IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ADRIAN COSS and MARIBEL OCAMPO, individually and on behalf of all others similarly situated, Plaintiffs, v. SNAP INC., Defendant.	)	Case No. 1:22-cv-02480

CLASS ACTION COMPLAINT

NOW COME the Plaintiffs, ADRIAN COSS and MARIBEL OCAMPO, by and through their counsel, James C. Vlahakis, and state as follows:

I. Introduction & Summary of the Illinois Biometric Information Privacy Act

1. Plaintiffs MARIBEL OCAMPO and ADRIAN COSS (hereafter "Plaintiffs") are citizens of Illinois and reside in the Northern District of Illinois.

2. Plaintiffs allege that Defendant violated Plaintiffs' privacy rights as codified by the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA").

3. BIPA was enacted in 2008 for the purpose of addressing a "very serious need for protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Session No. 276.

4. BIPA's express Legislative Findings provide as follows:

> (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) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.
>
> (f) The full ramifications of biometric technology are not fully known.
>
> (g) 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.

740 ILCS 14/5.

5. BIPA prohibits private entities from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric information unless the private entity: (1) informs that person in writing that identifiers and information will be collected and/or stored; (2) informs the person in writing of the specific purpose and length for which the identifiers or information is being collected, stored or used; (3) receives a written release from the person for the collection of that data; and (4) publishes publicly available written retention schedules and guidelines for permanently destroying said data. *See* 740 ILCS 14/15(a) and (b).

6. The Illinois Supreme Court has recognized that BIPA was enacted to preserve an individual's right to privacy and control over his/her/their biometric data:

> Through the Act, our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information. The duties imposed on private entities by section 15 of the Act (740 ILCS 14/15 (West 2016)) regarding the collection, retention, disclosure, and destruction of a person's or customer's biometric identifiers or biometric information define the contours of that statutory right. Accordingly, when a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or

> customer whose biometric identifier or biometric information is subject to the breach.
>
> * * *
>
> The Act vests in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent. . . . When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, "the right of the individual to maintain his or her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized." This is no mere "technicality." The injury is real and significant.

Rosenbach v. Six Flags Ent. Corp., 432 Ill. Dec. 654, 129 N.E.3d 1197, 1206 (Ill. 2019)).

7. Defendant Snap Inc. ("Defendant" or "Snap") is a Delaware corporation with its principal place of business located in Santa Monica, California.

8. Defendant is a publicly traded company, and is listed on the New York Stock Exchange under the trading symbol "SNAP."

9. Defendant is the owner and operator of a "Snapchat".

10. Defendant has described itself as "a camera company." See, Defendant's Form 10-Q for the quarterly period ending March 31, 2022, at p. 10.

11. Snap's Form 10-Q for the period ending March 31, 2022, is located at https://investor.snap.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=15745081[1]

12. Defendant has described "Snapchat" as its "flagship product. *Id.*

13. Snapchat "is a camera application that was created to help people communicate through short videos and images called 'Snaps.'" *Id.*

14. As detailed below, Snapchat utilizes technology that is subject to BIPA.

[1] A pdf version of this document is hosted at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001564408/c10435fc-36f6-4f32-b8f0-f1617a9e1e8a.pdf

15. As detailed below, certain technology utilized by Snapchat required Defendant to obtain informed written consent from Shapchat users before Defendant was able to acquire the biometric identifiers and/or biometric information of Snapchat users.

16. Plaintiff Coss has utilized the Snapchat app. to create and post Snaps by and through the Snapchat app.

17. Plaintiff Ocampo has utilized the Snapchat app. to create and post Snaps by and through the Snapchat app.

18. Plaintiff Coss has utilized the Snapchat app. to create and post photographic based Snaps where the Snaps involved their unique facial features.

19. Plaintiff Ocampo has utilized the Snapchat app. to create and post photographic based Snaps where the Snaps involved their unique facial features.

20. Plaintiff Coss has utilized the Snapchat app. to create and post video based Snaps where the Snaps involved their unique facial features.

21. Plaintiff Ocampo utilized the Snapchat app. to create and post video based Snaps where the Snaps involved their unique facial features.

22. Plaintiff Coss has utilized the Snapchat app. to create and post Snaps that depicted their unique voices.

23. Plaintiff Ocampo utilized the Snapchat app. to create and post Snaps that depicted their unique voices.

24. As described below, Defendant has violated Plaintiffs' privacy rights in violation of rights and prohibitions set forth by BIPA.

25. On November 26, 2021, Plaintiff Coss has opted out of Defendant's arbitration clause that was contained within Defendant's Terms of Service dated November 15, 2021.

26. Defendant acknowledged receipt of Plaintiff Coss' opt-out request at 1:13 p.m. on November 26, 2021.

27. On November 28, 2021, Plaintiff Ocampo has opted out of Defendant's arbitration clause that was contained within Defendant's Terms of Service dated November 15, 2021.

28. In November and December of 2020, More than forty (40) Illinois users of Snapchat have opted out of opted out of Defendant's arbitration clause that was contained within Defendant's Terms of Service dated November 15, 2021.

II. Jurisdiction and Venue

29. Section 20 of BIPA provides Plaintiffs with a private right of action to assert violations of BIPA. *See, Rosenbach*, 432 Ill. Dec. at 660, 129 N.E.3d at 1203; *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 620 (7th Cir. 2020).

30. The Class Action Fairness Act ("CAFA"), codified at 28 U.S.C. § 1332(d), provides jurisdiction for civil action on the basis of a diversity of citizenship, if the amount in controversy exceeds $5,000,000.

31. CAFA, in relevant part, states as follows:

> (2) The district courts shall have original jurisdiction of any civil action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which—
>
> (A) any member of a class of plaintiffs is a citizen of a State different from any defendant[.]
>
> ***
>
> (6) In any class action, the claims of the individual class members shall be aggregated to determine whether the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs.

28 U.S.C. §§ 1332(d)(2), 1332(d)(6).

32. For federal jurisdiction to exist under CAFA, more than 100 putative class members should theoretically exist. 28 U.S.C. § 1332(d)(5)(B).

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.