

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

**LATRINA COTHRON, Individually and  
on behalf of similarly situated individuals,** )

**Plaintiff,** )

**v.** )

**WHITE CASTLE SYSTEM, INC. D/B/A  
WHITE CASTLE and CROSS MATCH  
TECHNOLOGIES, INC.,** )

**Defendants.** )

**Case No. 1:19-cv-00382**

**NOTICE OF REMOVAL OF CROSS MATCH TECHNOLOGIES, INC.**

Pursuant to 28 U.S.C. §§ 1332, 1441, 1446 and 1453, Defendant Cross Match Technologies, Inc. (“Crossmatch”), by its counsel, hereby gives notice of removal of this action from the Circuit Court of Cook County, Illinois to the United States District Court for the Northern District of Illinois.

**I. FACTUAL BACKGROUND**

1. On December 6, 2018, Plaintiff Latrina Cothron (“Plaintiff”) filed a Class Action Complaint (“Complaint”) in the Circuit Court of Cook County, Illinois, styled Cothron v. White Castle Food Products, LLC et al., Case No. 2018-CH-15233. The Complaint named Crossmatch as a defendant, and was served on Crossmatch on December 21, 2018. See disc. infra at 7. A copy of all process, pleadings, and orders served upon Crossmatch with respect to this action are attached hereto as Group Exhibit 1.

2. On January 8, 2019, Plaintiff filed an Amended Class Action Complaint (“Amended Complaint”) in the Circuit Court of Cook County, Illinois, styled Cothron v. White Castle System, Inc. et al., Case No. 2018-CH-15233. See Am. Compl., Ex. 1 hereto, at passim. Crossmatch was served with the Amended Complaint on January 14, 2019.

3. Plaintiff also filed a Motion for Class Certification and Request for Discovery on Class Certification Issues on December 12, 2018, which was amended on January 8, 2019 (“Am. Mot. for Class Certification”). See Am. Mot. for Class Certification, Ex. 2 hereto, at passim. As of January 18, 2019, Crossmatch has not been served with the original or amended Motion for Class Certification and Request for Discovery on Class Certification Issues. Counsel for Crossmatch pulled the amended motion after reviewing the case docket.

4. Plaintiff’s Amended Complaint alleges that Crossmatch and co-defendant White Castle System, Inc. (“White Castle”) (collectively, Crossmatch and White Castle are referred to herein as “Defendants”) have violated the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 (“BIPA”) by purportedly “disregard[ing] White Castle employees’ statutorily protected privacy rights and unlawfully collect[ing], stor[ing], disseminat[ing], and us[ing] employees’ biometric data in violation of BIPA,” among other things.<sup>1</sup> See Am. Compl., Ex. 1 hereto, at ¶ 11; see also, e.g., id. at ¶¶ 11-16, 42-43, 56-57.

5. Plaintiff’s claims against White Castle rest upon the same factual allegations; namely, that upon hiring, White Castle requires its employees to scan their fingerprints in order “to enroll them in its DigitalPersona employee database(s).” See Am. Compl., Ex. 1 hereto, at ¶ 42. Plaintiff further alleges that White Castle “uses and has used employee software supplied by Cross Match that requires employees to use their fingerprints as a means of authentication” and that per White Castle’s policy, “all White Castle employees are required to use their fingerprints to access their weekly paystubs.” See id. at ¶ 43. In addition, Plaintiff alleges that she was

---

<sup>1</sup> Pursuant to 28 U.S.C. § 1453(b), it is not necessary for all Defendants to join this Notice of Removal.

required to scan her fingerprint “each time she accessed a White Castle computer.” See id. at ¶ 56.

6. Based on these and other allegations, Plaintiff asserts claims for violation of the BIPA and negligence and seeks declaratory and injunctive relief as well as statutory damages and attorneys’ fees and costs. See Am. Compl., Ex. 1 hereto, at ¶¶ 83-114 & pp. 23-24. Plaintiff seeks to bring her claims against Crossmatch on behalf of a proposed class of “[a]ll individuals working for White Castle in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by any Defendant during the applicable statutory period.” Id. at ¶ 73.

## **II. REMOVAL IS PROPER PURSUANT TO THE CLASS ACTION FAIRNESS ACT**

7. Plaintiff’s claims are removable because the Class Action Fairness Act (“CAFA”) provides this Court with jurisdiction. See 28 U.S.C. §§ 1332(d), 1453. CAFA extends federal jurisdiction over class actions where: (1) any member of the proposed class is a citizen of a state different from any defendant (i.e., minimal diversity exists); (2) the proposed class consists of more than 100 members; and (3) the amount in controversy is \$5 million or more, aggregating all claims and exclusive of interests and costs. See 28 U.S.C. §§ 1332(d)(2), 1332(d)(5)(B).<sup>2</sup> As shown below, each of these requirements is met. See disc. infra at 3-6.

### **A. Minimal Diversity**

8. Minimal diversity is established under CAFA, because Plaintiff and one or more members of the proposed class are citizens of different states from Crossmatch. See 28 U.S.C. § 1332(d)(2)(A).

---

<sup>2</sup> A “class action” includes any civil action filed under Federal Rule of Civil Procedure 23, or “similar State statute or rule of judicial procedure,” such as 735 ILCS 5/2-801. See 28 U.S.C. § 1332(d)(1)(B); Am. Compl., Ex. 1 hereto, at ¶ 73.

9. According to the allegations in the Amended Complaint, Plaintiff is a citizen of Illinois and seeks to represent a class of individuals from Illinois and other states who worked “for White Castle in the State of Illinois [and] had their fingerprints collected, captured, received, or otherwise obtained or disclosed by any Defendant during the applicable statutory period.” See Am. Compl., Ex. 1 hereto, at ¶¶ 23, 73.

10. Crossmatch is incorporated under the laws of the State of Delaware and has its principal place of business in Palm Beach Gardens, Florida. See Am. Compl., Ex. 1 hereto, at ¶ 25; Florida Secretary of State Record, Ex. 3 hereto. A corporation such as Crossmatch “shall be deemed to be a citizen of every [s]tate . . . by which it has been incorporated and . . . where it has its principal place of business . . . .” 28 U.S.C. §1332(c)(1). Accordingly, Crossmatch is a citizen of the States of Delaware and Florida for purposes of diversity jurisdiction and is not a citizen of the State of Illinois. See id.

11. White Castle is incorporated under the laws of the State of Ohio and has its principal place of business in Columbus, Ohio. See Am. Compl., Ex. 1 hereto, at ¶ 24; Illinois Secretary of State Record, Ex. 4 hereto. Accordingly, White Castle is a citizen of the State of Ohio for the purposes of diversity jurisdiction and is not a citizen of the State of Illinois. See id.; see also 28 U.S.C. §1332(c)(1).

12. Minimal diversity therefore exists under 28 U.S.C. §1332(d)(2)(A). See, e.g., Marconi v. Indiana Municipal Power Agency, 2015 WL 4778528, at \*5 (N.D. Ill. 2015) (finding minimal diversity pursuant to CAFA where one plaintiff was a citizen of Illinois and four of the five defendants were alleged to be citizens of states other than Illinois).

#### **B. Number Of Class Members**

13. Plaintiff purports to bring this action on behalf of “[a]ll individuals working for White Castle in the State of Illinois who had their fingerprints collected, captured, received, or

otherwise obtained or disclosed by any Defendant during the applicable statutory period.” Am. Compl., Ex. 1 hereto, at ¶ 73. Plaintiff herself alleges that “[u]pon information and belief, White Castle employs hundreds of workers, many of whom are members of the class.” See Am. Mot. for Class Certification, Ex. 2 hereto, at 7 n.2.

14. Based on these allegations, the Court can properly infer that the proposed class consists of more than 100 members, satisfying the requirement in CAFA that the proposed class consist of more than 100 members. See 28 U.S.C. § 1332(d)(5)(B).

### **C. Amount In Controversy**

15. The amount in controversy exceeds \$5 million. See 28 U.S.C. § 1332(d)(2). For purposes of determining the amount in controversy, CAFA requires that “the claims of the individual class members shall be aggregated[.]” See 28 U.S.C. § 1332(d)(6). Although Plaintiff has not alleged the amount of damages, CAFA’s amount in controversy threshold is met here based on Plaintiff’s allegations and the undisputed facts. See disc. infra at 5-6.

16. As noted above, Plaintiff alleges that “[u]pon information and belief, White Castle employs hundreds of workers, many of whom are members of the class.” See Am. Mot. for Class Certification, Ex. 2 hereto, at 7 n.2. As to each of those “hundreds of workers,” Plaintiff alleges multiple violations of the BIPA by Defendants. See, e.g., Am. Compl. Ex. 1 hereto, at ¶ 11 (alleging that each Defendant “has violated and continues to violate BIPA”); id. at ¶ 61 (alleging that Plaintiff has “continuously and repeatedly been exposed to the risks and harmful conditions” created by Defendants’ alleged BIPA violations); id. at ¶ 100 (seeking statutory damages for each violation of the BIPA). Specifically, Plaintiff alleges that she and other members of the putative class had their fingerprints scanned upon hiring to enroll them in White Castle’s employee database, and that she and other members of the putative class must use their fingerprints to access paystubs and White Castle computers. See id. at ¶¶ 42-43, 56.

Plaintiff also claims that Crossmatch violated the BIPA by failing to provide a data retention policy and by failing to obtain consent from Plaintiff and the members of the proposed class for dissemination of biometrics. See id. at ¶¶ 45-46.

17. The BIPA provides statutory damages of \$1,000 for a negligent violation and \$5,000 for an intentional or reckless violation, with damages calculated “for each violation.” See 740 ILCS 14/20. Given that Plaintiff alleges: (a) Defendants purportedly violated the BIPA multiple times for Plaintiff and members of the proposed class; (b) each of those violations was reckless and subject to a \$5,000 statutory fine; and (c) there are “hundreds” of individuals in the proposed class, the amount in controversy in this case will easily exceed the threshold requirement. See, e.g., Appert v. Morgan Stanley, 673 F.3d 609, 617-18 (7th Cir. 2012) (“Morgan Stanley has provided a good-faith estimate that plausibly explains how the stakes exceed \$5 million. That is sufficient.”); Bloomberg v. Service Corp. Int’l., 639 F.3d 761, 764 (7th Cir. 2011) (“Once the proponent of federal jurisdiction has explained plausibly how the stakes exceed \$5,000,000 . . . the case belongs in federal court unless it is legally impossible for the plaintiff to recover that much.”). Spivey v. Vertrue, 528 F.3d 982, 986 (7th Cir. 2008) (noting that for removal purposes under CAFA, defendant need only show that the recovery at the \$5,000,000 jurisdictional threshold is not “legally impossible”).<sup>3</sup>

---

<sup>3</sup> Plaintiff also alleges that she has suffered “monetary damages for the value of the collection and retention of her biometric data [and] by not obtaining additional compensation as a result of being denied access to material information about Defendants’ policies and procedures,” as well as “mental anguish,” indicating that she intends to seek damages beyond the statutory damages and further demonstrating that the amount in controversy is readily met. See Am. Compl. Ex. 1 hereto, at ¶¶ 68-69; see also Appert, 673 F.3d at 617-18.

### **III. COMPLIANCE WITH REMOVAL STATUTE**

18. The Notice of Removal was properly filed in the United States District Court for the Northern District of Illinois, because the Circuit Court of Cook County, Illinois is located in this federal judicial district. See 28 U.S.C. § 1441(a); 28 U.S.C. § 93(a)(1).

19. The Notice of Removal is signed pursuant to Rule 11 of the Federal Rules of Civil Procedure. See 28 U.S.C. § 1446(a).

20. The Complaint was served on Crossmatch on or about December 21, 2018. See Aff. of Service, Ex. 1 hereto. Accordingly, this Notice of Removal is timely under 28 U.S.C. § 1446(b), as it is filed within 30 days of service of the initial pleading.

21. Pursuant to 28 U.S.C. § 1446(a), a copy of all process, pleadings, and orders served upon Crossmatch with respect to this action are attached hereto as Group Exhibit 1.

22. Pursuant to 28 U.S.C. § 1446(d), a copy of this Notice of Removal is being served on counsel for Plaintiff and White Castle, and a copy, along with a Notice of Filing of the Notice of Removal, is being filed with the Clerk of the Circuit Court of Cook County, Illinois today.

### **IV. CONCLUSION**

21. Crossmatch respectfully requests that this Court exercise jurisdiction over this action and enter orders and grant relief as may be necessary to secure removal and to prevent further proceedings in this matter in the Circuit Court of Cook County, Illinois. Crossmatch further requests whatever other relief the Court deems appropriate.

Dated: January 18, 2019

Respectfully submitted,

/s/ Kathleen P. Lally

One of the Attorneys for Defendant  
Cross Match Technologies, Inc.

Mark S. Mester, Bar No. 6196140  
Kathleen P. Lally, Bar No. 6284954  
Peter A. Shaeffer, Bar No. 6313953  
LATHAM & WATKINS LLP  
330 North Wabash Avenue, Suite 2800  
Chicago, Illinois 60611  
Telephone: (312) 876-7700  
Facsimile: (312) 993-9767



**CERTIFICATE OF SERVICE**

I, Kathleen P. Lally, hereby certify that I caused a copy of the foregoing NOTICE OF REMOVAL OF CROSS MATCH TECHNOLOGIES, INC. to be served on the parties listed below, by email and U.S. mail, on January 18, 2019.

Ryan F. Stephen  
Andrew C. Ficzk  
STEPHAN ZOURAS, LLP  
100 North Riverside Plaza  
Suite 2150  
Chicago, IL 60606  
Tel: (312) 233-1550  
Fax: (312) 233-1560  
aficzko@stephanzouras.com

Counsel for Plaintiff and the Putative Class

Melissa A. Siebert  
BAKER & HOSTETLER LLP  
191 N. Wacker Drive  
Suite 3100  
Chicago, IL 60606  
Tel: (312) 416-6200  
msiebert@bakerlaw.com

Counsel for Defendant White Castle  
System, Inc.

/s/ Kathleen P. Lally  
One of the Attorneys for Defendant  
Cross Match Technologies, Inc.

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

**LATRINA COTHRON, Individually and  
on behalf of similarly situated individuals,** )

**Plaintiff,** )

**v.** )

**WHITE CASTLE SYSTEM, INC. D/B/A  
WHITE CASTLE and CROSS MATCH  
TECHNOLOGIES, INC.,** )

**Defendants.** )

**Case No. 1:19-cv-00382**

**INDEX OF EXHIBITS**

<b>Exhibit</b>	<b>Description</b>
1.	Group Exhibit containing the following documents: <ul style="list-style-type: none"> <li>• Class Action Complaint (December 6, 2018)</li> <li>• Affidavit of Service to Cross Match Technologies, Inc. (January 3, 2019)</li> <li>• Amended Class Action Complaint (January 8, 2019)</li> </ul>
2.	Plaintiff's Amended Motion for Class Certification and Request for Discovery on Certification Issues (January 8, 2019)
3.	Florida Secretary of State Record
4.	Illinois Secretary of State Record

# **GROUP EXHIBIT 1**

**12-Person Jury**

FILED  
12/6/2018 5:07 PM  
DOROTHY BROWN  
CIRCUIT CLERK  
COOK COUNTY, IL  
2018CH15233

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

<b>LATRINA COTHRON, individually,</b>	)	
<b>and on behalf of all others similarly situated,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	<b>Case No. 2018CH15233</b>
<b>v.</b>	)	
	)	
<b>WHITE CASTLE FOOD PRODUCTS, LLC</b>	)	<b>JURY TRIAL DEMANDED</b>
<b>D/B/A WHITE CASTLE, and CROSS MATCH</b>	)	
<b>TECHNOLOGIES, INC.,</b>	)	
	)	
<b>Defendant.</b>	)	

**CLASS ACTION COMPLAINT**

Plaintiff Latrina Cothron (“Cothron” or “Plaintiff”), by and through her attorneys, individually and on behalf of all others similarly situated (the “Class”), brings the following Class Action Complaint (“Complaint”) pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against White Castle Food Products, LLC and Cross Match Technologies, Inc., (Collectively “Defendants”), their subsidiaries and affiliates, to redress and curtail Defendants’ unlawful collection, use, storage, and disclosure of Plaintiff’s sensitive biometric data. Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

**NATURE OF THE ACTION**

1. Defendant White Castle Food Products, LLC (“White Castle”) is a food retailer that processes and distributes fast food products in retail stores and restaurants nationally.

2. Defendant Cross Match Technologies, INC. (“Crossmatch”) is a technology company that provides software and hardware that tracks and monitors employees’ biometric data to companies worldwide.

3. When White Castle hires an employee, he or she is enrolled in its DigitalPersona employee database using a scan of his or her fingerprint. White Castle uses the DigitalPersona employee database to distribute their employees’ paystubs on a weekly basis.

4. While many employers use conventional methods for payroll (direct deposit or paper check), White Castle’s employees are required to have their fingerprints scanned by a biometric device to retrieve their paystubs.

5. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as Defendants – and financial institutions have incorporated biometric applications into their workplace in the form of biometric authenticators, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

6. Unlike ID badges– which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes White Castle’s employees to serious and irreversible privacy risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses – employees have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

7. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), available at <https://www.opm.gov/cybersecurity/cybersecurity-incidents>.

8. An illegal market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. See Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), available at [https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm\\_term=.b3c70259f138](https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138).

9. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than \$8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), available at <http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>.

10. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1, *et seq.*, specifically to regulate companies that collect, store and use Illinois citizens’ biometrics, such as fingerprints.

11. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregard White Castle employees’ statutorily protected privacy rights and unlawfully collect, store, disseminate, and use employees’ biometric data in violation of BIPA. Specifically, each Defendant has violated and continues to violate BIPA because they did not and continue not to:

FILED DATE: 12/6/2018 5:07 PM 2018CH15233

- a. Properly inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, disseminated and used, as required by BIPA;
- b. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA; and,
- c. Receive a written release from Plaintiff and others similarly situated to collect, store, disseminate or otherwise use their fingerprints, as required by BIPA.

12. Plaintiff and other similarly-situated individuals are aggrieved because they were not: (1) informed in writing of the purpose and length of time for which their fingerprints were being collected, stored, disseminated and used; (2) provided a publicly available retention schedule or guidelines for permanent destruction of the biometric data; and (3) provided (nor did they execute) a written release, as required by BIPA.

13. Upon information and belief, Defendant White Castle improperly discloses its employees' fingerprint data to at least one third-party, DigitalPersona, and likely others.

14. Upon information and belief, Defendants White Castle and Crossmatch improperly disclose White Castle employees' fingerprint data to other, currently unknown, third parties, including, but not limited to third parties that host biometric data in their data center(s).

15. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have not and will not destroy their biometric data as required by BIPA.

16. Plaintiff and others similarly situated are aggrieved by each Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interactions with the company.

17. Plaintiff and others similarly situated have suffered an injury in fact based on each Defendant's improper disclosures of their biometric data to third parties.

18. Plaintiff and others similarly situated have suffered an injury in fact based on each Defendant's violations of their legal rights.

19. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties. The Illinois Attorney General has just ranked identity theft as the top scam targeting Illinois residents. (*See, e.g.,* Exhibit A).

20. Employees have a proprietary right to control their biometric information. In failing to comply with the requirements of BIPA, employers intentionally interfere with each employee's right of possession and control over their valuable, unique, and permanent biometric data.

21. Each Defendant is directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

22. Accordingly, Plaintiff, on behalf of himself as well as the putative Class, seeks an Order: (1) declaring that each Defendant's conduct violates BIPA; (2) requiring each Defendant to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

#### **PARTIES**

23. Plaintiff Latrina Cothron is a natural person and a citizen in the State of Illinois.

24. Defendant White Castle is an Ohio corporation that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.



25. Defendant Crossmatch is a corporation existing under the laws of the State of Illinois, that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

### **JURISDICTION AND VENUE**

26. This Court has jurisdiction over Defendants pursuant to 735 ILCS 5/2-209 because they conduct business transactions in Illinois, committed statutory violations and tortious acts in Illinois, and are registered to conduct business in Illinois.

27. Venue is proper in Cook County because Defendants are authorized to conduct business in this State, Defendants conduct business transactions in Cook County, and Defendants committed the statutory violations alleged herein in Cook County and throughout Illinois.

### **FACTUAL BACKGROUND**

#### **I. The Biometric Information Privacy Act.**

28. Major national corporations started using Chicago and other locations in Illinois in the early 2000s to test “new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias” 740 ILCS 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS 14/5.

29. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. The bankruptcy was alarming to the Illinois legislature because there was suddenly a serious risk that millions of fingerprint records – which, similar to other unique biometric identifiers, can be linked to people’s sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate

protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware the scanners were not transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

30. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

31. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover \$1,000 or actual damages, whichever is greater, for negligent violations and \$5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

32. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

- a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used;
- b. 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
- c. Receives a written release executed by the subject of the biometric identifier or biometric information."

*See* 740 ILCS 14/15(b).

33. BIPA specifically applies to employees who work in the State of Illinois. BIPA defines a “written release” specifically “in the context of employment [as] a release executed by an employee as a condition of employment.” 740 ILCS 14/10.

34. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and – most importantly here – fingerprints. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an individual’s biometric identifier that is used to identify an individual. *Id.*

35. BIPA also establishes standards for how companies must handle Illinois citizens’ biometric identifiers and biometric information. *See, e.g.,* 740 ILCS 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person’s or customer’s biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

36. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person’s biometric identifiers or biometric information (740 ILCS 14/15(c)) and requires companies to develop and comply with 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 such identifiers or information has been satisfied or within three years of the individual’s last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

37. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public’s hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are

FILED DATE: 12/6/2018 5:07 PM 2018CH15233

biologically unique to the individual and, once compromised, an individual is at heightened risk for identity theft and left without any recourse.

38. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

39. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

## **II. Defendants Violate the Biometric Information Privacy Act.**

40. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using employees' biometric data as an authentication method stopped doing so.

41. However, Defendants failed to take note of the shift in Illinois law governing the collection and use of biometric data. As a result, each Defendant continues to collect, store, use, and disseminate White Castle employees' biometric data in violation of BIPA.

42. Specifically, when employees are hired by White Castle, they are required to have their fingerprints scanned to enroll them in its DigitalPersona employee database(s).

43. White Castle uses and has used employee software supplied by Crossmatch that requires employees to use their fingerprint as a means of authentication. Per the company's policy, all White Castle employees were required to use their fingerprints to access their weekly paystubs.

44. Upon information and belief, White Castle failed and continues to fail to inform its employees that it discloses or disclosed their fingerprint data to at least one third party: DigitalPersona, and likely others; fails to inform its employees that it discloses their fingerprint data to other, currently unknown, third parties, which host the biometric data in their data centers; fails to inform its employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from employees before collecting their fingerprints.

45. Upon information and belief, White Castle fails to inform their employees that it discloses their fingerprint data to other, currently unknown, third parties, which host the biometric data in their data centers; fails to inform White Castle employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from White Castle employees before collecting their fingerprints.

46. Furthermore, each Defendant fails to provide employees with a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by BIPA.

47. The Pay by Touch bankruptcy, which triggered the passage of BIPA, highlights why such conduct – where individuals are aware that they are providing a fingerprint but are not aware to whom or for what purposes they are doing so – is dangerous. This bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers such as a fingerprint, who exactly is collecting their biometric data, where it will be transmitted, for what purposes it will be transmitted, and for how long. Each Defendant disregards these obligations and White Castle employees' statutory rights and instead



unlawfully collect, store, use, and disseminate employees' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

48. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have not and will not destroy Plaintiff's and other similarly-situated individuals' biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with each company.

49. White Castle employees are not told what might happen to their biometric data if and when any Defendant merges with another company or worse, if and when any Defendant's business folds, or when the other third parties that have received their biometric data businesses fold.

50. Since Defendants neither publish BIPA-mandated data retention policies nor disclose the purposes for their collection of biometric data, White Castle employees have no idea whether any Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated individuals are not told to whom any Defendant currently discloses their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.

51. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

52. By and through the actions detailed above, Defendants disregarded Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

FILED DATE: 12/6/2018 5:07 PM 2018CH15233

### **III. Plaintiff Latrina Cothron's Experience**

53. Plaintiff Latrina Cothron was hired by White Castle in 2004 and is currently working as a manager.

54. As a condition of employment, Cothron was required to scan her fingerprints so White Castle could use it as an authentication method for Plaintiff to access the computer as a manager and to access to her paystubs as an hourly employee.

55. White Castle subsequently stored Cothron's fingerprint data in its DigitalPersona employee database(s).

56. Cothron was required to scan her fingerprint each time she accessed a White Castle computer.

57. Cothron was also required to scan her fingerprint each time she accessed her paystub.

58. Cothron has never been informed of the specific limited purposes or length of time for which any Defendant collected, stored, used, and/or disseminated her biometric data.

59. Cothron has never been informed of any biometric data retention policy developed by any Defendant, nor has she ever been informed whether any Defendant will ever permanently delete her biometric data.

60. Cothron has never been provided with nor ever signed a written release allowing any Defendant to collect, store, use or disseminate her biometric data.

61. Cothron has continuously and repeatedly been exposed to the risks and harmful conditions created by each Defendant's violations of BIPA alleged herein.

62. No amount of time or money can compensate Cothron if her biometric data is compromised by the lax procedures through which each Defendant captured, stored, used, and

disseminated her and other similarly-situated individuals' biometrics. Moreover, Cothron would not have provided her biometric data to any Defendant if she had known that they would retain such information for an indefinite period of time without her consent.

63. A showing of actual damages is not necessary in order to state a claim under BIPA. Nonetheless, Cothron has been aggrieved because she suffered an injury-in-fact based on each Defendant's violations of her legal rights. Defendants intentionally interfered with Cothron's right to possess and control her own sensitive biometric data. Additionally, Cothron suffered an invasion of a legally protected interest when each Defendant secured her personal and private biometric data at a time when it had no right to do so, a gross invasion of her right to privacy. BIPA protects employees like Cothron from this precise conduct. Defendants had no lawful right to secure this data or share it with third parties absent a specific legislative license to do so.

64. Cothron's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow. As such, Cothron was not sufficiently compensated by any Defendant for its retention and use of her and other similarly-situated employees' biometric data. Cothron would not have agreed to work for White Castle for the compensation she received if she had known that Defendants would retain her biometric data indefinitely.

65. Cothron also suffered an informational injury because each Defendant failed to provide her with information to which she was entitled by statute. Through BIPA, the Illinois legislature has created a right: an employee's right to receive certain information prior to an employer securing their highly personal, private and proprietary biometric data; and an injury – not receiving this extremely critical information.



66. Cothron also suffered an injury in fact because each Defendant improperly disseminated her biometric identifiers and/or biometric information to third parties, including but not limited to DigitalPersona, and any other third party that hosted the biometric data in their data centers, in violation of BIPA.

67. Pursuant to 740 ILCS 14/15(b), Cothron was entitled to receive certain information prior to Defendants securing her biometric data; namely, information advising her of the specific limited purpose(s) and length of time for which each Defendant to collect, store, use and disseminate her private biometric data; information regarding each Defendant's biometric retention policy; and, a written release allowing each Defendant to collect, store, use, and disseminate her private biometric data. By depriving Cothron of this information, Defendants injured her. *Public Citizen v. U.S. Department of Justice*, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Akins*, 524 U.S. 11 (1998).

68. Finally, as a result of each Defendant's conduct, Cothron has experienced personal injury in the form of mental anguish. For example, Cothron experiences mental anguish and injury when contemplating what would happen to her biometric data if any Defendant went bankrupt, whether any Defendant will ever delete her biometric information, and whether (and to whom) any Defendant would share her biometric information.

69. Cothron has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of her biometric data; in the form of monetary damages by not obtaining additional compensation as a result of being denied access to material information about Defendants' policies and practices; in the form of the unauthorized disclosure of her confidential biometric data to third parties; in the form of interference with her right to

control and possess her confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

70. As Cothron is not required to allege or prove actual damages in order to state a claim under BIPA, she seeks statutory damages under BIPA as compensation for the injuries caused by Defendants.

### CLASS ALLEGATIONS

71. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS 5/2-801, Plaintiff brings claims on her own behalf and as a representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS 14/1, *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

72. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it first (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose and length of time 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.

73. Plaintiff seeks class certification under the Illinois Code of Civil Procedure, 735 ILCS 5/2-801 for the following class of similarly-situated employees under BIPA:

All individuals working for White Castle in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by any Defendant during the applicable statutory period.

74. This action is properly maintained as a class action under 735 ILCS 5/2-801

because:

- A. The class is so numerous that joinder of all members is impracticable;
- B. There are questions of law or fact that are common to the class;
- C. The claims of the Plaintiff are typical of the claims of the class; and,
- D. The Plaintiff will fairly and adequately protect the interests of the class.

**Numerosity**

75. The total number of putative class members exceeds fifty (50) individuals. The exact number of class members can easily be determined from White Castle's payroll records.

**Commonality**

76. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendants' failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

- A. Whether any Defendant collected, captured or otherwise obtained Plaintiff's biometric identifiers or biometric information;
- B. Whether any Defendant properly informed Plaintiff of their purposes for collecting, using, and storing her biometric identifiers or biometric information;
- C. Whether any Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff's biometric identifiers or biometric information;
- D. Whether any Defendant has disclosed or re-disclosed Plaintiff's biometric identifiers or biometric information;
- E. Whether any Defendant has sold, leased, traded, or otherwise profited from Plaintiff's biometric identifiers or biometric information;
- F. Whether any Defendant developed 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 three years of their last interaction with the individual, whichever occurs first;

- G. Whether any Defendant complies with any such written policy (if one exists);
- H. Whether any Defendant used Plaintiff's fingerprints to identify her;
- I. Whether any Defendant's violations of BIPA have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties;
- J. Whether the violations of BIPA were committed negligently; and
- K. Whether the violations of BIPA were committed willfully.

77. Plaintiff anticipates that Defendants will raise defenses that are common to the class.

#### **Adequacy**

78. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

#### **Typicality**

79. The claims asserted by Plaintiff are typical of the class members she seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

80. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, he or she can "opt out" of this action pursuant to 735 ILCS 5/2-801.

### **Predominance and Superiority**

81. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

82. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendants and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

### **FIRST CAUSE OF ACTION Violation of 740 ILCS 14/1, *et seq.* (On Behalf of Plaintiff and the Class)**

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

84. BIPA requires companies to obtain informed written consent from employees 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).

85. BIPA also prohibits private entities from disclosing a person’s or customer’s biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

86. Furthermore, BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company’s last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

87. Each Defendant fails to comply with these BIPA mandates.

88. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

89. Defendant Crossmatch is a corporation registered to do business in Illinois and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

90. Plaintiff is an individual who had her “biometric identifiers” collected by each Defendant (in the form of her fingerprints), as explained in detail in Sections II and III, *supra*. See 740 ILCS 14/10.

91. Plaintiff’s biometric identifiers were used to identify her and, therefore, constitute “biometric information” as defined by BIPA. See 740 ILCS 14/10.

92. Each Defendant systematically and automatically collected, used, stored, and disclosed Plaintiff’s biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

93. Upon information and belief, White Castle systematically disclosed Plaintiff’s biometric identifiers and biometric information to at least one third party, DigitalPersona.

94. Upon information and belief, each Defendant systematically disclosed Plaintiff’s biometric identifiers and biometric information to other, currently unknown, third parties, which hosted the biometric data in their data centers.

95. No Defendant informed Plaintiff in writing that her biometric identifiers and/or biometric information were being collected, stored, used, and disseminated, nor did any Defendant inform Plaintiff in writing of the specific purpose and length of term for which her biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

96. No Defendant provides a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. See 740 ILCS 14/15(a).

97. By collecting, storing, and using Plaintiff’s and the Class’s biometric identifiers and biometric information as described herein, each Defendant violated Plaintiff’s and the Class’s

rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

98. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and have not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

99. These violations have raised a material risk that Plaintiff's and the Class's biometric data will be unlawfully accessed by third parties.

100. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of \$5,000 for each willful 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).

**SECOND CAUSE OF ACTION**  
**Negligence**  
**(On Behalf of Plaintiff and the Class)**

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

102. Each Defendant owed Plaintiff and the Class a duty of reasonable care. Such duty required Defendants to exercise reasonable care in the collection and use of Plaintiff's and the Class's biometric data.



FILED DATE: 12/6/2018 5:07 PM 2018CH15233

103. Additionally, White Castle owed Plaintiff and the Class a heightened duty – under which it assumed a duty to act carefully and not put Plaintiff and the Class at undue risk of harm – because of the employment relationship of the parties.

104. Each Defendant breached its duties by failing to implement a BIPA-compliant biometric authentication system with reasonable data security safeguards.

105. Specifically, each Defendant breached its duties by failing to properly inform Plaintiff and the Class in writing of the specific purpose or length of time for which their fingerprints were being collected, stored, used, and disseminated.

106. Defendants also breached their duties by failing to provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and the Class's fingerprint data.

107. Upon information and belief, each Defendant breached its duties because it lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and have not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with either company.

108. Upon information and belief, White Castle breached its duties because it systematically disclosed Plaintiff's biometric identifiers and biometric information to at least one third party: DigitalPersona.

109. Upon information and belief, each Defendant breached its duties because it systematically disclosed Plaintiff's biometric identifiers and biometric information to other, currently unknown, third parties, which hosted the biometric data in their data centers.

110. These violations have raised a material risk that Plaintiff's and the Class's biometric data will be unlawfully accessed by third parties.

111. As a direct and proximate cause of each Defendant's negligent misrepresentations, Plaintiff and the other Class members have suffered from diminution in the unique identifying value of their biometric information caused by Defendants' repeated dissemination and exposure of such information to third-parties, including DigitalPersona, and data storage vendors, among others.

112. Defendants knew or should have known that their breaches would cause Plaintiff and the other Class members to experience the foreseeable harms associated with the exposure of their biometrics to third parties, including the discontinuation of Plaintiff's and the Class member's exclusive possession and control of their biometrics and the accompanying loss of the unique identifying value of their biometrics.

113. Further, each Defendant's breach of its duty proximately caused and continues to cause an invasion of Plaintiff's and the Class's privacy, an informational injury, and mental anguish, in addition to the statutory damage provided in BIPA.

114. Accordingly, Plaintiff seeks an order declaring that Defendants' conduct constitutes negligence and awarding Plaintiff and the Class damages in an amount to be calculated at trial.

#### **PRAYER FOR RELIEF**

Wherefore, Plaintiff Latrina Cothron respectfully requests that this Court enter an Order:

- A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Latrina Cothron as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;
- B. Declaring that Defendants' actions, as set forth above, violate BIPA;
- C. Awarding statutory damages of \$5,000 for each willful and/or reckless violation of

BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of \$1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

- D. Declaring that Defendants' actions, as set forth above, constitute negligence;
- E. Declaring that Defendants' actions, as set forth above, were willful;
- F. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendants to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;
- G. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);
- H. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,
- I. Provide such further relief as the Court deems just and equitable.

#### **JURY TRIAL**

Plaintiff demands a trial by jury for all issues so triable.

Date: December 6, 2018

Respectfully Submitted,

/s/ Andrew C. Ficzko

Ryan F. Stephan

Andrew C. Ficzko

**STEPHAN ZOURAS, LLP**

100 N. Riverside Plaza

Suite 2150

Chicago, Illinois 60606

312.233.1550

312.233.1560 f

Firm ID: 43734

Aficzko@stephanzouras.com

Filed: 01/18/2019 3:13 PM  
 Hearing: No  
 Courtroom: No  
 Location: No hearing scheduled

# SHERIFF'S OFFICE

RIC L. BRADSHAW, SHERIFF



2018CH15233  
 2018CH15233  
 JORDEN BROWN  
 CIRCUIT CLERK  
 COOK COUNTY, IL  
 2018CH15233

County: COOK

Court: CIRCUIT

State of: ILLINOIS

## AFFIDAVIT OF SERVICES

LATRINA COTHORN

Plaintiff

WHITE CASTLE FOOD PRODUCTS LLC AND CROSS MATCH TECHNOLOGIES  
 INC

Defendant

STATE OF FLORIDA  
 COUNTY OF PALM BEACH  
 CITY OF WEST PALM BEACH

Eric Stull, of the Sheriff's Office Palm Beach County, being duly sworn, deposes and says that he/she is not a party to this action and he/she is over eighteen years of age; that he/she is a resident elector of the County of Palm Beach County, State of Florida;

That on 12/21/2018 at 12:12 PM deponent served the following:  
 SUMMONS & COPY & COPY OF CLASS ACTION COMPLAINT

On CROSS MATCH TECHNOLOGIES INC defendant therein named.

