NO

EXHIBITS

CASE NO. 2018CH11884

DATE: 9/20/2018

CASE TYPE: Class Action

PAGE COUNT: 13

CASE NOTE

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

MICHAEL KOMORSKI, individually and on behalf of similarly situated individuals,	)	
Plaintiff,	)	No. 2018CH11884
v.	)	Hon.
U-TEC GROUP INC., a California corporation.	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Michael Komorski, both individually and on behalf of similarly situated individuals, brings this Class Action Complaint against Defendant U-TEC GROUP INC. ("Defendant"), to stop its capture, collection, use, and storage of individuals' biometric identifiers and/or biometric information in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (the "BIPA"), and to obtain redress for all persons injured by its conduct. Plaintiff alleges as follows based upon personal knowledge as to his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

INTRODUCTION

1. BIPA defines a "biometric identifier" as any personal feature that is unique to an individual, including fingerprints and palm scans. "Biometric information" is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS § 14/10. Collectively, biometric identifiers and biometric information are known as "biometrics."

2. Defendant is a company that manufactures electronic, biometric-enabled door locks. However, through its biometric door lock technology, Defendant captures, collects, stores,

and otherwise uses Plaintiff's and other users' biometrics without regard to BIPA and the concrete privacy rights and pecuniary interests that BIPA protects. Defendant's technology requires users to upload, store, and repeatedly transmit their biometrics, *i.e.* their fingerprints, in order to open Defendant's smart lock to homes and/or private areas.

3. The Illinois Legislature passed BIPA to provide individuals with statutory protection in their biometric data privacy rights; to ensure that they would receive certain disclosures before a private entity could collect, obtain and/or use their biometrics; to decrease the risk of a misappropriation of one's identity or a similar compromise of one's privacy; and to ensure that individuals whose biometrics were being collected, obtained and/or used could provide informed consent and be fully aware of how their biometrics were being handled and disposed.

4. Indeed, "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5. For example, even sensitive information like Social Security numbers, when compromised, can be changed. "Biometrics, however, are biologically unique to each individual; therefore, once compromised, the individual has no recourse, is at a heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions. *Id.* The risk is compounded when a person's biometric information is also associated with access to home and vehicle keys.

5. As biometric technology has continued to develop, its usage is becoming more mainstream and is no longer relegated to esoteric corners of commerce. Many businesses and have incorporated biometric applications into their products and/or services, including smart phones and employee timekeeping systems.

6. BIPA provides, *inter alia*, that private entities, such as Defendant, may not obtain and/or possess an individual's biometrics unless it first:

(1) informs that person in writing that biometric identifies or biometric information will be collected or stored;

(2) informs that person in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored and used; and

(3) receives a written release from the person for the collection of their biometric identifiers or biometric information.

740 ILCS 14/5.

7. Compliance with BIPA is straightforward and may be accomplished through a single, signed sheet of paper. BIPA's requirements bestow a right to privacy in biometrics and a right to make an *informed* decision when electing whether to provide or withhold biometrics.

8. In direct violation of the foregoing provisions, Defendant actively captures, collects, stores, and uses, without obtaining informed written consent, the biometrics of hundreds, if not thousands, of Illinois residents whose fingerprints are captured and stored through its biometric door-lock system. In order to authenticate the identity of individuals and, ultimately, open a given door lock, Defendant's system requires users to input their fingerprints, or data derived therefrom. This data is used and transmitted each time a user open's their door.

9. Plaintiff brings this action for damages and other remedies resulting from the actions of Defendant in capturing, storing, using, and disseminating his biometrics, and those of hundreds or thousands of its customers throughout the state of Illinois, without informed written consent, and without informing them through a publicly available policy of how and when the subject biometrics would be stored or disposed of, in direct violation of BIPA.

10. On behalf of himself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendant to comply with BIPA, as well as an award of statutory damages to the Class members and common law monetary damages to be determined at trial, together with costs and reasonable attorneys' fees.

PARTIES

11. At all relevant times, Defendant is a California corporation authorized to transact business in Cook County, Illinois. Defendant transacts business throughout Illinois and in Cook County.

12. At all relevant times, Plaintiff has been a resident and citizen of the State of Illinois.

JURISDICTION AND VENUE

13. This court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant is doing business within this State, and because Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Defendant captured, collected, stored, transferred and/or used Plaintiff's and Class Member's biometrics in this State.

14. Venue is proper in Cook County because Plaintiff resides in Cook County and a substantial part of the events giving rise to Plaintiff's claims occurred in Cook County, as Defendant collected Plaintiff's biometrics when Plaintiff used its technology in Cook County for the purpose of authenticating a door lock.

