenced therein is the Department of Consumer Protection's rule to implement Local Law 3 of 2021,[33] which states:

> To comply with section 22-1202 of chapter 12 of title 22 of the New York City Administrative Code, a commercial establishment covered by such section must post a sign in a clear and conspicuous manner at every entrance used by customers in a size of at least 8.5 inches by 11 inches that discloses if customers' biometric identifier information is being collected, retained, converted, stored, or shared. The requirements of this section may be fulfilled by posting a color copy of the Biometric Identifier Information Disclosure, as made publicly available on the Department's website, in a clear and conspicuous manner at every entrance used by customers in a size of at least 8.5 inches by 11 inches.[34]

11. The "sign" mentioned by the Department of Consumer Protection's rule is called the "Biometric Identifier Information Disclosure" sign, and it has been made available at https://www1.nyc.gov/assets/dca/downloads/pdf/businesses/Biometric-Identifier-Information-Disclosure-Sign.pdf.

[33] https://rules.cityofnewyork.us/rule/biometric-identifier-information/.
[34] https://rules.cityofnewyork.us/wp-content/uploads/2021/07/NOA_DCWP-Rule-re-Biometric-Data-Collection.pdf.



12. None of Defendant's stores in New York City display this sign.

13. In direct violation of each of the foregoing provisions of the NYC BIIL, Defendants: collected, retained, converted, stored, and/or shared – without first placing clear and conspicuous signs near all of its commercial establishments' customer entrances – the biometrics and associated personally identifying information of thousands of its customers.

14. Defendants have been engaged in the practice of collecting, retaining, converting, storing, and/or sharing the biometric identifier information of all individuals who have visited Target in New York City.

15. If Defendants' database of digitized biometric identifier information were to fall into the wrong hands, by data breach or otherwise, the customers to whom these sensitive and immutable biometric identifiers belong could have their identities stolen, among other serious issues.

16. NYC BIIL confers on Plaintiffs and all other similarly situated New York City residents a right to know of such risks, which are inherently presented by the collection, storage, and use of biometrics.

17. The bill provides for a private right of action that allows for judgments of $500 for each violation of section 22-1202. *Id.* § 22-1203.

18. Plaintiffs bring this action to prevent Defendants from further violating the privacy rights of New York City residents and to recover statutory damages for Defendants' having collected and stored individuals' biometrics in violation of NYC BIIL.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendants.

20. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because a substantial portion of the events that gave rise to this cause of action occurred here.

21. This court has personal jurisdiction over Defendants because a substantial portion

of the events that gave rise to this cause of action occurred here, and Defendants own and operate hundreds of stores throughout the State of New York.

PARTIES

22. Plaintiff Benjamin Chen is a citizen and resident of Brooklyn, New York. In or around November 2023, Plaintiff Chen visited a Target store located in Long Island City, New York and made purchases using Defendants' self-checkout.

23. Plaintiff Rory Kessler is a citizen and resident of Flushing, New York. In or around February 2024, Plaintiff Kessler visited a Target store located in Manhattan, New York and made purchases using Defendants' self-checkout.

24. Defendant Target Corporation is a Minnesota corporation, with its principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota.

25. Defendant Target Brands, Inc. is a subsidiary of Target Corporation, with its principal executive offices located at 1000 Nicollet Mall, Minneapolis, Minnesota.

FACTUAL BACKGROUND

I. The New York City Biometric Identifier Information Law.

26. The use of a biometric scanning system in commercial establishments entails serious risks. Facial and body scans are permanent, unique biometric identifiers associated with particular consumers. This exposes consumers to serious and irreversible privacy risks. For example, if a device or database containing employees' facial scan data is hacked, breached, or otherwise exposed, consumers have no means by which to prevent identity theft and unauthorized tracking.

27. Recognizing the need to protect citizens from these risks, New York City enacted the Biometric Identifier Information law, New York City, N.Y., Code § 22-1201, *et seq*. ("NYC

BII") in 2021, to regulate companies that collect and store biometric information. *See* New York City Council Committee on Consumer Affairs and Business Licensing, Transcript December 10, 2020.

28. As alleged below, Defendants' practice of collecting, retaining, converting, storing, and/or sharing biometric identifier information without having first placing clear and conspicuous signs near all of its commercial establishments' customer entrances violated NYC BIIL.