Substitute Served  
 3950 RCA BOULEVARD SUITE 5001 PALM BEACH GARDENS, FL 33410

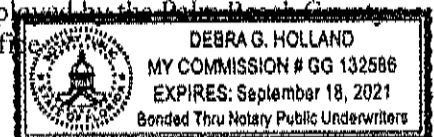
RIC L. BRADSHAW, SHERIFF  
PALM BEACH COUNTY, FLORIDA

Eric Stull 9172

Sworn to before me this 3rd  
 day of January, A.D. 2019 at  
 West Palm Beach, Florida

*Debra G. Holland*

This notary and the sworn Deputy Sheriff  
 are both employed by the Palm Beach County  
 Sheriff's Office



Return Date: No return date scheduled  
Hearing Date: No hearing scheduled  
Courtroom Number: No hearing scheduled  
Location: No hearing scheduled

FILED  
1/8/2019 2:16 PM  
DOROTHY BROWN  
CIRCUIT CLERK  
COOK COUNTY, IL  
2018CH15233

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

**LATRINA COTHRON, individually,** )  
**and on behalf of all others similarly situated,** )

**Plaintiff,** )

**v.** )

**WHITE CASTLE SYSTEM, INC. D/B/A** )  
**WHITE CASTLE and CROSS MATCH** )  
**TECHNOLOGIES, INC.,** )

**Defendants.** )

**Case No. 18-CH-15233**

**JURY TRIAL DEMANDED**

**AMENDED CLASS ACTION COMPLAINT**

Plaintiff Latrina Cothron ("Cothron" or "Plaintiff"), by and through her attorneys, individually and on behalf of all others similarly situated (the "Class"), brings the following Amended Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against White Castle System, Inc. d/b/a White Castle and Cross Match Technologies, Inc., (collectively "Defendants"), their subsidiaries and affiliates, to redress and curtail Defendants' unlawful collection, use, storage, and disclosure of Plaintiff's sensitive biometric data. Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

**NATURE OF THE ACTION**

1. Defendant White Castle System, Inc. ("White Castle") is an Ohio corporation that owns and operates hundreds of White Castle fast-food restaurants throughout the country, including Illinois.

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

2. Defendant Cross Match Technologies, Inc. (“Cross Match”) is a technology company that provides software and hardware that tracks and monitors employees’ biometric data to companies worldwide.

3. When White Castle hires an employee, he or she is enrolled in its DigitalPersona employee database using a scan of his or her fingerprint. White Castle uses the DigitalPersona employee database to distribute its employees’ paystubs on a weekly basis.

4. While many employers use conventional methods for payroll (direct deposit or paper check), White Castle’s employees are required to have their fingerprints scanned by a biometric device to retrieve their paystubs.

5. Biometrics are not relegated to esoteric corners of commerce. Many businesses — such as Defendants — and financial institutions have incorporated biometric applications into their workplace in the form of biometric authenticators, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

6. Unlike ID badges— which can be changed or replaced if stolen or compromised — fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes White Castle’s employees to serious and irreversible privacy risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed — like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses — employees have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.



FILED DATE: 1/8/2019 2:16 PM 2018CH15233

7. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), available at <https://www.opm.gov/cybersecurity/cybersecurity-incidents>.

8. An illegal market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. See Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), available at [https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm\\_term=.b3c70259f138](https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138).

9. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than \$8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), available at <http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>.

10. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1, *et seq.*, specifically to regulate companies that collect, store and use Illinois citizens’ biometrics, such as fingerprints.

11. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregard White Castle employees’ statutorily protected privacy rights and unlawfully collect, store, disseminate, and use employees’ biometric data in violation of BIPA. Specifically, each Defendant has violated and continues to violate BIPA because they did not and continue not to:

- a. Properly inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, disseminated and used, as required by BIPA;
- b. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA; and,
- c. Receive a written release from Plaintiff and others similarly situated to collect, store, disseminate or otherwise use their fingerprints, as required by BIPA.

12. Plaintiff and other similarly-situated individuals are aggrieved because they were not: (1) informed in writing of the purpose and length of time for which their fingerprints were being collected, stored, disseminated and used; (2) provided a publicly available retention schedule or guidelines for permanent destruction of the biometric data; and (3) provided (nor did they execute) a written release, as required by BIPA.

13. Upon information and belief, Defendant White Castle improperly discloses its employees' fingerprint data to at least one third-party, Cross Match, and likely others.

14. Upon information and belief, Defendants White Castle and Cross Match improperly disclose White Castle employees' fingerprint data to other, currently unknown, third parties, including, but not limited to third parties that host biometric data in their data center(s).

15. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have not and will not destroy their biometric data as required by BIPA.

16. Plaintiff and others similarly situated are aggrieved by each Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interactions with the company.



FILED DATE: 1/18/2019 2:16 PM 2018CH15233

17. Plaintiff and others similarly situated have suffered an injury in fact based on each Defendant's improper disclosures of their biometric data to third parties.

18. Plaintiff and others similarly situated have suffered an injury in fact based on each Defendant's violations of their legal rights.

19. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties. The Illinois Attorney General has just ranked identity theft as the top scam targeting Illinois residents. (*See, e.g.,* Exhibit A).

20. Employees have a proprietary right to control their biometric information. In failing to comply with the requirements of BIPA, employers intentionally interfere with each employee's right of possession and control over their valuable, unique, and permanent biometric data.

21. Each Defendant is directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

22. Accordingly, Plaintiff, on behalf of herself as well as the putative Class, seeks an Order: (1) declaring that each Defendant's conduct violates BIPA; (2) requiring each Defendant to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

#### **PARTIES**

23. Plaintiff Latrina Cothron is a natural person and a citizen in the State of Illinois.

24. Defendant White Castle is an Ohio corporation that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

25. Defendant Cross Match is a Delaware corporation with its headquarters located in Palm Beach Gardens, Florida. Cross Match conducts business in the State of Illinois, including Cook County, and throughout the United States.

#### **JURISDICTION AND VENUE**

26. This Court has jurisdiction over Defendants pursuant to 735 ILCS 5/2-209 because they conduct business transactions in Illinois, committed statutory violations and tortious acts in Illinois, and are registered to conduct business in Illinois.

27. Venue is proper in Cook County because Defendants conduct business transactions in Cook County and Defendants committed the statutory violations alleged herein in Cook County and throughout Illinois.

#### **FACTUAL BACKGROUND**

##### **I. The Biometric Information Privacy Act.**

28. Major national corporations started using Chicago and other locations in Illinois in the early 2000s to test “new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias” 740 ILCS 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS 14/5.

29. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. The bankruptcy was alarming to the Illinois legislature because there was suddenly a serious risk that millions of fingerprint records – which, similar to other unique biometric identifiers, can be linked to people’s sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate

FILED DATE: 1/18/2019 2:16 PM 2018CH15233

protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware the scanners were not transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

30. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS 14/5.

31. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover \$1,000 or actual damages, whichever is greater, for negligent violations and \$5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

32. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

- a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used;
- b. 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
- c. Receives a written release executed by the subject of the biometric identifier or biometric information."

*See* 740 ILCS 14/15(b).

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

33. BIPA specifically applies to employees who work in the State of Illinois. BIPA defines a “written release” specifically “in the context of employment [as] a release executed by an employee as a condition of employment.” 740 ILCS 14/10.

34. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and – most importantly here – fingerprints. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an individual’s biometric identifier that is used to identify an individual. *Id.*

35. BIPA also establishes standards for how companies must handle Illinois citizens’ biometric identifiers and biometric information. *See, e.g.,* 740 ILCS 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person’s or customer’s biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

36. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person’s biometric identifiers or biometric information (740 ILCS 14/15(c)) and requires companies to develop and comply with 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 such identifiers or information has been satisfied or within three years of the individual’s last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

37. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public’s hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are

biologically unique to the individual and, once compromised, an individual is at heightened risk for identity theft and left without any recourse.

38. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

39. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

## **II. Defendants Violate the Biometric Information Privacy Act.**

40. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using employees' biometric data as an authentication method stopped doing so.

41. However, Defendants failed to take note of the shift in Illinois law governing the collection and use of biometric data. As a result, each Defendant continues to collect, store, use, and disseminate White Castle employees' biometric data in violation of BIPA.

42. Specifically, when employees are hired by White Castle, they are required to have their fingerprints scanned to enroll them in its DigitalPersona employee database(s).

43. White Castle uses and has used employee software supplied by Cross Match that requires employees to use their fingerprint as a means of authentication. Per the company's policy, all White Castle employees are required to use their fingerprints to access their weekly paystubs.

FILED DATE: 1/18/2019 2:16 PM 2018CH15233

44. Upon information and belief, White Castle failed and continues to fail to inform its employees that it discloses their fingerprint data to out-of-state third parties, including Cross Match, and other, currently unknown, third party vendors that maintain the biometric data in their data centers; fails to inform its employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from employees before collecting their fingerprints.

45. Upon information and belief, Cross Match fails to inform White Castle employees that it discloses their fingerprint data to other, currently unknown, third parties, which host the biometric data in its data centers; fails to inform White Castle employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from White Castle employees before collecting their fingerprints.

46. Furthermore, each Defendant fails to provide employees with a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by BIPA.

47. The Pay by Touch bankruptcy, which triggered the passage of BIPA, highlights why such conduct – where individuals are aware that they are providing a fingerprint but are not aware to whom or for what purposes they are doing so – is dangerous. This bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers such as a fingerprint, who exactly is collecting their biometric data, where it will be transmitted, for what purposes it will be transmitted, and for how long. Each Defendant disregards these obligations and White Castle employees' statutory rights and instead

FILED DATE: 1/18/2019 2:16 PM 2018CH15233

unlawfully collect, store, use, and disseminate employees' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

48. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have not and will not destroy Plaintiff's and other similarly-situated individuals' biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with each company.

49. White Castle employees are not told what might happen to their biometric data if and when any Defendant merges with another company or worse, if and when any Defendant's business folds, or when the other third parties that have received their biometric data businesses fold.

50. Since Defendants neither publish BIPA-mandated data retention policies nor disclose the purposes for their collection of biometric data, White Castle employees have no idea whether any Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and other similarly situated individuals are not told to whom any Defendant currently discloses their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.

51. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

52. By and through the actions detailed above, Defendants disregarded Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.



FILED DATE: 1/18/2019 2:16 PM 2018CH15233

### **III. Plaintiff Latrina Cothron's Experience**

53. Plaintiff Latrina Cothron was hired by White Castle in 2004 and is currently working as a manager.

54. As a condition of employment, Cothron was required to scan her fingerprint(s) so White Castle could use it as an authentication method for Plaintiff to access the computer as a manager and to access her paystubs as an hourly employee.

55. White Castle subsequently stored Cothron's fingerprint data in its DigitalPersona employee database(s).

56. Cothron was required to scan her fingerprint each time she accessed a White Castle computer.

57. Cothron was also required to scan her fingerprint each time she accessed her paystubs.

58. Cothron has never been informed of the specific limited purposes or length of time for which any Defendant collected, stored, used, and/or disseminated her biometric data.

59. Cothron has never been informed of any biometric data retention policy developed by any Defendant, nor has she ever been informed whether any Defendant will ever permanently delete her biometric data.

60. Cothron has never been provided with nor ever signed a written release allowing any Defendant to collect, store, use or disseminate her biometric data.

61. Cothron has continuously and repeatedly been exposed to the risks and harmful conditions created by each Defendant's violations of BIPA alleged herein.

62. No amount of time or money can compensate Cothron if her biometric data is compromised by the lax procedures through which each Defendant captured, stored, used, and

disseminated her and other similarly-situated individuals' biometrics. Moreover, Cothron would not have provided her biometric data to any Defendant if she had known that they would retain such information for an indefinite period of time without her consent.

63. A showing of actual damages is not necessary in order to state a claim under BIPA. Nonetheless, Cothron has been aggrieved because she suffered an injury-in-fact based on each Defendant's violations of her legal rights. Defendants intentionally interfered with Cothron's right to possess and control her own sensitive biometric data. Additionally, Cothron suffered an invasion of a legally protected interest when each Defendant secured her personal and private biometric data at a time when it had no right to do so, a gross invasion of her right to privacy. BIPA protects employees like Cothron from this precise conduct. Defendants had no lawful right to secure this data or share it with third parties absent a specific legislative license to do so.

64. Cothron's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow. As such, Cothron was not sufficiently compensated by any Defendant for its retention and use of her and other similarly-situated employees' biometric data. Cothron would not have agreed to work for White Castle for the compensation she received if she had known that Defendants would retain her biometric data indefinitely.

65. Cothron also suffered an informational injury because each Defendant failed to provide her with information to which she was entitled by statute. Through BIPA, the Illinois legislature has created a right: an employee's right to receive certain information prior to an employer securing their highly personal, private and proprietary biometric data; and an injury – not receiving this extremely critical information.

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

66. Cothron also suffered an injury in fact because each Defendant improperly disseminated her biometric identifiers and/or biometric information to third parties, including but not limited to Cross Match, and any other third party that hosted the biometric data in their data centers, in violation of BIPA.

67. Pursuant to 740 ILCS 14/15(b), Cothron was entitled to receive certain information prior to Defendants securing her biometric data; namely, information advising her of the specific limited purpose(s) and length of time for which each Defendant collects, stores, uses and disseminates her private biometric data; information regarding each Defendant's biometric retention policy; and, a written release allowing each Defendant to collect, store, use, and disseminate her private biometric data. By depriving Cothron of this information, Defendants injured her. *Public Citizen v. U.S. Department of Justice*, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Akins*, 524 U.S. 11 (1998).

68. Finally, as a result of each Defendant's conduct, Cothron has experienced personal injury in the form of mental anguish. For example, Cothron experiences mental anguish and injury when contemplating what would happen to her biometric data if any Defendant went bankrupt, whether any Defendant will ever delete her biometric information, and whether (and to whom) any Defendant would share her biometric information.

69. Cothron has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of her biometric data; in the form of monetary damages by not obtaining additional compensation as a result of being denied access to material information about Defendants' policies and practices; in the form of the unauthorized disclosure of her confidential biometric data to third parties; in the form of interference with her right to

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

control and possess her confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

70. As Cothron is not required to allege or prove actual damages in order to state a claim under BIPA, she seeks statutory damages under BIPA as compensation for the injuries caused by Defendants.

### CLASS ALLEGATIONS

71. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS 5/2-801, Plaintiff brings claims on her own behalf and as a representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS 14/1, *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

72. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it first (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose and length of time 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.

73. Plaintiff seeks class certification under the Illinois Code of Civil Procedure, 735 ILCS 5/2-801 for the following class of similarly-situated employees under BIPA:

All individuals working for White Castle in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by any Defendant during the applicable statutory period.

74. This action is properly maintained as a class action under 735 ILCS 5/2-801

because:

- A. The class is so numerous that joinder of all members is impracticable;
- B. There are questions of law or fact that are common to the class;
- C. The claims of the Plaintiff are typical of the claims of the class; and,
- D. The Plaintiff will fairly and adequately protect the interests of the class.

**Numerosity**

75. The total number of putative class members exceeds fifty (50) individuals. The exact number of class members can easily be determined from White Castle's payroll records.

**Commonality**

76. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendants' failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

- A. Whether any Defendant collected, captured or otherwise obtained Plaintiff's biometric identifiers or biometric information;
- B. Whether any Defendant properly informed Plaintiff of their purposes for collecting, using, and storing her biometric identifiers or biometric information;
- C. Whether any Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff's biometric identifiers or biometric information;
- D. Whether any Defendant has disclosed or re-disclosed Plaintiff's biometric identifiers or biometric information;
- E. Whether any Defendant has sold, leased, traded, or otherwise profited from Plaintiff's biometric identifiers or biometric information;
- F. Whether any Defendant developed 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

FILED DATE: 1/18/2019 2:16 PM 2018CH15233

satisfied or within three years of their last interaction with the individual, whichever occurs first;

- G. Whether any Defendant complies with any such written policy (if one exists);
- H. Whether any Defendant used Plaintiff's fingerprints to identify her;
- I. Whether any Defendant's violations of BIPA have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties;
- J. Whether the violations of BIPA were committed negligently; and
- K. Whether the violations of BIPA were committed willfully.

77. Plaintiff anticipates that Defendants will raise defenses that are common to the class.

#### **Adequacy**

78. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

#### **Typicality**

79. The claims asserted by Plaintiff are typical of the class members she seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

80. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, he or she can "opt out" of this action pursuant to 735 ILCS 5/2-801.

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

**Predominance and Superiority**

81. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

82. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendants and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

**FIRST CAUSE OF ACTION**  
**Violation of 740 ILCS 14/1, *et seq.***  
**(On Behalf of Plaintiff and the Class)**

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

84. BIPA requires companies to obtain informed written consent from employees 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).

85. BIPA also prohibits private entities from disclosing a person’s or customer’s biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

86. Furthermore, BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company’s last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

87. Each Defendant fails to comply with these BIPA mandates.

88. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

89. Defendant Cross Match is a Delaware corporation that does business in Illinois and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

FILED DATE: 1/18/2019 2:16 PM 2018CH15233

90. Plaintiff is an individual who had her “biometric identifiers” collected by each Defendant (in the form of her fingerprints), as explained in detail in Sections II and III, *supra*. See 740 ILCS 14/10.

91. Plaintiff’s biometric identifiers were used to identify her and, therefore, constitute “biometric information” as defined by BIPA. See 740 ILCS 14/10.

92. Each Defendant systematically and automatically collected, used, stored, and disclosed Plaintiff’s biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

93. Upon information and belief, White Castle systematically disclosed Plaintiff’s biometric identifiers and biometric information to at least one third party, Cross Match.

94. Upon information and belief, each Defendant systematically disclosed Plaintiff’s biometric identifiers and biometric information to other, currently unknown, third parties, which hosted the biometric data in their data centers.

95. No Defendant informed Plaintiff in writing that her biometric identifiers and/or biometric information were being collected, stored, used, and disseminated, nor did any Defendant inform Plaintiff in writing of the specific purpose and length of term for which her biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

96. No Defendant provides a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. See 740 ILCS 14/15(a).

97. By collecting, storing, and using Plaintiff’s and the Class’s biometric identifiers and biometric information as described herein, each Defendant violated Plaintiff’s and the Class’s

rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

98. Upon information and belief, each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and have not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

99. These violations have raised a material risk that Plaintiff's and the Class's biometric data will be unlawfully accessed by third parties.

100. On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of \$5,000 for each willful 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).

**SECOND CAUSE OF ACTION**  
**Negligence**  
**(On Behalf of Plaintiff and the Class)**

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

102. Each Defendant owed Plaintiff and the Class a duty of reasonable care. Such duty required Defendants to exercise reasonable care in the collection and use of Plaintiff's and the Class's biometric data.

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

103. Additionally, White Castle owed Plaintiff and the Class a heightened duty – under which it assumed a duty to act carefully and not put Plaintiff and the Class at undue risk of harm – because of the employment relationship of the parties.

104. Each Defendant breached its duty by failing to implement a BIPA-compliant biometric authentication system with reasonable data security safeguards.