FACTS SPECIFIC TO PLAINTIFF

15. Defendant's biometric door-lock technology relies on the capture, collection, storage and transmission of its user's biometrics, *i.e.* fingerprints, in order to authenticate whether an individual may open a given door lock.

16. Defendant's locks store up to 95 fingerprints on a single smart lever lock and are connected to the internet via Defendant's Ultraloq App ("App") which enables users to remotely unlock a door with their smartphone.

17. The App also tracks, stores, and logs the data of all users that have authenticated a given lock using their biometrics.

18. During the relevant time period, and seeking entry to his Illinois home via a doorway secured by Defendant's biometric door-lock, Plaintiff was required to scan his fingerprints, resulting in the capture, collection, storage, and transmission to third parties of his biometrics.

19. Despite handling Plaintiff's biometrics through its door-lock, Defendant failed to provide Plaintiff with any of the statutorily-required disclosures necessary for him to render an informed decision that considered the risks of inputting his biometrics in Defendant's door-lock technology, including the risk that a data breach by Defendant involving biometric data may place his home at risk for unauthorized access. To the extent Defendant's system has suffered a data breach since Plaintiff's use of its system, Plaintiff's biometric information, and therefore "keys" to his physical location, are potentially in the possession of thieves or other criminals.

20. Prior to obtaining Plaintiff's biometrics, *i.e.* his fingerprint scans, not only did Defendant fail to obtain Plaintiff's informed written consent, but it also failed to publish or otherwise make available any policies concerning biometric collection, retention and destruction.

21. Additionally, Defendant did not obtain consent to transmit or disseminate Plaintiff's biometrics to third parties, including data storage and equipment vendors. Defendant has violated BIPA on each occasion it transmitted biometrics to third parties.

22. Indeed, each time Defendant, via its biometric door-lock, used Plaintiff's fingerprint in order to authenticate his identity, Defendant necessarily violated BIPA.

23. To this day, Plaintiff is unaware of the status of his biometric information that was obtained by Defendant. Defendant has not informed him whether it still retains his biometric information, and if it does, for how long it intends to retain such information with his consent.

24. By knowingly and willfully failing to comply with the BIPA's mandatory notice, release, third-party dissemination, and policy publication requirements, Defendant has violated substantive privacy rights protected under the BIPA, and as a result, Plaintiff and the other members of the Class have continuously been exposed to substantial and irreversible loss of privacy in addition to other pecuniary and non-pecuniary harms.

25. Plaintiff and the Class utilized Defendant's biometric door-lock technology with the understanding that any sensitive data provided to Defendant would be handled in compliance with state law and not disclosed without their consent. Indeed, they would not have utilized such biometric-facilitated technology had they known Defendant was not complying with state data privacy law.

CLASS ALLEGATIONS

26. Plaintiff brings this action on behalf of himself and similarly situated individuals pursuant to 735 ILCS § 5/2-801. Plaintiff seeks to represent a Class defined as follows:

> **The Class**: All persons in Illinois whose biometrics were captured, collected, obtained, stored or used by Defendant without lawful consent within the applicable limitations period.

27. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

28. Upon information and belief, there are hundreds, if not thousands, of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiff, the members can be ascertained through Defendant's records.

29. Plaintiff's claims are typical of the claims of the Class members they seek to represent because the factual and legal bases of Defendant's liability to Plaintiff and the other Class members are the same and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class. As alleged herein, Plaintiff and the other putative Class members have all suffered damages as a result of Defendant's BIPA violations.

30. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant collects, captures, stores, or uses the biometrics of Class members;

b. Whether Defendant developed and made available to the public a written policy which establishes a retention schedule and guidelines for permanently destroying biometric identifiers and information as required by BIPA;

c. Whether Defendant obtained a written release from Class members before capturing, collecting, or otherwise obtaining individual's biometrics;

d. Whether Defendant provided a written disclosure to individuals that explains the specific purposes, and the length of time, for which their biometrics were being collected, stored and used before taking their biometrics;

e. Whether Defendant's conduct violates BIPA;

f. Whether Defendant's violations of BIPA are willful and reckless; and

g. Whether Plaintiff and the Class members are entitled to damages and injunctive relief.

31. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

32. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

33. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I

Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (On behalf of Plaintiff and the Class)

34. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

35. BIPA requires private entities, such as Defendant, to obtain informed written consent from individuals before acquiring their biometric information. Specifically, BIPA makes it unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or 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 for which a biometric identifier or biometric information is being captured, 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).