II. Defendants Violate The New York City Biometric Identifier Information Law.

29. In direct violation of NYC BIIL, Defendants have collected, retained, converted, stored, and/or shared the biometric identifier information of all individuals who have visited Target in New York City.

30. Defendants' United States patent, published on December 20, 2018, for their Volumetric Modeling To Identify Image Areas For Pattern Recognition technology ("Pattern Recognition Technology"), lays out how Defendants capture, collect, and store customers' biometrics, including customers facial geometry scans and body shapes.[35]

31. Defendants' Pattern Recognition Technology at issue here is described as follows in Defendants' patent:

> The embodiments described below use volumetric modeling of objects in a building to identify portions of camera images that would be useful during pattern recognition. For example, one embodiment uses volumetric modeling to identify a region of a camera image that will contain a face. This region of the camera image is then provided to a facial recognition system to link the image to an identifier for a person.

32. Defendants use their technology for a variety of recognition purposes, including

[35] Donnie Scott Tolbert, Michael Tyler Ahlm. Target Brands, Inc. Volumetric Modeling To Identify Image Areas For Pattern Recognition. Patent US 2018/0365481 A1. Pub. Dec. 20, 2018.

"pedestrian detection, clothing recognition, body-shape recognition, and facial recognition." Some if not all of these categories are deemed "biometric identifier information" under BIIL.

33. Simply put, Defendants use their patented Pattern Recognition Technology in Target store locations to capture customers' biometric identifier information via camera images throughout the store. Defendants recognize customers' characteristics, capturing and collecting their biometrics, allowing Defendants to track customers' data as they move throughout the store and retain this data in their database.

34. The figure below "is a flow diagram for performing volumetric modeling to identify volumes representing people" included in Defendants' patent:

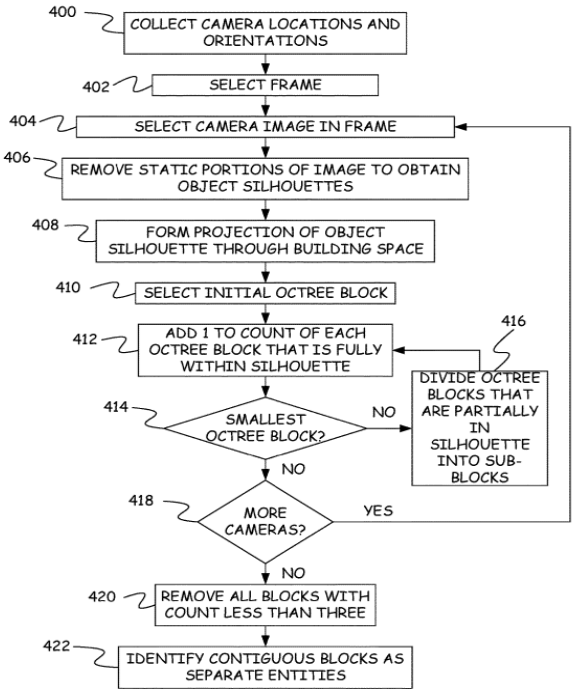


FIG. 4

35. Defendants' pattern recognition technology identifies volumes that represent people, determines their location, searches for these volumes in previous frames to either update

the database of customers' location or generate a new entity in the record with a new entity ID. After a customer is recognized or has a new entity generated within the system, the "volumetric recognition engine generates snapshots of the volume [of the person] for an alternative pattern recognition engine[,]"enabling the technology to track customers as they move about the store. These alternative recognition techniques that "identify entities from camera images" include "pedestrian detection, clothing recognition, body-shape recognition and facial recognition[.]"