105. Specifically, Defendants breached their duties by failing to properly inform Plaintiff and the Class in writing of the specific purpose or length of time for which their fingerprints were being collected, stored, used, and disseminated.

106. Defendants also breached their duties by failing to provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and the Class's fingerprint data.

107. Upon information and belief, Defendants breached their duties because they lack retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and have not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with either company.

108. Upon information and belief, White Castle breached its duties because it systematically disclosed Plaintiff's biometric identifiers and biometric information to at least one third party: Cross Match.

109. Upon information and belief, each Defendant breached its duties because it systematically disclosed Plaintiff's biometric identifiers and biometric information to other, currently unknown, third parties, which hosted the biometric data in their data centers.

110. These violations have raised a material risk that Plaintiff's and the Class's biometric data will be unlawfully accessed by third parties.

111. As a direct and proximate cause of each Defendant's negligent misrepresentations, Plaintiff and the other Class members have suffered from diminution in the unique identifying value of their biometric information caused by Defendants' repeated dissemination and exposure of such information to third-parties, including Cross Match, and data storage vendors, among others.

112. Defendants knew or should have known that their breaches would cause Plaintiff and the other Class members to experience the foreseeable harms associated with the exposure of their biometrics to third parties, including the discontinuation of Plaintiff's and the Class member's exclusive possession and control of their biometrics and the accompanying loss of the unique identifying value of their biometrics.

113. Further, each Defendant's breach of its duty proximately caused and continues to cause an invasion of Plaintiff's and the Class's privacy, an informational injury, and mental anguish, in addition to the statutory damage provided in BIPA.

114. Accordingly, Plaintiff seeks an order declaring that Defendants' conduct constitutes negligence and awarding Plaintiff and the Class damages in an amount to be calculated at trial.

#### **PRAYER FOR RELIEF**

Wherefore, Plaintiff Latrina Cothron respectfully requests that this Court enter an Order:

- A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Latrina Cothron as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;
- B. Declaring that Defendants' actions, as set forth above, violate BIPA;
- C. Awarding statutory damages of \$5,000 for *each* willful and/or reckless violation of

BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of \$1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

- D. Declaring that Defendants' actions, as set forth above, constitute negligence;
- E. Declaring that Defendants' actions, as set forth above, were willful;
- F. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendants to collect, store, use and disseminate biometric identifiers and/or biometric information in compliance with BIPA;
- G. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);
- H. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,
- I. Provide such further relief as the Court deems just and equitable.

#### **JURY TRIAL**

Plaintiff demands a trial by jury for all issues so triable.

Date: January 8, 2019

Respectfully Submitted,

/s/ Andrew C. Ficzko  
Ryan F. Stephan  
Andrew C. Ficzko  
**STEPHAN ZOURAS, LLP**  
100 N. Riverside Plaza  
Suite 2150  
Chicago, Illinois 60606  
312.233.1550  
312.233.1560 *f*  
Firm ID: 43734  
Aficzko@stephanzouras.com

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

**CERTIFICATE OF SERVICE**

I, the attorney, hereby certify that on January 8, 2019, I electronically filed the attached with the Clerk of the Court using the ECF system which will send such filing to all attorneys of record.

/s/ Ryan F. Stephan



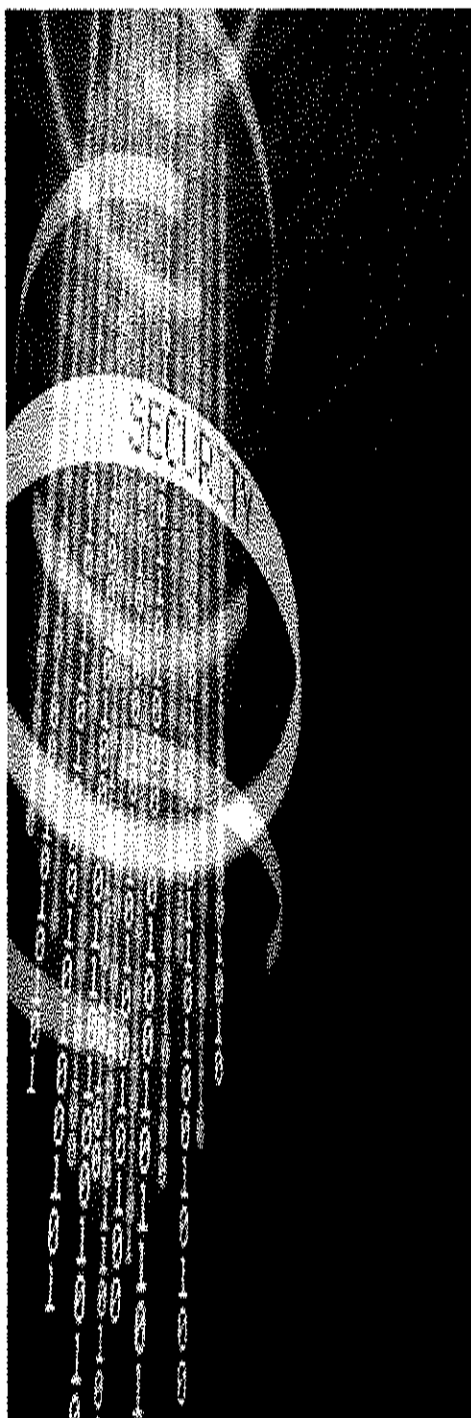
Return Date: No return date scheduled  
Hearing Date: No hearing scheduled  
Courtroom Number: No hearing scheduled  
Location: No hearing scheduled

FILED  
1/8/2019 2:16 PM  
DOROTHY BROWN  
CIRCUIT CLERK  
COOK COUNTY, IL  
2018CH15233

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

## EXHIBIT A

FILED DATE: 1/8/2019 2:16 PM 2018CH15233



Not Just Security, the Right  
Security.

## Data Breach QuickView Report

### Data Breach Trends - First Six Months of 2017

Sponsored by:  
**Risk Based Security**

Issued in July 2017

#### Mega breaches continue while pace of disclosure shows signs of slowing

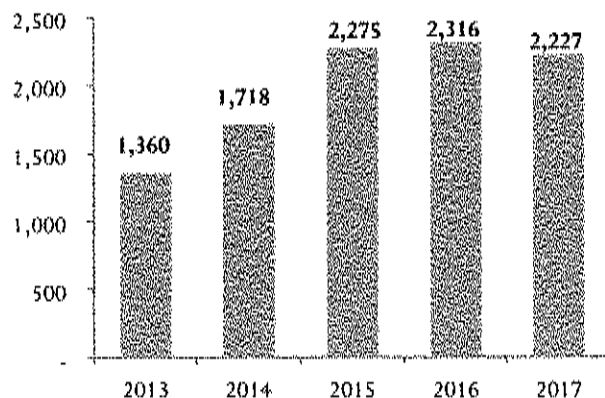
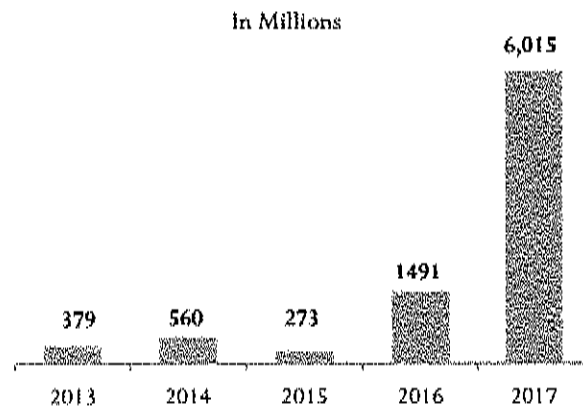
- There were 2,227 breaches reported in the first half of 2017, exposing over **6 billion** records.
- Top 10 breaches exposed 5.6 billion of the 6 billion records compromised.
- Top 10 Severity scores averaged 9.82 out of 10.0.
- The Business sector accounted for 56.5% of reported breaches, followed by Unknown (17%), Government (9.1%), Medical (9%), and Education (8.4%).
- The Business sector accounted for 93% of the total records exposed, followed by Government and Unknown (approximately 3% for each). Medical and Education sectors combined accounted for less than 1% of the total records exposed year to date.
- Web (inadvertent online disclosure) continues to be the leading cause of records compromised in 2017, accounting for 68.3% of records exposed, but only 7.1% of incidents reported so far this year.
- 41.6% of reported breaches were the result of Hacking, yet accounted for 30.6% of the exposed records.
- Breaches involving U.S. entities accounted for 61% of the breaches and approximately 30% of the exposed records.
- 29.3% of the breaches exposed between one and 1,000 records, 43.6% of breaches exposed between one and 10,000 records – virtually unchanged from Q12017.
- 121 breaches, or 5.4%, affected Third Parties.
- Fifty (50) breaches - 19 in Q2 and 31 in Q1 - exposed one million or more records.
- Four 2017 breaches are now on the Top 10 List of All Time Largest Breaches.
- The company DU Called, replaced River City Media for the top spot of the single largest breach disclosed, impacting 2 billion records.

## Table of Contents

MID-YEAR 2017 COMPARED TO MID-YEAR OF THE PREVIOUS FOUR YEARS .....	3
MID-YEAR 2017 BY INDUSTRY, BY MONTH .....	3
MID-YEAR 2017 ANALYSIS BY BREACH TYPE .....	4
MID-YEAR 2017 DATA BREACH ANALYSIS BY THREAT VECTOR .....	5
MID-YEAR 2017 EXPOSED RECORDS BY THREAT VECTOR .....	5
MID-YEAR 2017 ANALYSIS BY DATA FAMILY .....	6
MID-YEAR 2017 CONFIDENTIALITY IMPACT .....	6
PERCENTAGE OF BREACHES EXPOSING DATA TYPES YTD 2017 VS. PRIOR YEARS .....	7
MID-YEAR 2017 ANALYSIS OF RECORDS PER BREACH .....	8
MID-YEAR 2017 BREACH TYPES/RECORDS EXPOSED – TOP 5 .....	8
DISTRIBUTION OF BUSINESS GROUPS WITHIN ECONOMIC SECTORS – TOP 3 .....	9
MID-YEAR 2017 ANALYSIS BY COUNTRY .....	9
MID-YEAR 2017 ANALYSIS BY COUNTRY – TOP 10 .....	10
MID-YEAR 2017 EXPOSED RECORDS BY COUNTRY .....	10
MID-YEAR 2017 DISTRIBUTION OF BREACHES BY STATE .....	11
MID-YEAR 2017 ANALYSIS OF US STATE RANKINGS- EXPOSED RECORDS .....	11
MID-YEAR 2017 BREACHES INVOLVING THIRD PARTIES .....	12
MID-YEAR 2017 – BREACH SEVERITY SCORES & SCORING .....	13
MID-YEAR 2017 – BREACH SEVERITY SCORES – TOP 10 .....	13
TOP 20 LARGEST BREACHES ALL TIME (EXPOSED RECORDS COUNT) .....	14
METHODOLOGY & TERMS .....	17

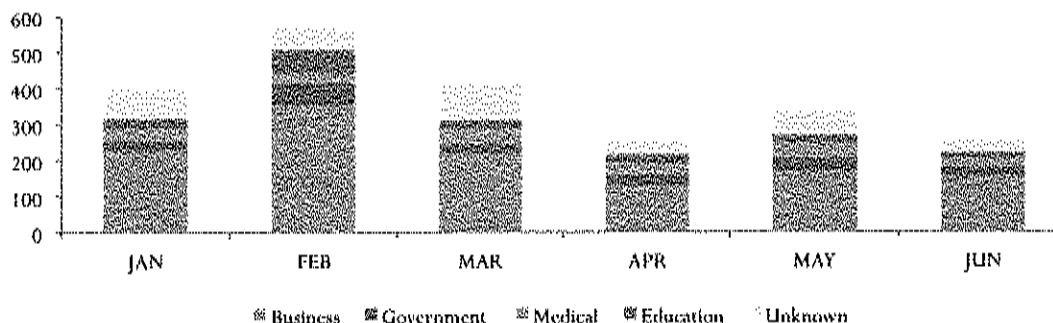
FILED DATE: 1/8/2019 2:16 PM 2018CH15233

## Mid-Year 2017 Compared to Mid-Year of the Previous Four Years

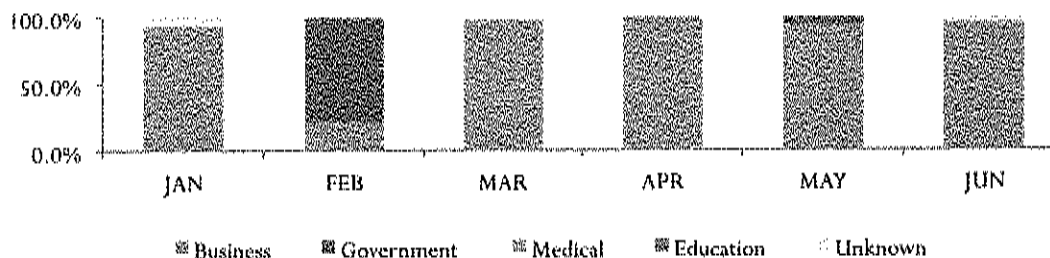
Number of Incidents by Year -  
First 6 MonthsNumber of Records Exposed by  
Year - First 6 Months

## Mid-Year 2017 by Industry, by Month

Distribution of Incidents by Industry, by Month

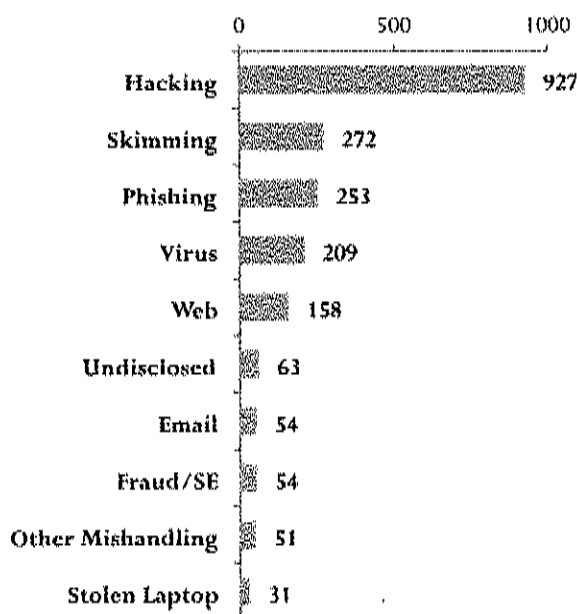


Distribution of Exposed Records by Industry, by Month



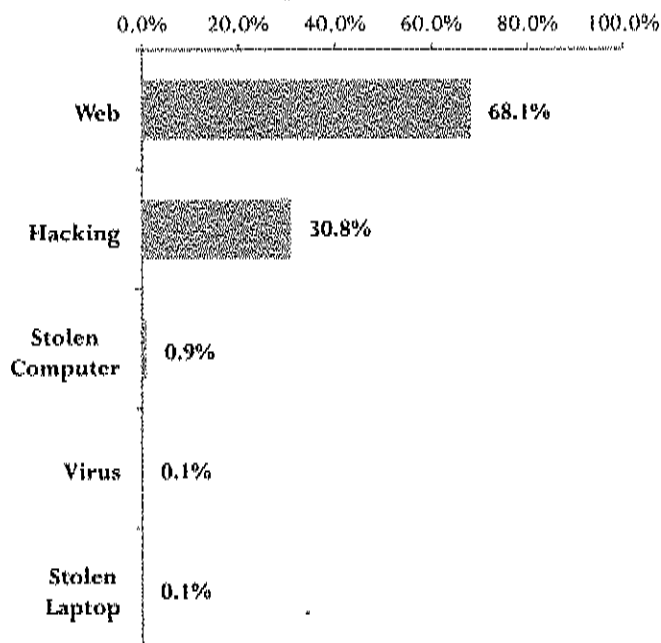
## Mid-Year 2017 Analysis by Breach Type

## Top 10 Breach Types - First 6 Months



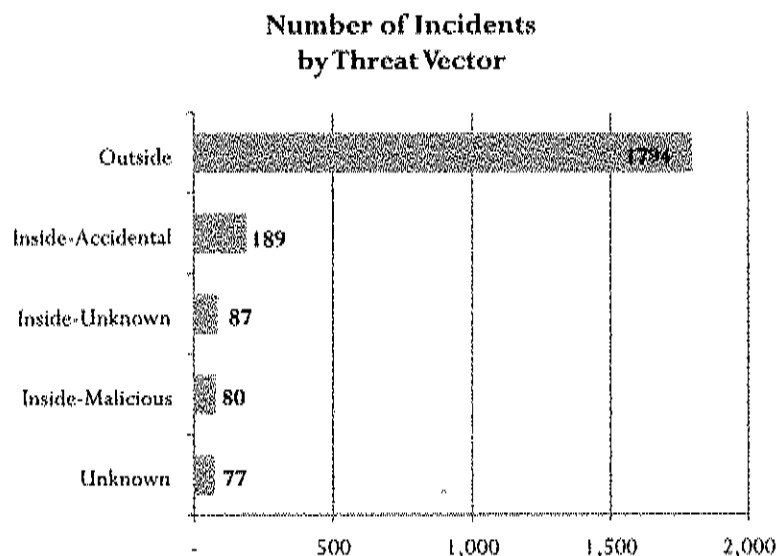
The number of phishing incidents started to decline once the U.S. tax season came to a close.

Despite being the leading cause of records exposed, Web (inadvertent online disclosure) ranked fifth on number of incidents.

Top 5 Breach Types by Records Exposed  
First 6 Months

While not making the top 5 list very often, a Stolen Computer from the COMELEC (Philippines Election Commission) offices resulted in 55.1 million voter records exposed.

## Mid-Year 2017 Data Breach Analysis by Threat Vector



16.0% of incidents were the result of insider activity, up slightly from 12.1% of incidents reported in Q12017.

## Mid-Year 2017 Exposed Records by Threat Vector

Threat Vector	Records Exposed
Outside	2,227,842,612
Inside-Unknown	2,001,248,057
Inside-Accidental	1,739,943,232
Unknown	45,540,090
Inside-Malicious	567,571
<b>Total</b>	<b>6,015,141,562</b>

A single insider incident exposed Two billion records.