36. BIPA also requires that private entities in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. Entities which possess biometric identifiers or information must (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information (entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) must adhere to the publicly posted retention and deletion schedule.

37. Defendant is a "private entity" as defined under the BIPA. *See* 740 ILCS 14/10.

38. Plaintiff and the other Class members have had their "biometric identifiers," namely their fingerprints, collected, captured, received or otherwise obtained by Defendant. Plaintiff's and the other Class members' biometric identifiers were also used to identify them, and therefore constitute "biometric information" as defined by the BIPA. 740 ILCS 14/10.

39. Additionally, beyond Defendant's immediate collection of Plaintiff's and Class members' fingerprints, every instance that Defendant required Plaintiff and the other Class members to verify their identity and account by matching their fingerprints with their respective

stored fingerprints, Defendant captured, collected, stored, and/or used Plaintiff's and the Class members' biometric identifiers or biometric information without valid consent and without complying with and, thus, in violation of the BIPA.

40. Defendant's practice with respect to capturing, collecting, storing, and using biometric identifiers and biometric information fails to comply with applicable BIPA requirements. Specifically, with respect to Plaintiff and the other Class members, Defendant failed to:

a. Obtain the written release required by 740 ILCS 14/15(b)(3);

b. Inform Plaintiff and the Class in writing of the specific purpose for which their biometric information and/or biometric identifiers were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

c. Inform Plaintiff and the Class in writing of the specific length of term their biometric information and/or biometric identifiers were being captured, collected, stored and used, as required by 740 ILCS 14/15(b)(2); and

d. Provide a publicly available retention schedule detailing the length of time biometric information is stored and guidelines for permanently destroying the biometric information it stores, as required by 740 ILCS 14/15(a).

41. By capturing, storing, and using Plaintiff's and the other Class members' biometric identifiers and/or biometric information as described herein, Defendant violated Plaintiff's and the other Class members' respective rights to privacy as set forth in the BIPA. 740 ILCS 14/15(a).

42. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of the BIPA and, alternatively, damages of $1,000 for each negligent violation of the BIPA. 740 ILCS 14/20(1).

43. Defendant's violations of the BIPA, as set forth herein, were knowing and willful, or were in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with the BIPA disclosure, consent, and policy posting requirements.

COUNT II
Negligence
(On behalf of Plaintiff and the Class)

44. Plaintiff hereby incorporates the foregoing allegations as if fully set forth herein.

45. To the extent that a finder of fact concludes that Defendant did not intentionally withhold information from Plaintiff and the Class relating to its biometric system, Defendant was nonetheless careless and negligent in its failure to act reasonably in the circumstances.

46. Special relationships existed between Plaintiff and the Class and Defendant which gave rise to various duties and obligations concerning the biometric data at issue because Defendant had full control over all information regarding its biometric door-lock technology, including any policies related thereto, relative to Plaintiff's limited knowledge and power.

47. Further, BIPA establishes and defines a reasonable duty of care for private entities, such as Defendant, who collect, obtain, transact, transmit, store, or otherwise use biometrics.

48. Defendant knew, or should have known, of the irreversible risks inherent in collecting, storing, using, and disseminating the biometrics of its customers, particularly when such biometrics are tied to address, key templates, and other sensitive information.

49. Defendant breached its duties to Plaintiff and the Class with regards to biometric privacy by, among other things, failing to implement a BIPA-compliant biometric system with reasonable data security policies.

50. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered pecuniary and non-pecuniary injury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, respectfully requests that this Court enter an Order:

a. Certifying the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;

b. Declaring that Defendant's actions, as set forth herein, violate the BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with the BIPA requirements for the capture, collection, storage, and use of biometric identifiers and biometric information, including an injunction requiring Defendant to permanently destroy all biometric information of Plaintiff and of Class members in their possession and compensation in an amount to be determined at trial for the commercial value of Plaintiff's biometric information;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);

e. Awarding statutory damages of $1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(3);

f. Awarding monetary damages and equitable relief for Defendant's fraudulent conduct and negligence in an amount to be determined at trial, as well as punitive damages for such fraudulent conduct;

g. Awarding reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);

h. Awarding pre- and post-judgment interest, as allowable by law; and

i. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiff request trial by jury of all claims that can be so tried.

Dated: September 20, 2018

Respectfully submitted,

MICHAEL KOMORSKI, individually and on behalf of a class of similarly situated individuals

By: /s/ Jad Sheikali
One of Plaintiff's Attorneys

Jad Sheikali
William P. Kingston
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
jsheikali@mcgpc.com
wkingston@mcgpc.com

Attorneys for Plaintiff and the Putative Class