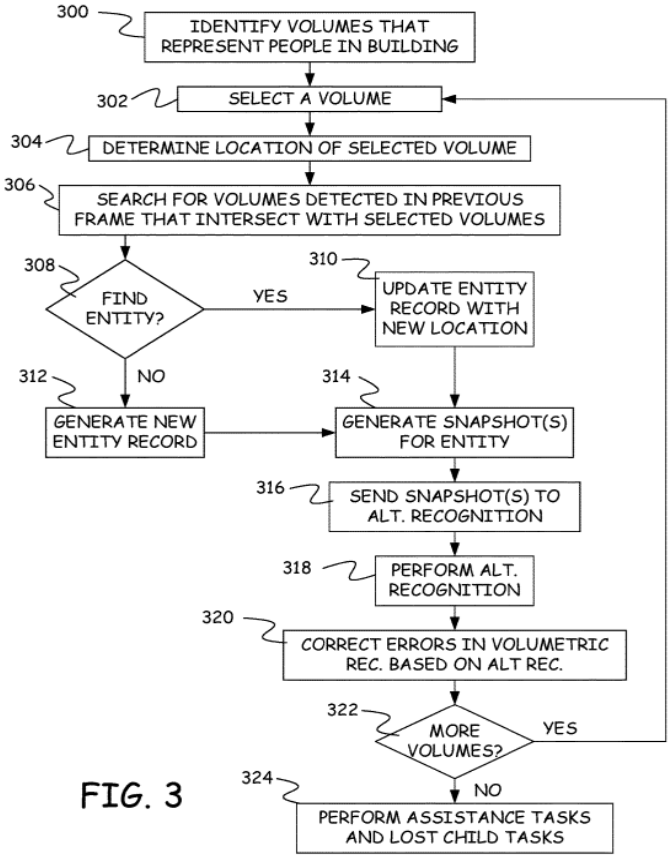


FIG. 3

36. Defendants' technology collects individuals' biometric identifier information to track customers' location, "perform AI recognition" and "perform assistance tasks and lost child tasks." Further, Defendants are able to differentiate children from adults, record this data, and locate a lost child based on previous captured data of the related adult and child's locations and

the child's current location.

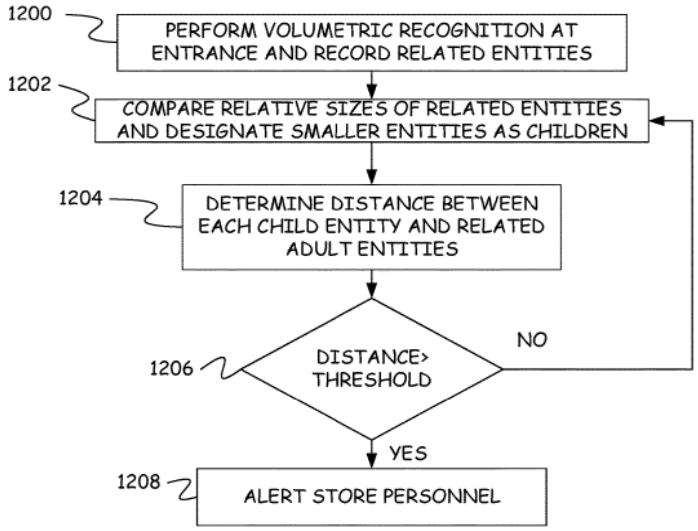


FIG. 12

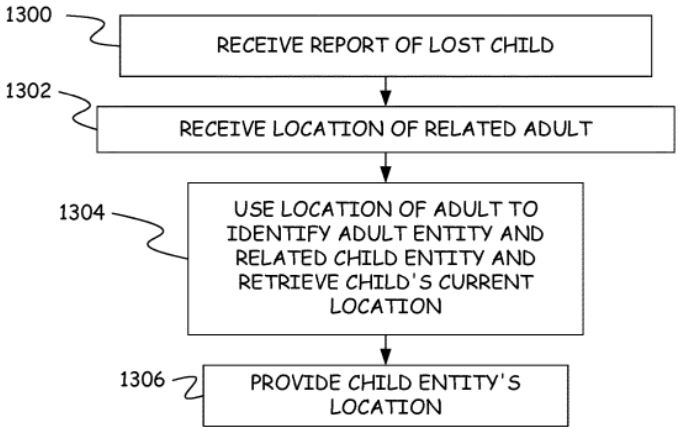


FIG. 13

37. Defendants have hundreds of cameras throughout their stores, including cameras that actively monitor customers when they utilize Defendants' self-checkouts. Each of Defendants cameras are equipped with their patented technology explained above.

38. Given the foregoing, Target has collected, retained, converted, stored and/or shared biometric identifier information of customers in violation of New York City, N.Y., Code § 22-1202(a).

III. Experience of Plaintiff Benjamin Chen.

39. In or around November 2023, Plaintiff Chen visited a Target store located in Long Island City, New York and made purchases using Defendants' self-checkout.

40. During the course of visiting the store and the self-checkout transaction, Defendants collected, retained, converted, stored, and/or shared Plaintiff's biometric identifier information.

41. Defendants never disclosed to Plaintiff, through clear and conspicuous signage near all of the Target location's customer entrances, that it collects, retains, converts, stores or shares biometric identifier information, including that of Plaintiff Chen.