## Mid-Year 2017 – Breach Discovery Method

	Internal Discovery - Incidents	Internal Discovery - Records	External Discovery - Incidents	External Discovery - Records	Undisclosed Discovery - Incidents	Undisclosed Discovery - Records
Q1	221	65,173,264	783	3,345,957,501	376	17,670,845
Q2	222	2,966,956	314	486,285,236	311	2,097,077,760
YTD	443	68,140,220	1,097	3,832,242,737	687	2,114,748,605



Mid-Year 2017 Top 10 Breaches Data Types and Severity Scores<sup>1</sup>

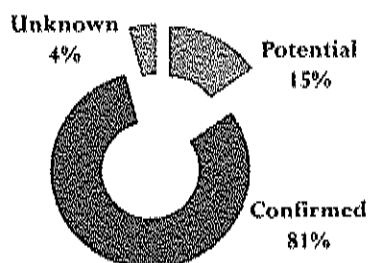
Breach Type	Records Exposed	Percentage of Total Exposed	Data Type <sup>2</sup>	Severity Score
Web	2,000,000,000	33.2%	ADD/NAA/NUM	10.0
Web	1,374,159,612	22.8%	ADD/EMA/FIN/MISC/NAA	10.0
Hack	1,221,893,767	20.3%	EMA/PWD	10.0
Web	267,693,854	4.5%	EMA/NUM	9.80
Web	198,000,000	3.3%	ADD/DOB/MISC/NAA/NUM	10.0
Web	135,000,000	2.2%	ADD/FIN/MISC/NAA/NUM/SSN	9.68
Hack	129,696,449	2.2%	EMA/PWD	9.71
Hack	126,761,168	2.1%	ADD/NAA/NUM	9.40
Hack	91,890,110	1.5%	EMA/PWD/USR	9.56
Hack	77,000,000	1.3%	EMA/PWD/USR	9.96
The top 10 breaches exposed 5,622,094,960 records, or 93.4% of the total records exposed in the first 6 months				

## Mid-Year 2017 Analysis by Data Family

	Percentage of Total Breaches	Percentage of Total Exposed Records	Percentage of Total Breaches	Percentage of Total Exposed Records
Data Family	Mid-Year 2016	Mid-Year 2016	Mid-Year 2017	Mid-Year 2017
Electronic	90.18%	99.98%	93.22%	99.98%
Physical	6.75%	<1%	4.62%	<1%
Unknown	3.07%	<1%	2.16%	<1%

## Mid-Year 2017 Confidentiality Impact

## Confidentiality Impact



The majority of breaches continue to result in confirmed unauthorized access to sensitive data

<sup>1</sup> See page 13 for additional detail on these incidents.

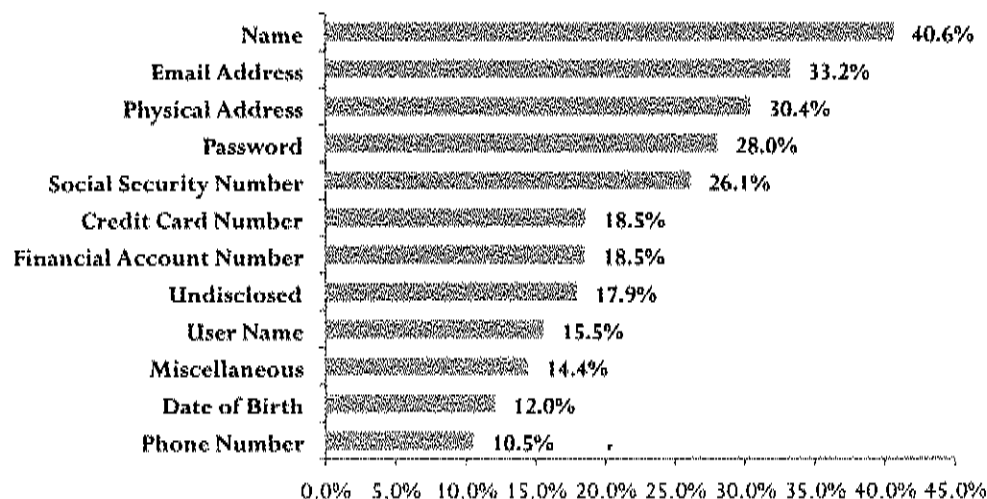
<sup>2</sup> See page 17 for a description of abbreviations.



FILED DATE: 1/18/2019 2:16 PM 2018CH15233

## Mid-Year 2017 Analysis by Data Type - Percentage of Breaches

## Incidents by Data Type Exposed



Compared to the same time period in 2016, the percentage of breaches impacting Social Security numbers increased from 17.6% in 2016 to 26.1% in 2017. Likewise, the percentage of breaches impacting Names increased from 36.1% to 40.6% and the percentage impacting physical addresses increased from 21.6% to 30.4%. Research indicates this effect is attributable to the steady rise of successful phishing campaigns targeting W-2 data during the first 4 months of the year.

## Percentage of Breaches Exposing Data Types YTD 2017 vs. Prior Years

Data Type	First 6 Months 2017	First 6 Months 2016	First 6 Months 2015
Name	40.6%	36.1%	27.8%
Email Address	33.2%	42.9%	45.5%
Physical Address	30.4%	21.6%	12.3%
Password	28%	39.8%	52.2%

The "W-2 phishing effect" is more evident when comparing the percentage of breaches impacting 2017's top four data types over time. Access credentials in the form of username / email address and password remain popular targets, but the overall number of breaches impacting these records has steadily declined during the first half of 2017 as attention turns to data more directly useful for tax fraud.

## Mid-Year 2017 Analysis of Records per Breach

Exposed Records	Number of Breaches	Percent of Total
Unknown/Undisclosed	1024	46.0%
1 to 100	317	14.2%
101 to 1,000	336	15.1%
1,001 to 10,000	320	14.4%
10,001 to 100,000	132	5.9%
100,001 to 500,000	36	1.6%
500,001 to 999,999	12	0.5%
1 M to 10 M	30	1.3%
> 10 M	20	0.9%

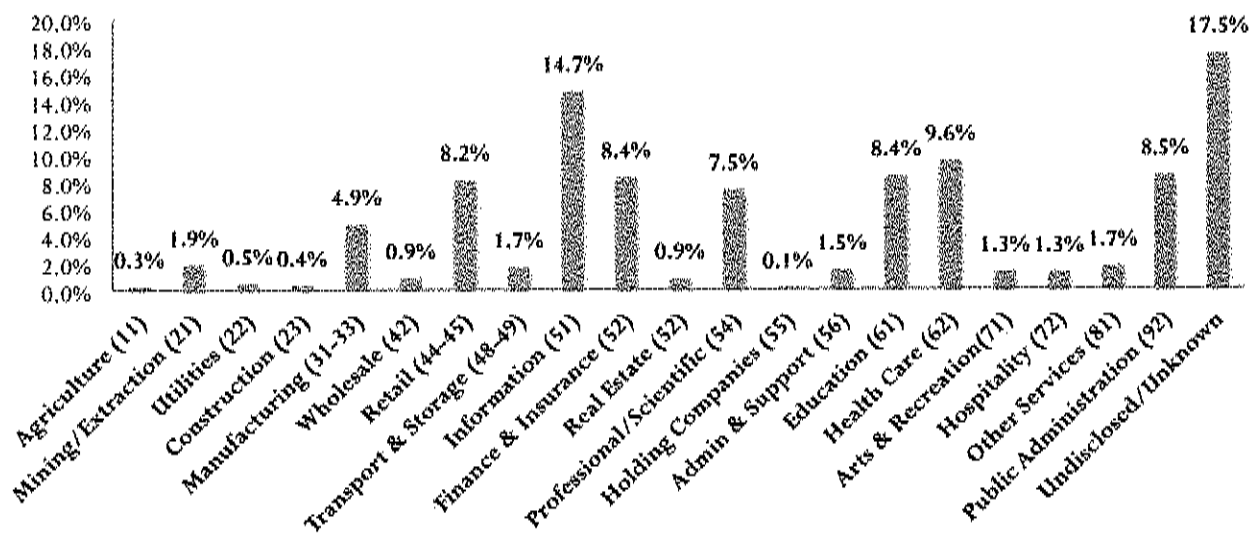
For the third year in a row, the number of incidents with exposed records either unknown or unreported increased. At this point in 2015, it was 27.6%; in 2016, it was 35.4%.

## Mid-Year 2017 Breach Types/Records Exposed – Top 5

Breach Category	Number of Breaches	Number of Records Exposed	Average Records per Breach	Percent of Total Records Exposed
Hacking	927	1,839,750,699	1,984,629	30.59%
Skimming	272	4,874	18	0.00%
Phishing	253	458,964	1,814	0.01%
Virus/Malware	209	6,918,120	33,101	0.12%
Web	158	4,069,836,698	25,758,460	67.67%

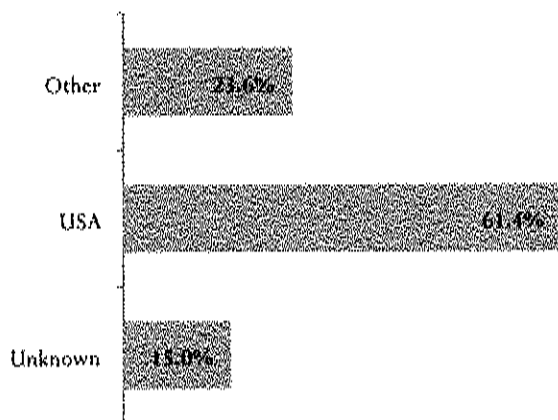
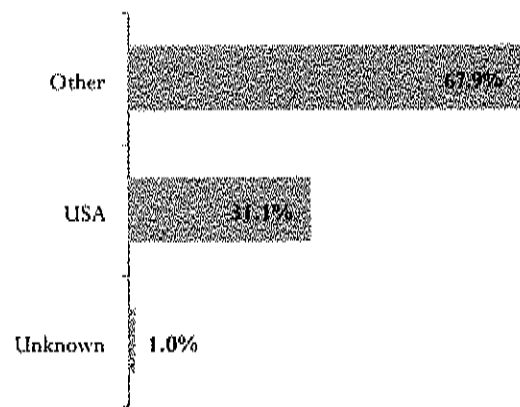
## Mid-Year 2017 Analysis of Incidents by NAICS Economic Sector

## Distribution of Incidents by Economic Sector



**Distribution of Business Groups Within Economic Sectors – Top 3**

Economic Sector	Business Group	Percentage of Breaches Within Economic Sector
Information (51)	Software / Web Services	79.9%
	Mass Media	11.2%
	Telecommunications	7.3%
HealthCare (62)	Non-Hospital Facilities	33.3%
	Hospitals	29.5%
	Practitioner Offices	29.5%
Public Sector (92)	Federal	33.8%
	State	20.6%
	Cities	19.5%

**Mid-Year 2017 Analysis by Country****Incidents by Location****Records Exposed by Location**

The Top 10 countries accounted for 1,708, or 76.6% of the breaches reported and 97.7% of the records compromised.

## Mid-Year 2017 Analysis by Country – Top 10

## Incidents by Country - Top 10

United States	1367
United Kingdom	104
Canada	59
India	52
Australia	34
China	22
Ukraine	19
Russian Federation	19
Indonesia	18
Iran	14

North America  
accounted for  
64.2% of breaches

## Mid-Year 2017 Exposed Records by Country

Ranking	Number of Breaches	Country	Total Exposed Records	Average Records per Breach	Median Number of Records	Percentage of Exposed Records
1	22	China	3,822,024,257	173,728,375	3,371,754	48.83%
2	1367	United States	3,746,193,334	2,740,449	1,700	47.86%
3	52	India	179,055,018	3,443,366	308	2.29%
4	2	Philippines	55,254,020	27,627,010	-	0.71%
5	7	Hong Kong	12,041,792	1,720,256	1,890,876	0.15%
6	4	South Africa	6,700,000	1,675,000	-	0.09%
7	104	United Kingdom	2,401,829	23,095	669	0.03%
8	59	Canada	2,107,262	35,716	503	0.03%
9	2	Finland	1,100,023	550,012	-	0.01%
10	7	Japan	722,096	103,157	121	0.01%

Large breaches affecting 1,000,000 or more records heavily influences the average number of records lost in certain countries. The median number of records lost in the five countries reporting the most breaches ranges between 308 and 1,700, with Australia coming in at 872.

## Mid-Year 2017 Distribution of Breaches By State

Incidents by US State -  
Top 10

CA	140
TX	98
FL	94
NY	90
PA	60
VA	46
OH	45
IL	44
MD	44
NC	35

The top 10 states  
represent 51% of  
US breaches.

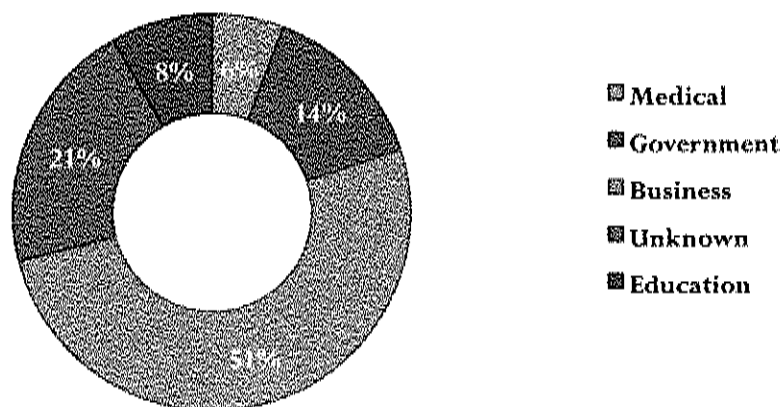
## Mid-Year 2017 Analysis of US State Rankings- Exposed Records

Exposed Records Ranking	US State	Total Exposed Records	Number of Breaches	Exposed Records/Breach	Percentage of USA Exposed Records
1	WA	1,375,336,881	27	50,938,403	73.42%
2	NJ	33,724,579	29	1,162,917	1.31%
3	CA	10,690,370	140	76,360	0.31%
4	NY	8,163,474	90	90,705	0.19%
5	AR	4,890,000	7	698,571	0.16%
6	TX	4,777,984	98	48,755	0.15%
7	GA	3,798,732	23	165,162	0.10%
8	MD	2,674,211	44	60,778	0.09%
9	MI	2,426,296	22	110,286	0.07%
10	FL	1,519,843	94	16,169	0.02%

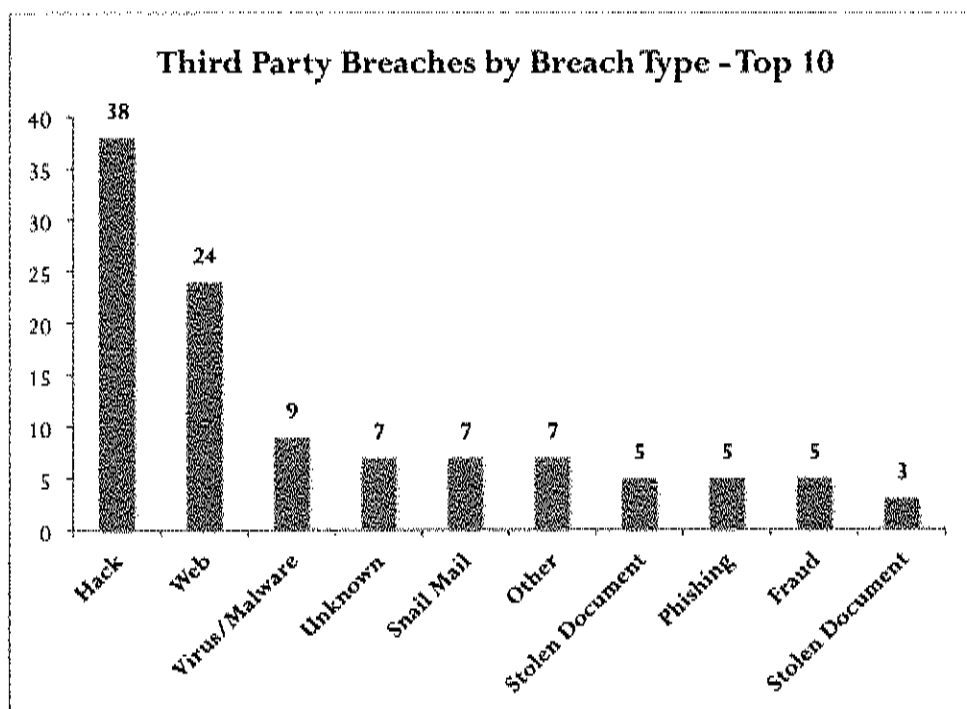


## Mid-Year 2017 Breaches Involving Third Parties

## Third Party Breaches by Business Type



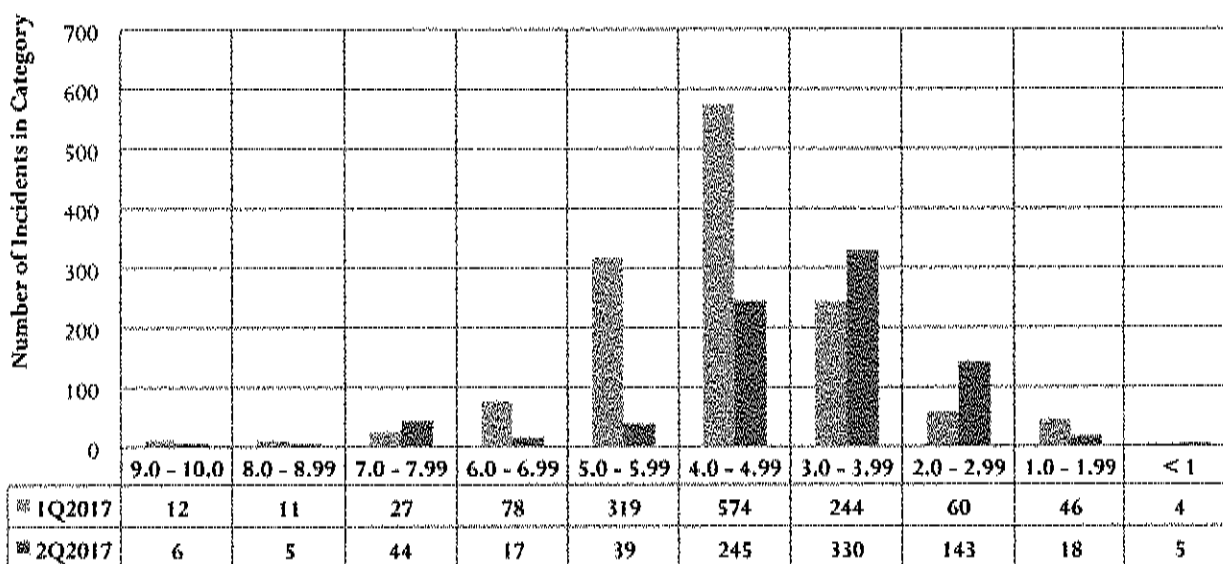
- Organizations classified in the business sector account for more than 50% of the breaches impacting data belonging to customers, clients or other 3<sup>rd</sup> parties.
- Three of the largest breaches reported in the first six months impacted 3<sup>rd</sup> parties.
- Hacking remains the dominant breach type for incidents impacting 3<sup>rd</sup> Parties, with regard to both the number of breaches and the number of records compromised.



## Mid-Year 2017 – Breach Severity Scores & Scoring

We can all readily agree that not all data breaches are created equal. Where disagreement arises is when we attempt to rate the 'severity' or 'impact' of a breach. At Risk Based Security we have combined our knowledge of the security industry, business experience and our comprehensive data breach information to calculate a Data Breach Severity Score.

**Breach Severity Scores by Quarter**



On a positive note, breach severity scores declined in the second quarter of 2107. 58.2% of breaches reported in Q2 scored 3 or below while 25.7% of Q1 reported breaches scored 3 or below.

## Mid-Year 2017 – Breach Severity Scores – Top 10

Score	Reported	Organization	Top 10 Summary
10	Q2	DU Group dba DU Caller	(Web) 2,000,000,000 user phone numbers, names and addresses inappropriately made accessible in an uncensored public directory
10	Q1	NetEase, Inc. dba 163.com	(Hacking) 1,221,893,767 email addresses and passwords stolen by hackers and sold on the Dark Web by DoubleFlag
10	Q1	River City Media, LLC	(Web) 1,374,159,612 names, addresses, IP addresses, and email addresses, as well as an undisclosed number of financial documents, chat logs, and backups exposed by faulty rsync backup
10	Q2	Deep Root Analytics	(Web) Approximately 198,000,000 voter names, addresses, dates of birth, phone numbers, political party affiliations, and other demographic information exposed in an unsecured Amazon S3 bucket



Score	Reported	Organization	Top 10 Summary
9.96	Q2	Edmodo	(Hacking) 77,000,000 user email addresses, usernames, and bcrypt hashed passwords with salts stolen by hackers through undisclosed means
9.80	Q1	EmailCar	(Web) 267,693,854 email addresses and phone numbers exposed in an unsecure MongoDB installation and later dumped on the Internet
9.71	Q1	Tencent Holdings Ltd dba QQ.com	(Hacking) 129,696,449 email addresses and passwords stolen by hackers and sold on the Dark Web by DoubleFlag
9.68	Q2	National Social Assistance Programme (India)	(Web) Roughly 135,000,000 Aadhaar numbers and 100,000,000 linked bank account numbers, as well as names, caste, religion, addresses, phone numbers, photographs, and assorted financial details leaked on government web portals
9.56	Q2	Youku	(Hacking) 91,890,110 user accounts with usernames, email addresses and MD5 encrypted passwords compromised by hackers and offered for sale
9.45	Q1	Yahoo Japan	(Hacking) 23,590,165 email addresses and passwords stolen by hackers and sold on the Dark Web by DoubleFlag

### Top 20 Largest Breaches All Time (Exposed Records Count)

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
<b>Highest All Time</b> 5/13/2017	User phone numbers, names and addresses inappropriately made accessible in an uncensored public directory	2 Billion	DU Caller Group (DU Caller)	Business - Technology	China
<b>Number 2</b> 3/3/2017	Names, addresses, IP addresses, and email addresses, as well as an undisclosed number of financial documents, chat logs, and backups, exposed by faulty rsync backup.	1.3 Billion	River City Media, LLC	Business - Technology	United States
<b>Number 3</b> 1/25/2017	A database holding email addresses and passwords stolen by hackers and offered for sale on the dark web.	1.2 Billion	NetEase, Inc. dba 163.com	Business – Technology	China

FILED DATE: 1/8/2019 2:16 PM 2018CH15233

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
<b>Number 4</b> 12/14/2016	While investigating the #4 incident on this list, a second hacking event was discovered targeting user names, email addresses, phone numbers, dates of birth, hashed passwords and security questions and associated answers.	1 Billion	Yahoo	Business - Technology	United States
<b>Number 5</b> 9/22/2016	Hack exposes user names, email addresses, phone numbers, dates of birth, hashed passwords and security questions and associated answers.	500 Million	Yahoo	Business - Technology	United States
<b>Number 6</b> 10/18/2016	Hackers exploit a Local File Inclusion vulnerability, compromising member email addresses, usernames, and encrypted passwords, IP addresses and membership statuses.	412 Million	FriendFinder Networks, Inc	Business - Technology	United States
<b>Number 7</b> 5/27/2016	Hack exposes user account records containing SHA1 encrypted passwords, email addresses.	360 Million	MySpace	Business - Technology	United States
<b>Number 8</b> 1/1/2017	Email addresses and phone numbers were exposed in an unsecure MongoDB installation, which was later downloaded and dumped on the Internet	267 Million	EmailCar	Business - Technology	China
<b>Number 9</b> 8/22/2014	Hack of websites exposes names, registration numbers, usernames and passwords.	220 Million	Organization's Name has not been reported	Unknown	South Korea
<b>Number 10</b> 12/3/2016	Hackers offer for sale a database containing a variety of personal and financial details.	203 Million	Organization's Name has not been reported	Unknown	Unknown
<b>Number 11</b> 10/19/2013	Fraudulent account used to gain access to credit card numbers, social security numbers, names, and financial account numbers.	200 Million	Court Ventures, Inc.	Business - Data	United States
<b>Number 12</b> 6/19/2017	Unsecured Amazon S3 bucket exposes voter names, addresses, dates of birth, contact information and voter preferences.	198 Million	Deep Root Analytics	Business / Business	United States

FILED DATE: 1/18/2019 2:16 PM 2018CH15233

Breach Reported Date	Summary	Records Exposed	Organization's Name	Industry-Sector	Breach Location
<b>Number 13</b> 12/28/2015	Mis-configured database exposes voter names, dates of birth, addresses, phone numbers, political party affiliations, and genders.	191 Million	Organization's Name has not been reported	Unknown	United States
<b>Number 14</b> 6/21/2014	Hack exposes trip details of customers after cracking MD5 hashes	173 Million	NYC Taxi & Limousine Commission	Government - City	United States
<b>Number 15</b> 6/23/2016	Hack exposes USA voter information.	154 Million	Organization's Name has not been reported	Unknown	United States
<b>Number 16</b> 10/3/2013	Hack exposed customer names, IDs, encrypted passwords and debit/ credit card numbers with expiration dates, source code and other customer order information.	152 Million	Adobe Systems, Inc.	Business - Technology	United States
<b>Number 17</b> 3/17/2012	Firm may have illegally bought and sold customers' information.	150 Million	Shanghai Roadway D&B Marketing Services Co.	Business - Data	China
<b>Number 18</b> 5/21/2014	Hack exposes names, encrypted passwords, email addresses, registered addresses, phone numbers and dates of birth.	145 Million	eBay, Inc.	Business - Retail	United States
<b>Number 19</b> 6/8/2013	North Korean Hackers expose email addresses and identification numbers.	140 Million	Organization's Name has not been reported	Unknown	South Korea
<b>Number 20</b> 5/2/2017	Leaky governmental websites expose Aadhaar numbers, banking details, names and other personal information.	135 Million	National Social Assistance Programme	Government - Federal	India

## Methodology & Terms

Risk Based Security's research methods include automated processes coupled with traditional human research and analysis. Our proprietary applications crawl the Internet 24x7 to capture and aggregate potential data breach breaches for our researchers to analyze. In addition, the research team manually verifies news feeds, blogs, and other sources looking for new data breaches as well as new information on previously disclosed incidents. The database also includes information obtained through Freedom of Information Act (FOIA) requests, seeking breach notification documentation from various state and federal agencies in the United States. The research team extends our heartfelt thanks to the individuals and agencies that assist with fulfilling our requests for information.

### Data Standards and the use of "Unknown"

In order for any data point to be associated with a breach entry, Risk Based Security requires a high degree of confidence in the accuracy of the information reported as well as the ability to reference a public source for the information. In short, the research team does not guess at the facts. For this reason the term "Unknown" is used when the item cannot be verified in accordance with our data validation requirements. This can occur when the breached organization cannot be identified but leaked data is confirmed to be valid or when the breached organization is unwilling or unable to provide sufficient clarity to the data point.

**Breach Types are defined as follows:**

Name	Description
Disposal Computer	Discovery of computers not disposed of properly
Disposal Document	Discovery of documents not disposed of properly
Disposal Drive	Discovery of disk drives not disposed of properly
Disposal Mobile	Discovery of mobile devices not disposed of properly
Disposal Tape	Discovery of backup tapes not disposed of properly
Email	Email communication exposed to unintended third party
Fax	Fax communication exposed to unintended third party
Fraud SE	Fraud or scam (usually insider-related), social engineering
Hack	Computer-based intrusion
Lost Computer	Lost computer (unspecified type in media reports)
Lost Document	Discovery of documents not disposed of properly, not stolen
Lost Drive	Lost data drive (unspecified if IDE, SCSI, thumb drive, etc.)
Lost Laptop	Lost laptop (generally specified as a laptop in media reports)
Lost Media	Media (e.g. disks) reported to have been lost by a third party
Lost Mobile	Lost mobile phone or device such as tablets, etc.
Lost Tape	Lost backup tapes
Missing Document	Missing document, unknown or disputed whether lost or stolen
Missing Drive	Missing drive, unknown or disputed whether lost or stolen
Missing Laptop	Missing laptop, unknown or disputed whether lost or stolen
Missing Media	Missing media, unknown or disputed whether lost or stolen
Other	Miscellaneous breach type not yet categorized
Phishing	Masquerading as a trusted entity in an electronic communication to obtain data
Seizure	Forcible taking of property by a government law enforcement official
Skimming	Using electronic device (skimmer) to swipe victims' credit/debit card numbers
Snail Mail	Personal information in "snail mail" exposed to unintended third party
Snooping	Exceeding intended privileges and accessing data not authorized to view
Stolen Computer	Stolen desktop (or unspecified computer type in media reports)
Stolen Document	Documents either reported or known to have been stolen by a third party
Stolen Drive	Stolen data drive, unspecified if IDE, SCSI, thumb drive, etc.
Stolen Laptop	Stolen Laptop (generally specified as a laptop in media reports)
Stolen Media	Media generally reported or known to have been stolen by a third party

Name	Description
Stolen Mobile	Stolen mobile phone or device such as tablets, etc.
Stolen Tape	Stolen backup tapes
Unknown	Unknown or unreported breach type
Virus (Malware)	Exposure to personal information via virus or Trojan (possibly classified as hack)
Web	Web-based intrusion, data exposed to the public via search engines, public pages

**Data Type Definitions**

Abbreviation	Description
CCN	Credit Card Numbers
SSN	Social Security Numbers (or Non-US Equivalent)
NAA	Names
EMA	Email Addresses
MISC	Miscellaneous
MED	Medical
ACC	Account Information
DOB	Date of Birth
FIN	Financial Information
UNK	Unknown
PWD	Passwords
ADD	Addresses
USR	User Name
NUM	Phone Number
IP	Intellectual Property

**NO WARRANTY.**

*Risk Based Security, Inc. makes this report available on an "As-is" basis and offers no warranty as to its accuracy, completeness or that it includes all the latest data breach breaches. The information contained in this report is general in nature and should not be used to address specific security issues. Opinions and conclusions presented reflect judgment at the time of publication and are subject to change without notice. Any use of the information contained in this report is solely at the risk of the user. Risk Based Security, Inc. assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. If you have specific security concerns please contact Risk Based security, Inc. for more detailed data loss analysis and security consulting services.*



## About Risk Based Security

Risk Based Security (RBS) provides detailed information and analysis on Data Breaches, Vendor Risk Scores and Vulnerability Intelligence. Our products, Cyber Risk Analytics (CRA) and VulnDB, provide organizations with access to the most comprehensive threat intelligence knowledge bases available, including advanced search capabilities, access to raw data via API, and email alerting to assist organizations in taking the right actions in a timely manner. In addition, our YourCISO offering provides organizations with on-demand access to high quality security and information risk management resources in one, easy to use web portal.

VulnDB is the most comprehensive and timely vulnerability intelligence available and provides actionable information about the latest in security vulnerabilities via an easy-to-use SaaS Portal, or a RESTful API for easy integration into GRC tools and ticketing systems. VulnDB allows organizations to search on and be alerted to the latest vulnerabilities, both in end-user software and the third-party libraries or dependencies that help build applications. A subscription to VulnDB provides organizations with simple to understand ratings and metrics on their vendors and products, and how each contributes to the organization's risk-profile and cost of ownership.

Cyber Risk Analytics (CRA) provides actionable security ratings and threat intelligence on a wide variety of organizations. This enables organizations to reduce exposure to the threats most likely to impact them and their vendor base. In addition, our PreBreach vendor risk rating, the result of a deep-view into the metrics driving cyber exposures, are used to better understand the digital hygiene of an organization and the likelihood of a future data breach. The integration of PreBreach ratings into security processes, vendor management programs, cyber insurance processes and risk management tools allows organizations to avoid costly risk assessments, while enabling businesses to understand its risk posture, act quickly and appropriately to proactively protect its most critical information assets.

YourCISO provides organizations with on-demand access to high quality security and information risk management resources in one, easy to use web portal. YourCISO provides organization ready access to a senior executives and highly skilled technical security experts with a proven track record, matched specifically to your needs. The YourCISO service is designed to be an affordable long term solution for addressing information security risks. YourCISO brings together all the elements an organization needs to develop, document and manage a comprehensive information security program.

For more information, please visit:

<https://www.riskbasedsecurity.com/>  
<https://vulndb.cyberriskanalytics.com/>  
<https://www.cyberriskanalytics.com/>  
<https://www.yourciso.com/>

Or call 855-RBS- RISK.

# **EXHIBIT 2**



Return Date: No return date scheduled  
Hearing Date: 1/16/2019 9:30 AM - 9:30 AM  
Courtroom Number:  
Location:

FILED  
1/8/2019 2:36 PM  
DOROTHY BROWN  
CIRCUIT CLERK  
COOK COUNTY, IL  
2018CH15233

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

**LATRINA COTHRON, individually,** )  
**and on behalf of all others similarly situated,** )  
) )  
**Plaintiff,** )  
) )  
**v.** )  
) )  
**WHITE CASTLE SYSTEM, INC. D/B/A** )  
**WHITE CASTLE, and CROSS MATCH** )  
**TECHNOLOGIES, INC.,** )  
) )  
**Defendants.** )

**Case No. 18-CH-15233**

**PLAINTIFF'S AMENDED MOTION FOR CLASS CERTIFICATION AND REQUEST  
FOR DISCOVERY ON CERTIFICATION ISSUES**

Plaintiff Latrina Cothron ("Plaintiff") alleges that Defendants White Castle System, Inc. d/b/a White Castle ("White Castle") and Cross Match Technologies, Inc., ("Cross Match") (collectively, "Defendants"), systematically violated the Biometric Information Privacy Act ("BIPA") 740 ILCS 14/1, *et seq.* This case is well suited for class certification pursuant to 735 ILCS 5/2-801. Specifically, Plaintiff seeks to certify a class consisting of hundreds of former and current similarly-situated employees who worked for White Castle in the State of Illinois who had their fingerprints unlawfully collected, captured, received, otherwise obtained, or disclosed by Defendants during the applicable statutory period in violation of BIPA. The question of liability is a legal question that can be answered in one fell swoop. As Plaintiff's claims and the claims of similarly-situated individuals all arise from Defendants' uniform policies and practices, they satisfy the requirement of 735 ILCS 5/2-801 and should be certified.

Plaintiff moves for class certification to protect members of the proposed class, individuals whose proprietary and legally protected personal and private biometric data was invaded by

FILED DATE: 1/8/2019 2:36 PM 2018CH15233

Defendants. Plaintiff believes that the evidence and argumentation submitted within this motion are sufficient to allow the class to be certified now. However, in the event the Court (or Defendants) wishes for the parties to undertake formal discovery prior to the Court's consideration of this motion, Plaintiff requests that the Court allow her to supplement her briefing and defer the response and reply deadlines.

## **I. RELEVANT BACKGROUND**

### **A. The Biometric Information Privacy Act**

Major national corporations started using Chicago and other locations in Illinois in the early 2000s to test “new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.” 740 ILCS 14/5(c). Given its relative infancy, an overwhelming portion of the public became wary of this then-growing, yet unregulated, technology. *See* 740 ILCS 14/5.

The Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* was enacted in 2008, arising from concerns that these experimental uses of finger-scan technologies created a “very serious need of protections for the citizens of Illinois when it comes to biometric information.” Illinois House Transcript, 2008 Reg. Sess. No. 276. Under the Act, it is unlawful for a private entity to, among other things, “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers or biometric information unless it 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).

Although there may be benefits with using biometrics in the workplace, there are also serious risks. Unlike ID badges— which can be changed or replaced if stolen or compromised — fingerprints are a unique, permanent biometric identifier associated with each individual. These biometrics are biologically unique to the individual; once compromised, the individual has *no* means by which to prevent identity theft, unauthorized tracking, or other unlawful or improper use of this information. This exposes individuals to serious and irreversible privacy risks. For example, if a biometric database is hacked, breached, or otherwise exposed — as in the recent Equifax, Home Depot, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches, to name a few — individuals have no means to prevent the misappropriation and theft of their proprietary biometric makeup. Thus, recognizing the need to protect its citizens from harms like these, Illinois enacted BIPA specifically to regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

#### **A. Factual Allegations**

Plaintiff Latrina Cothron filed the original class action against Defendants on December 6, 2018, to redress Defendants' unlawful collection, use, storage, and disclosure of biometric information of White Castle employees under BIPA. Plaintiff filed an Amended Class Action Complaint on January 8, 2019. In her Amended Class Action Complaint, Cothron provided detailed allegations that White Castle employees were and continue to be universally required to scan their fingerprints for enrollment in an employee database(s) as a condition of their employment, but are not: (1) informed in writing of the purpose(s) and length of time for which fingerprint data is being collected, stored, used, and disseminated by Defendants; (2) provided a publicly available retention schedule or guidelines for permanent destruction of the biometric data

by Defendants; and (3) provided (nor did they execute) a written release for Defendants, as required by BIPA. *See* Amended Compl. ¶¶ 11-12.