42. Thus, Defendants invaded Plaintiff Chen's statutorily protected right to privacy in his biometrics.

IV. Experience of Plaintiff Rory Kessler.

43. In or around February 2024, Plaintiff Rory Kessler visited a Target store located in Manhattan, New York and made purchases using Defendants' self-checkout.

44. During the course of visiting the store and the transaction, Defendants collected, retained, converted, stored, and/or shared Plaintiff's biometric identifier information.

45. Defendants never disclosed to Plaintiff, through clear and conspicuous signage near all of the Target location's customer entrances, that it collects, retains, converts, stores or shares biometric identifier information, including that of Plaintiff Kessler.

46. Thus, Defendants invaded Plaintiff Kessler's statutorily protected right to privacy in his biometrics.

CLASS ALLEGATIONS

47. **Class Definition:** Plaintiffs bring this action pursuant to New York City, N.Y., Code § 22-1201, *et seq*. on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All individuals who had their biometric identifier information collected, captured, received or otherwise obtained and/or stored by Defendants upon visiting Defendants' stores located in New York City.

48. **Numerosity:** The number of persons within the Class is substantial, believed to amount to thousands of persons. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class 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 Class is ascertainable and identifiable from Defendant's records.

49. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. 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 Defendants collected, retained, converted, stored and/or shared Plaintiffs' and the Class' biometric identifier information;

(b) whether Defendants placed a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that Plaintiffs' and the Class' biometric identifier information was being collected, retained, converted, stored or shared.

50. **Adequate Representation:** 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 a Class. Neither Plaintiffs nor their counsel has any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs have raised viable statutory claims or the type reasonably expected to be raised by members of the Class, 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 Class, additional claims as may be appropriate, or to amend the Class definition to address any steps that Defendants took.

51. **Superiority:** 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 Class 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 Class. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with NYC BIIL.

COUNT I

Violations of New York City, N.Y., Code § 22-1202, *et seq.*

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

53. NYC BIIL states:

> [a]ny commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable. New York City, N.Y., Code § 22-1202(a).

54. Plaintiffs and the Class are individuals who have had their "biometric identifier information" collected and/or captured by Defendants, through its patented pattern recognition technology employed at Target store locations in New York City, as explained in detail above. This includes facial geometry scans and body shape recognition.

55. Plaintiffs' and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by NYC BIIL. *See* § 22-1201.

56. Defendants did not provide proper notice to Plaintiffs and the putative class. NYC BIIL requires any "commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable." New York City, N.Y., Code § 22-1202(a). Defendants failed to comply with these BIIL mandates.

57. Under NYC BIIL, "the term 'commercial establishment' means a place of entertainment, a retail store, or a food and drink establishment." New York City, N.Y., Code § 22-1201.

58. The Target locations at which Plaintiffs and the Class had their biometric identifier information collected, retained, converted, stored, and/or shared were thus commercial establishments under NYC BIIL.

59. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by

requiring Defendants to comply with NYC BIIL's requirements for the collection, captures, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $500 for each violation of New York City, N.Y., Code § 22-1202(a) pursuant to New York City, N.Y., Code § 22-1203(1); and (4) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses pursuant to New York City, N.Y., Code § 22-1203(4).

60. In accordance with New York City, N.Y., Code § 22-1203, on May 1, 2024 — "[a]t least 30 days prior to initiating any action"— Plaintiffs provided written notice to Defendants of the allegations set forth herein. Defendants did not cure such actions alleged by Plaintiffs and continue to violate New York City, N.Y., Code § 22-1202(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Benjamin Chen and Plaintiff Rory Kessler, on behalf of themselves and the proposed Class, respectfully requests that this Court enter an Order:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class members;

b. For an order declaring that Defendants' conduct violates the statutes referenced herein;

c. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

d. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

e. For prejudgment interest on all amounts awarded;

f. For an order of restitution and all other forms of equitable monetary relief;

g. For an order enjoining Defendants from continuing the illegal practices detailed herein and compelling Defendants to undertake a corrective advertising campaign; and

h. For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY DEMAND

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

Dated: July 19, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta
Matthew A. Girardi
Caroline C. Donovan
1330 Avenue of the Americas, Fl 32
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: pfraietta@bursor.com
mgirardi@bursor.com
cdonovan@bursor.com

Attorneys for Plaintiffs