Cothron was hired by White Castle in 2004 and is currently working as a manager. *Id.* ¶ 53. As a condition of employment, Cothron was required to scan her fingerprint to access White Castle computers and her paystubs. *Id.* ¶ 54. White Castle subsequently stored Cothron's fingerprint data in its DigitalPersona employee database. *Id.* ¶ 55. Cothron was required to scan her fingerprint each time she accessed her paystub or a company computer. *Id.* ¶¶ 56-57. However, Defendants failed and continue to fail to inform White Castle employees, including Cothron, of the extent of the purposes for which they collect individuals' sensitive biometric data or to whom the data is disclosed. *Id.* ¶¶ 11, 12, 44, 45, 50, 58. Defendants similarly failed to provide White Castle employees, including Cothron, with a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying individuals' fingerprint data when the initial purpose for collecting or obtaining their fingerprint is no longer relevant, as required by BIPA. *Id.* ¶¶ 11-12, 15, 46, 48, 50, 59, 95-96, 106. Employees, including Cothron, have no knowledge when they leave the company of when – if ever – their biometric identifiers will be removed from Defendants' database(s). *Id.* ¶¶ 48-49, 98. White Castle employees are not told what might happen to their biometric data if and when Defendants merge with another company or, worse, if and when Defendants' entire businesses fold. *Id.* Since Defendants neither publish a BIPA-mandated data retention policy nor disclose the purposes for their collection of biometric data, employees, including Cothron, have no idea whether any Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. *Id.* ¶ 50. Nor are employees told to whom any Defendant currently discloses their biometric data or what might happen to their biometric data in the event of a merger or a bankruptcy. *Id.* Finally, Defendants never secured a written

FILED DATE: 1/8/2019 2:36 PM 2018CH15233

release executed by any of White Castle' employees, including Cothron, permitting them to collect, store, use, and disseminate employees' biometric data, as required by BIPA. *Id.* ¶¶ 11-12, 44-45, 60, 67, 92.

Accordingly, Defendants' practices violated BIPA. As a result of Defendants' violations, Plaintiff and similarly-situated individuals were subject to Defendants' common and uniform policies and practices and were victims of their schemes to unlawfully collect, store, use, and disseminate White Castle employees' biometric data in direct violation of BIPA. As a result of Defendants' violations of BIPA, Plaintiff and all other similarly-situated individuals suffered an invasion of privacy and other damages.<sup>1</sup>

Plaintiff now seeks class certification for the following similarly-situated individuals, defined as:

All individuals working for White Castle in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by any Defendant during the applicable statutory period.

Given Defendants' standard practices defined above and the straightforward and common legal questions presented in this case, Plaintiff now moves for class certification. Notably, this motion is being filed shortly after the Amended Complaint was filed and before any Defendant has responded. The parties have not discussed settlement, neither settlement offers nor demands have been made, and a scheduling order has not been issued. For the reasons discussed herein, Plaintiff's request should be granted.

---

<sup>1</sup> BIPA does not require Plaintiff and the putative class to have suffered actual damages. Nonetheless, Plaintiff and the putative class have suffered an invasion of a legally protected interest when Defendants secured their personal and private biometric data at a time when they had no right to do so, an invasion of Plaintiff's and the putative Class's right to privacy; an informational injury because Defendants did not provide them with information to which they were entitled by statute; and mental anguish when contemplating what would happen to their biometric data if and when Defendants go out of business, whether Defendants will ever delete their biometric information, and whether (and to whom) Defendants share their biometric information.

## II. STANDARD FOR CLASS CERTIFICATION

“The basic purpose of a class action is the efficiency and economy of litigation.” *CE Design Ltd. v. C & T Pizza, Inc.*, 2015 IL App. (1st) 131465, ¶ 9 (Ill. App. Ct. May 8, 2015) (citing *Miner v. Gillette Co.*, 87 Ill. 2d 7, 14 (1981)). “In determining whether to certify a proposed class, the trial court accepts the allegations of the complaint as true and should err in favor of maintaining class certification.” *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶ 9 (citing *Ramirez v. Midway Moving & Storage, Inc.*, 378 Ill. App. 3d 51, 53 (2007)). Under Section 2-801 of the Code of Civil Procedure, a class may be certified if the following four requirements are met:

- (1) the class is so numerous that a joinder of all members is impracticable;
- (2) there are questions of fact or law common to the class that predominate over any questions affecting only individual members;
- (3) the representative parties will fairly and adequately protect the interest of the class; and
- (4) the class action is an appropriate method for the fair and efficient adjudication of the controversy.

See *Smith v. Illinois Cent. R.R. Co.*, 223 Ill. 2d 441, 447 (2006) (citing 735 ILCS 5/2-801). Notably, “[a] trial court has broad discretion in determining whether a proposed class meets the requirements for class certification.” *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶ 9 (citing *Ramirez*, 378 Ill. App. 3d at 53). Here, the allegations and facts in this case amply demonstrate that the four certification factors are met.

## III. ARGUMENT

Plaintiff’s claims here are especially suited for class certification because Defendants treated all White Castle employees identically for the purposes of applying BIPA. All of the putative class members in this case were uniformly subjected to the same illegal and unlawful collection, storage, use, and dissemination of their biometric data that was required as a condition

of employment throughout the class period. Plaintiff meets each of the statutory requirements for maintenance of this suit as a class action. Thus, the class action device is ideally suited and is far superior to burdening the Court with many individual lawsuits to address the same issues, undertake the same discovery, and rely on the same testimony.

**A. The Class Is So Numerous That Joinder of All Members Is Impracticable.**

Numerosity is not dependent on a plaintiff setting forth a precise number of class members or a listing of their names. *See Cruz v. Unilock Chicago*, 383 Ill. App. 3d 752, 771 (2d Dist. 2008) (“Of course, plaintiffs need not demonstrate a precise figure for the class size, because a good-faith, non-speculative estimate will suffice; rather, plaintiffs need demonstrate only that the class is sufficiently numerous to make joinder of all of the members impracticable.”) (internal citations omitted); *Hayna v. Arby’s, Inc.*, 99 Ill. App. 3d 700, 710-11 (1st Dist. 1981) (“It is not necessary that the class representative name the specific individuals who are possibly members of the class.”). Courts in Illinois generally find numerosity when the class is comprised of at least 40 members. *See Wood River Area Dev. Corp. v. Germania Fed. Sav. Loan Ass’n*, 198 Ill. App. 3d 445, 450 (5th Dist. 1990).

In the present case, there can be no serious dispute that Plaintiff meets the numerosity requirement. The class of potential plaintiffs is sufficiently large to make joinder impracticable.<sup>2</sup> As a result of Defendants’ violations of BIPA, Plaintiff and all similarly-situated individuals were subjected to Defendants’ common and uniform policies and practices and were victims of Defendants’ schemes to unlawfully collect, store, use, and disseminate their extremely personal and private biometric data in direct violation of BIPA. As a result of Defendants’ violations of the

---

<sup>2</sup> Upon information and belief, White Castle employs hundreds of workers, many of whom are members of the class.



FILED DATE: 1/8/2019 2:36 PM 2018CH15233

Act, Plaintiff and all other similarly-situated individuals suffered an invasion of privacy as well as informational and personal injury. The precise number in the class cannot be determined until discovery records are obtained from Defendants. Nevertheless, class membership can be easily determined by reviewing Defendants' records. A review of Defendants' files regarding the collection, storage, use, and dissemination of White Castle employees' biometric data performed during the class period is all that is needed to determine membership in Plaintiff's proposed class. *See e.g., Chultem v. Ticor Title Ins. Co.*, 401 Ill. App. 3d 226, 233 (1st Dist. 2010) (reversing Circuit Court's denial of class certification and holding that class was certifiable over defendant's objection that "the proposed class was not ascertainable, because the process of reviewing defendant's transaction files to determine class membership would be burdensome"); *Young v. Nationwide Mut. Ins. Co.*, 693 F.3d 532, 539-40 (6th Cir. 2012)<sup>3</sup> (rejecting the argument that manual review of files should defeat certification, agreeing with district court's reasoning that, if manual review was a bar, "defendants against whom claims of wrongful conduct have been made could escape class-wide review due solely to the size of their businesses or the manner in which their business records were maintained," and citing numerous courts that are in agreement, including *Perez v. First Am. Title Ins. Co.*, 2009 WL 2486003, at \*7 (D. Ariz. Aug. 12, 2009) ("Even if it takes a substantial amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery")). Once Defendants' records are obtained, the Court will know the precise number of persons affected.

Absent certification of this class action, White Castle employees may never know that their legal rights have been violated, and as a result, may never obtain the redress to which they are

---

<sup>3</sup> "Section 2-801 is patterned after Rule 23 of the Federal Rules of Civil Procedure and, because of this close relationship between the state and federal provision, 'federal decisions interpreting Rule 23 are persuasive authority with regard to questions of class certification in Illinois.'" *Cruz*, 383 Ill. App. 3d at 761 (quoting *Avery v. State Farm Mutual Automobile Insurance Co.*, 216 Ill.2d 100, 125 (2005)).

entitled under BIPA. Illinois courts have noted that denial of class certification where members of the putative class have no knowledge of the lawsuit may be the “equivalent of closing the door of justice” on the victims. *Wood River Area Dev. Corp. v. Germania Fed. Sav. & Loan Assn.*, 198 Ill.App.3d 445, 452 (5th Dist. 1990). Further, recognizing the need to protect its citizens from harms such as identity theft, Illinois enacted BIPA specifically to regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information. A class action would help ensure that Plaintiff and all other similarly-situated individuals have a means of redress against Defendants for their widespread violations of BIPA.

**B. Common Questions Of Law And Fact Exist That Predominate Over Any Questions Solely Affecting Individual Members Of The Class.**

Courts analyze commonality and predominance under Section 2-801 by identifying the substantive issues that will control the outcome of the case. *See Bemis v. Safeco Ins. Co. of Am.*, 407 Ill. App. 3d 1164, 1167 (5th Dist. 2011); *Cruz*, 383 Ill. App. 3d at 773. The question then becomes whether those issues will predominate and whether they are common to the class, meaning that “favorable adjudication of the claims of the named plaintiffs will establish a right of recovery in other class members.” *Cruz*, 383 Ill. App. 3d at 773. As stated by the Court of Appeals, the question is will “common . . . issues be the subject of the majority of the efforts of the litigants and the court[?]” *Bemis*, 407 Ill. App. 3d at 1168. The answer here is “yes.”

At the heart of this litigation is Defendants’ culpable conduct under BIPA. The issues are simple and straightforward legal questions that plainly lend themselves to class-wide resolution. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregarded Plaintiff’s and other similarly-situated individuals’ statutorily-protected privacy rights and unlawfully collected, stored, used, and disseminated their biometric data in direct violation of BIPA. Specifically, Defendants have violated and continues to violate BIPA because they failed

and continue to fail to: (1) inform Plaintiff or the putative class in writing of the specific purpose(s) and length of time for which their fingerprints were being collected, stored, used, and disseminated as required by BIPA; (2) provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and the putative class's fingerprints, as required by BIPA; and (3) receive a written release from Plaintiff or the putative class to collect, capture, use or otherwise obtain their fingerprints, as required by BIPA. Defendants treated the entire proposed class in precisely the same manner, resulting in identical violations of BIPA. These common practices create common issues of law and fact. In fact, the legality of Defendants' collection, storage, use, and dissemination of White Castle employees' biometric data is the focus of this litigation.

Indeed, once this Court determines whether Defendants' practices of collecting, storing, and using individuals' biometric data without adhering to the specific requirements of BIPA constitutes violations thereof, liability for the claims of class members will be determined in one stroke. The material facts and issues of law are substantially the same for the members of the class, and therefore these common issues could be tried such that proof as to one claimant would be proof as to all members of the class. This alone establishes predominance. The only remaining questions will be whether Defendants' violations caused members of the class to suffer damages and the proper measure of damages and injunctive relief, which in and of themselves are questions common to the class. Accordingly, a favorable adjudication of the Plaintiff's claims in this case will establish a right of recovery to all other class members, and thus the commonality and predominance requirements weigh in favor of certification of the class.

**C. The Named Plaintiff And Class Counsel Are Adequate Representatives Of The Class.**

When evaluating adequacy, courts look to whether the named plaintiff has the same interests as those of the class and whether he or she will fairly represent them. *See CE Design Ltd.*,

FILED DATE: 1/18/2019 2:36 PM 2018CH15233

2015 IL App. (1st) 131465, ¶ 16. In this case, Plaintiff's interest arises from statute. The class representative, Latrina Cothron, is a member of the proposed class and will fairly and adequately protect the class's interests. Plaintiff, as a condition of employment, was required to have her fingerprints scanned to access her paystubs and company computers. Defendants subsequently stored Plaintiff's fingerprints in their database(s). Plaintiff has never been informed of the specific limited purposes (if any) or length of time for which any Defendant collected, stored, used, or disseminated her biometric data. Plaintiff has never been informed of any biometric data retention policy developed by any Defendant, nor has she ever been informed whether any Defendant will ever permanently delete her fingerprints. Finally, Plaintiff has never been provided, nor did she ever sign, a written release allowing any Defendant to collect, store, use, or disseminate her fingerprints. Thus, Plaintiff was a victim of the same uniform policies and practices of Defendants as the individuals she seeks to represent and is not seeking any relief that is potentially antagonistic to other members of the class. What is more, Plaintiff has the interests of those class members in mind, as demonstrated by her willingness to sue on a class-wide basis and step forward as the class representative, which subjects her to discovery. (*See* Exhibit A – Affidavit of Latrina Cothron). This qualifies her as a conscientious representative plaintiff and satisfies the adequacy of representation requirement.

Proposed Class Counsel, Stephan Zouras, LLP, will also fairly and adequately represent the class. Proposed Class Counsel are highly qualified and experienced attorneys. (*See* Exhibit B – Affidavit of Andrew C. Ficzkowski and the Firm Resume attached thereto as Exhibit 1). Stephan Zouras, LLP, are recognized attorneys in class action lawsuits and have been designated as class counsel in numerous class actions in state and federal courts. (*See* Exhibit B, Exhibit B-1). Thus,

proposed Class Counsel, too, are adequate and have the ability and resources to manage this lawsuit.

**D. A Class Action Is The Appropriate Method For Fair And Efficient Adjudication Of This Controversy.**

Finally, a class action is the most appropriate method for the fair and efficient adjudication of this controversy, rather than bringing individual suits which could result in inconsistent determinations and unjust results. “It is proper to allow a class action where a defendant is alleged to have acted wrongfully in the same basic manner toward an entire class.” *P.J.’s Concrete Pumping Service, Inc. v. Nextel West Corporation*, 345 Ill. App. 3d 992, 1003 (2d Dist. 2004). “The purported class representative must establish that a successful adjudication of its individual claims will establish a right of recovery or resolve a central issue on behalf of the class members.” *Id.*

Here, Plaintiff’s claims stem from Defendants’ common and uniform policies and practices, resulting in common violations of BIPA for all members of the class. Thus, class certification will obviate the need for unduly duplicative litigation that might result in inconsistent judgments concerning Defendants’ practices. *Wenthold v. AT&T Technologies, Inc.*, 142 Ill. App. 3d 612 (1st Dist. 1986). Without a class, the Court would have to hear dozens, if not hundreds, of additional individual cases raising identical questions of liability. Moreover, class members are better served by pooling resources rather than attempting to litigate individually. *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶¶ 28-30 (certifying TCPA class where statutory damages were alleged and rejecting arguments that individual lawsuits would be superior). In the interests of justice and judicial efficiency, it is desirable to concentrate the litigation of all class members’ claims in a single forum. For all of these reasons, the class action is the most appropriate mechanism to adjudicate the claims in this case.

**E. In The Event The Court Or Defendants Seeks More Factual Information Regarding This Motion, The Court Should Allow Supplemental And Deferred Briefing Following Discovery.**

There is no meaningful need for discovery for the Court to certify a class in this matter; Defendants' practices and policies are uniform. If, however, the Court wishes for the Parties to engage in discovery, the Court should keep the instant motion pending during the discovery period, allow Plaintiff a supplemental brief, and defer Defendants' response and Plaintiff's reply. Plaintiff is moving as early as possible for class certification in part to avoid the "buy-off problem," which occurs when a defendant seeks to settle with a class representative on individual terms in an effort to moot the class claims asserted by the class representative. Plaintiff is also moving for class certification now because the class should be certified, and because no meaningful discovery is necessary to establish that fact. The instant motion is far more than a placeholder or barebones memorandum. Rather, Plaintiff's full arguments are set forth based on the facts known at this extremely early stage of litigation. Should the Court wish for more detailed factual information, the briefing schedule should be extended.

**IV. Conclusion**

For the reasons stated above, Plaintiff respectfully requests that the Court enter an Order: (1) certifying Plaintiff's claims as a class action; (2) appointing Plaintiff Latrina Cothron as Class Representative; (3) appointing Stephan Zouras, LLP as Class Counsel; and (4) authorizing court-facilitated notice of this class action to the class. In the alternative, this Court should allow discovery, allow Plaintiff to supplement this briefing, and defer response and reply briefs.

Date: January 8, 2019

Respectfully Submitted,

/s/ Andrew C. Ficzko

Ryan F. Stephan

Andrew C. Ficzko

**STEPHAN ZOURAS, LLP**

100 North Riverside Plaza

Suite 2150

Chicago, Illinois 60606

312.233.1550

312.233.1560 *f*

Firm ID: 43734

aficzko@stephanzouras.com

**ATTORNEYS FOR PLAINTIFF**

FILED DATE: 1/8/2019 2:36 PM 2018CH15233



FILED DATE: 1/8/2019 2:36 PM 2018CH15233

**CERTIFICATE OF SERVICE**

I, the attorney, hereby certify that on January 8, 2019, I electronically filed the attached with the Clerk of the Court using the ECF system which will send such filing to all attorneys of record.

/s/ Andrew C. Ficzko

Return Date: No return date scheduled  
Hearing Date: 1/16/2019 9:30 AM - 9:30 AM  
Courtroom Number:  
Location:

FILED  
1/8/2019 2:36 PM  
DOROTHY BROWN  
CIRCUIT CLERK  
COOK COUNTY, IL  
2018CH15233

FILED DATE: 1/8/2019 2:36 PM 2018CH15233

## EXHIBIT A

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

**LATRINA COTHRON, individually,** )

**and on behalf of all others similarly situated,** )

**Plaintiff,** )

**v.** )

**WHITE CASTLE SYSTEM, INC. D/B/A** )

**WHITE CASTLE and CROSS MATCH** )

**TECHNOLOGIES, INC.,** )

**Defendant.** )

**Case No. 18-CH-15233**

**AFFIDAVIT OF LATRINA COTHRON**

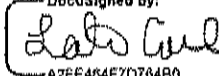
I, Latrina Cothron, being first duly cautioned, swear and affirm as follows:

1. I am over the age of 18 and competent to testify.
2. I am the Named Plaintiff and proposed Class Representative in this case.
3. I understand what it means to be a class representative. As a class representative, I am looking out for the interests of the other class members.
4. I do not have any conflicts with the class members because they were treated like I was with respect to this lawsuit. I have their interests in mind, as well as my own, in bringing this lawsuit.

FURTHER YOUR AFFIANT SAYETH NOT.

1/7/2019

Date: \_\_\_\_\_

DocuSigned by:  
  
AZF6464F7D784B0...

\_\_\_\_\_  
Latrina Cothron

Return Date: No return date scheduled  
Hearing Date: 1/16/2019 9:30 AM - 9:30 AM  
Courtroom Number:  
Location:

FILED  
1/8/2019 2:36 PM  
DOROTHY BROWN  
CIRCUIT CLERK  
COOK COUNTY, IL  
2018CH15233

FILED DATE: 1/8/2019 2:36 PM 2018CH15233

## EXHIBIT B

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

LATRINA COTHRON, individually, and on  
behalf of all others similarly situated,

Plaintiff,

v.

WHITE CASTLE SYSTEM, INC. D/B/A  
WHITE CASTLE and CROSS MATCH  
TECHNOLOGIES, INC.,

Defendants.

Case No. 2018-CH-15233

AFFIDAVIT OF ANDREW C. FICZKO

I, Andrew C. Ficzkco, being first duly cautioned, swears and affirms as follows:

1. I am one of Plaintiff's Counsel in the above-referenced matter.
2. I submit this Affidavit in support of Plaintiff's Amended Motion for Class Certification and Request for Discovery on Certification Issues.
3. I am a partner of the law firm of Stephan Zouras, LLP. Attached hereto as Exhibit 1 is a true and correct copy of the firm's resume.

FURTHER YOUR AFFIANT SAYETH NOT.

Date: January 8, 2019

Andrew C. Ficzkco

Subscribed and sworn to  
before me on this 8<sup>th</sup> day of  
January, 2019

Notary Public



FILED DATE: 1/8/2019 2:36 PM 2018CH15233

# EXHIBIT 1



100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1560  
stephanzouras.com

## FIRM PROFILE

**STEPHAN ZOURAS, LLP** is a law firm concentrating on helping people in class and individual civil litigation. The firm's attorneys have broad litigation, trial and appellate experience in the areas of wage and hour law and other employment disputes, mass torts and catastrophic personal injury, consumer protection, products liability and other complex litigation.

Our Chicago-based firm actively litigates cases in federal and state courts throughout the United States. The firm's two founding partners, James B. Zouras and Ryan F. Stephan, have successfully prosecuted claims ranging from individual wrongful death and other catastrophic injury cases to complex, multi-district class and collective actions on behalf of over one hundred thousand individuals against many of the largest corporations in the world.

## PRINCIPAL ATTORNEYS

**JAMES B. ZOURAS** is a founder and principal of Stephan Zouras, LLP. A 1995 graduate of DePaul University College of Law, Jim served as Editor of the Law Review, graduated in the top 10% of his class and was admitted to the Order of the Coif. Jim has helped thousands of people recover tens of millions of dollars in damages in individual and class actions arising under federal wage and hour laws including the Fair Labor Standards Act ("FLSA") and comparable state wage laws, other complex litigation, and catastrophic personal injury actions involving wrongful death, vehicle crashes, products liability, premises liability and construction negligence. Jim has been appointed lead or co-lead counsel on a large number of contested class actions throughout the United States. He has successfully tried over a dozen jury trials and argued over 14 appeals as lead appellate counsel before the federal and state appellate courts. In 2000, Jim was named among the *Chicago Daily Law Bulletin's* "Top 40 Lawyers Under Age 40," one of the youngest lawyers ever bestowed that honor. Jim and his cases have been profiled by numerous media outlets including the Chicago Tribune, the Chicago Sun-Times, Bloomberg BNA, Billboard Magazine and TMZ. Jim has also been interviewed by CBS Consumer Watch. Jim is frequently invited as a speaker at national class action litigation seminars.

**RYAN F. STEPHAN** is a founder and principal of Stephan Zouras, LLP. A 2000 graduate from Chicago Kent College of Law, Ryan has helped thousands of clients recover damages in cases involving unpaid overtime, employment disputes, business litigation, products liability and personal injury. Ryan has successfully tried cases to verdict including obtaining a \$9,000,000 verdict on behalf of 200 employees who were misclassified and denied overtime pay. Ryan has also served as lead or co-lead counsel on numerous complex class and collective action cases involving wage and hour matters and has helped recover damages for tens of thousands of wronged employees. In these cases, Ryan has helped establish precedent in wage and hour law, forced major corporations to change unlawful employment practices and helped recover tens of millions of dollars in unpaid wages for his clients. Ryan and his cases have been profiled by numerous media outlets including Good Morning America, Fortune, ESPN, Fox News, The Guardian, The New York Times, Think Progress, USA Today and Vice Sports.

Ryan and Jim are admitted to the United States Supreme Court as well as the Trial Bar of the United States District Court for the Northern District of Illinois. In addition, they have been admitted or admitted *pro hac vice* to prosecute class actions in the Southern and Eastern Districts of New York, the District of New Jersey, the Eastern and Middle Districts of Pennsylvania, the Western District of North Carolina, the Superior Court for the State of California, the Central District





100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1500  
stephanzouras.com

of Illinois, the District of Minnesota the Eastern District of Michigan, the Eastern District of Missouri, the District of Maryland, the Southern District of Ohio, the Northern, Middle and Southern Districts of Florida, the Northern District of Texas, the District of Massachusetts, the District of Minnesota, the First Judicial District of Pennsylvania, the Western District of Washington and the Southern and Northern Districts of Iowa.

In every consecutive year since 2009, *Chicago Magazine's* Super Lawyer Section selected both Jim and Ryan as two of the top attorneys in Illinois, a distinction given to no more than 5% of the lawyers in the state.

## PARTNERS

**ANDREW C. FICZKO** graduated from Drake University Law School in 2009. A tireless advocate for working people, Andy has spent his entire professional career litigating on behalf of employees in class and collective actions nationwide. Andy has helped thousands of clients recover damages in cases involving unpaid minimum and overtime wages and other benefits. Andy served as the second chair in two major federal jury trials to verdict on behalf of Plaintiffs in wage and hour matters and one state jury trial to verdict on behalf of Plaintiffs in a breach of contract matter.

Andy has been admitted to the Trial Bar of the United States District Court for the Northern District of Illinois since December 2012 and has been admitted or admitted *pro hac vice* to the Southern District of New York, the Southern and Northern Districts of Iowa, District of Massachusetts, Eastern District of Pennsylvania, and the Western District of Washington.

In 2014, 2015, and 2016 Andy was recognized by Chicago Magazine's Super Lawyer section as a Rising Star, a distinction given to no more than 2.5% of Illinois lawyers.

**TERESA M. BECVAR** is a 2013 graduate of Chicago-Kent College of Law, where she served as Editor of the Law Review and graduated in the top 15% of her class. Teresa assists Stephan Zouras, LLP clients with employment and consumer protection issues. Teresa has experience working on a wide range of employment cases, including wage and hour class and collective actions and employment discrimination cases. Teresa has been admitted *pro hac vice* to the Eastern and Southern Districts of New York, the Western District of Washington, the Middle District of Florida and the Central District of California.

In 2016, Teresa was recognized by Chicago Magazine's Super Lawyer section as a Rising Star, a distinction given to no more than 2.5% of Illinois lawyers.

## ASSOCIATE ATTORNEYS

**CATHERINE T. MITCHELL** graduated from The John Marshall Law School in 2015. Catherine litigates on behalf of Stephan Zouras, LLP's clients in both class action and individual litigation, representing people in a wide-range of legal disputes, including unpaid wages, employee misclassification, mass torts, antitrust, and consumer fraud. Catherine is an active member of the Women's Bar Association of Illinois and the Young Lawyers Society of the Chicago Bar Association, and served as a Chapter Editor for the Second Edition of BNA's Age Discrimination in Employment Act Treatise. Catherine is admitted to practice in Illinois, the District of Colorado, the Eastern District of Wisconsin and has been admitted *pro hac vice* to the Southern and Eastern District of New York, the District of Florida-Tampa Division, the Southern District



100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1560 | F 312-233-1560  
stephanzouras.com

of Iowa and the Eastern District of North Carolina.

**HALEY R. JENKINS** graduated *cum laude* from Chicago-Kent College of Law in 2016. Haley litigates on behalf of Stephan Zouras, LLP's clients in both class action and individual litigation. A spirited advocate, Haley represents clients in legal disputes involving unpaid wages, employee misclassification, antitrust, consumer fraud, whistleblower actions, and *qui tam* cases. She is currently a member of the legal team pursuing the first-ever lawsuit for minimum wage violations on behalf of the cheerleading squad of an NBA team. Haley is admitted to practice in Illinois and the District of Colorado and has been admitted *pro hac vice* to the Middle District of Pennsylvania.

## OF COUNSEL

**DAVID J. COHEN**, a highly skilled and successful class-action attorney, joined Stephan Zouras, LLP in April 2016 and manages our Philadelphia office. Dave has spent 22 years fighting to protect the rights of thousands of employees, consumers, shareholders, and union members. Before joining Stephan Zouras, Dave worked on, and ran, dozens of significant antitrust, consumer, employment and securities matters for four highly-regarded Philadelphia firms. Before joining the private sector, Dave completed a unique clerkship with the Hon. Stephen E. Levin in the Philadelphia Court of Common Pleas, during which he not only helped to develop a respected and efficient system for the resolution of the Court's class action cases, but also contributed to several well-regarded works on class actions. Dave earned a J.D. from the Temple University School of Law in 1994. While attending law school, Dave was awarded the Barristers Award for excellence in trial advocacy and worked as a teaching assistant for Hon. Legrome Davis (E.D. Pa.) as part of Temple's award-winning Integrated Trial Advocacy program. Dave graduated with honors from the University of Chicago in 1991.

Dave is admitted to practice in the United States Court of Appeals for the Third Circuit, the United States Court of Appeals for the Sixth Circuit, the United States District Court for the Eastern District of Pennsylvania, the United States District Court for the Middle District of Pennsylvania, the United States District Court for the Western District of Pennsylvania, the United States District Court for the District of New Jersey and the state courts of Pennsylvania and New Jersey. He is a member of the American and Philadelphia Bar Associations.

**PHILIP J. GIBBONS, JR.**, a highly-accomplished Plaintiff's class action attorney in his own right, joined Stephan Zouras, LLP in June 2017 and manages our Charlotte office. Phil focuses entirely on employment law, with an emphasis on helping employees recover unpaid wages including overtime. Phil began his legal career with a large national law firm, representing and counseling corporations and employers. Since 2001, Phil has exclusively represented employees. Phil is recognized by his peers as a highly skilled employment lawyer. He is listed in Best Lawyers in America and Super Lawyers. In addition, he has a perfect 10.0 rating on Avvo.com and an "A/V" rating with Martindale Hubble, which is the highest rating an attorney can receive. Phil has extensive experience litigating single and multi-plaintiff wage and hour lawsuits under the Fair Labor Standards Act, recovering unpaid overtime and minimum wages for thousands of employees throughout the United States.

Phil is admitted to practice in North Carolina, Indiana, Seventh Circuit Court of Appeals, Sixth Circuit Court of Appeals, Third Circuit Court of Appeals, Tenth Circuit Court of Appeals, U.S. District Courts Western District North Carolina, Middle District North Carolina, Southern District of Indiana, Northern District of Indiana, and Eastern District of Michigan.



100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1560  
stephanzouras.com

## REPRESENTATIVE TRIALS, VERDICTS AND JUDGMENTS

**Franco, et al. v. Ideal Mortgage Bankers, d/b/a Lend America** 12/14/17 – Trial Court Judgment  
*No. 07-cv-3956 (United States District Court for the Eastern District of New York)*

The Court entered a \$15.2 million judgment on behalf of several hundred loan officers who were deprived of minimum wages and overtime in violation of federal and state law.

**Frisari v. DISH Network** 8/25/16 – Arbitration Judgment  
*No. 18-160-001431-12 (AAA Arbitration)*

The Arbitrator certified and granted final judgment in excess of seven figures for a class of over 1,000 New Jersey inside sales associates who performed work before and/or after their shifts without pay and were not paid the proper overtime rate when they worked in excess of 40 hours a week.

**Huskey v. Ethicon Inc.** 9/10/2014 – Jury Verdict  
*No. 2:12-cv-05201 (United States District Court for the Southern District of West Virginia)*

Stephan Zouras, LLP helped secure a \$3,270,000.00 jury verdict in one of the bell-weather trial cases in the multi-district litigation against Johnson & Johnson's Ethicon unit for defective design, failure to warn and negligence related to transvaginal mesh device.

**Lee v. THR** 5/22/14 – Trial Court Judgment  
*No. 12-cv-3078 (United States District Court for the Central District of Illinois)*

As a result of the efforts of class counsel Stephan Zouras, LLP, the Court entered a judgment for a class of employees given job titles such as "Buyers," "Auditors" and "Managers" for unpaid overtime in the sum of \$12,207,880.84.

**Vilches et al. v. The Travelers Companies, Inc.** 12/12/12 - Arbitration Judgment  
*No. 11-160-000355-11 (American Arbitration Association)*

Following a contested evidentiary hearing, Stephan Zouras, LLP secured a significant monetary award on behalf of a group of insurance appraiser employees seeking unpaid earned overtime under the FLSA.

**Kyriakoulis, at al. v. DuPage Health Center** 11/8/12 - Jury Verdict  
*No. 10-cv-7902 (United States District Court for the Northern District of Illinois)*

Stephan Zouras, LLP achieved a favorable jury verdict on behalf of several medical assistants deprived of minimum and overtime wages in violation of federal and Illinois law.

**Smith v. Safety-Kleen Systems, Inc.** 7/11/12 - Jury Verdict  
*No. 10-cv-6574 (United States District Court for the Northern District of Illinois)*

Stephan Zouras, LLP achieved a favorable jury verdict on behalf of a chemical handler deprived of overtime wages in this donning and doffing action brought under the FLSA.

**Wong v. Wice Logistics** 1/30/12 - Jury Verdict  
*No. 08 L 13380 (Circuit Court of Cook County, Illinois)*

Stephan Zouras, LLP recovered unpaid commissions and other damages for Plaintiff based on her claims under the Illinois Wage Payment and Collection Act.

FILED DATE: 1/8/2019 2:36 PM 2018CH15233



100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1560  
stephanzouras.com

**Daniels et al. v. Premium Capital Financing** **10/18/11 - Jury Verdict**  
*No. 08-cv-4736 (United States District Court for the Eastern District of New York)*  
Stephan Zouras, LLP were appointed lead class and trial counsel and achieved a jury verdict in excess of \$9,000,000.00 on behalf of over 200 loan officers who were deprived of minimum wages and overtime pay.

**Ferrand v. Lopas** **5/22/01 - Jury Verdict**  
*No. 00 L 2502 (Circuit Court of Cook County, Law Division, State of Illinois)*  
Jury verdict in excess of available liability insurance policy limits entered in favor of seriously-injured pedestrian, resulting in liability against insurance carrier for its bad faith refusal to tender the policy limits before trial.

## REPRESENTATIVE RESOLVED CLASS AND COLLECTIVE ACTIONS

Courts have appointed the firm's partners as lead or co-lead counsel in numerous class and collective actions in which they achieved six, seven and eight-figure verdicts or settlements including:

**Eggleston v. USCC Services, LLC.** **2/16/18 – Final Approval**  
*No. 16-cv-06775 (United States District Court for the Northern District of Illinois)*  
As co-lead counsel, Stephan Zouras, LLP helped obtain final approval of a \$1,250,000 class settlement for unpaid overtime wages on behalf of misclassified Sales Managers.

**Caison v. Sogeti USA, LLC, et al.** **2/12/18 – Final Approval**  
*No. 17-cv-2786 (United States District Court for the Northern District of Illinois)*  
As lead counsel, Stephan Zouras, LLP achieved a class wide settlement on behalf of hundreds of Business Analysts who worked in excess of 40 hours per week and were not paid proper overtime compensation.

**Kaminski v. Bank of America, N.A.** **2/15/18 – Final Approval**  
*No. 16-cv-10844 (United States District Court for the Northern District of Illinois)*  
Final approval for class settlement in the amount of \$850,000 in unpaid wages was granted and awarded to a class of approximately 100 employees working as Senior Specialist-Securities and Operation Market Professionals.

**Byrne v. Centegra Health System** **1/29/18 – Final Approval**  
*No. 17-cv-00018 (United States District Court for the Northern District of Illinois)*  
The Court granted final approval of class settlement for \$425,000 in unpaid overtime wages on behalf of registered nurses, physical therapists, occupational therapists, speech therapists and other similarly-designated skilled care positions who were misclassified as exempt under federal and state wage laws.

**Donoghue v. Verizon Communications, Inc.** **11/16/17 – Final Approval**  
*No. 16-cv-4742 (United States District Court for the Eastern District of Pennsylvania)*  
The Court granted final approval of class settlement for \$800,000 in unpaid overtime wages on behalf of wireline workers who were hired to fill in for Verizon employees during a strike. Despite regularly working 65 hours per week, these employees were classified as exempt and denied overtime wages.

**Tompkins v. Farmers Insurance Exchange** **9/27/17 – Final Approval**  
*No. 14-cv-3737 (United States District Court for the Eastern District of Pennsylvania)*  
The Court granted final approval of a \$775,000.00 class settlement on behalf misclassified loan officers seeking unpaid overtime wages.



**STEPHANZOURAS, LLP**  
ATTORNEYS AT LAW

100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1550  
stephanzouras.com

**In re Sears Holdings Corporation Stockholder and Derivative Litigation**

**5/9/17 – Final Approval**

***No. 11081-VCL (Court of Chancery of the State of Delaware)***

Stephan Zouras, LLP represented the Named Plaintiff in a \$40 million settlement in connection with a 2015 sale by Sears of 235 properties to Seritage Growth Properties.

**Oaks v. Sears**

**4/12/17 – Final Approval**

***No. 1:15-cv-11318 (United States District Court for the Northern District of Illinois)***

Stephan Zouras, LLP settled on behalf of thousands of consumers who own or once owned Sears Kenmore grills in a product defect class action.

**Hauser v. Alexian Brothers Home Health**

**4/06/17 – Final Approval**

***No. 15-cv-6462 (United States District Court for the Northern District of Illinois)***

Stephan Zouras, LLP settled for \$1 million on behalf of home health care clinicians who were misclassified as "exempt" and deprived of earned overtime wages.

**Leiner v. Johnson & Johnson**

**1/31/17 – Final Approval**

***No. 15-cv-5876 (United States District Court for the Northern District of Illinois)***

The Court granted final approval of a \$5 million settlement for consumers nationwide in a consumer fraud class action. Stephan Zouras, LLP represented consumers who were deceived into paying premium prices for Johnson & Johnson baby bedtime products which falsely claimed to help babies sleep better.

**McPhearson v. 33 Management**

**11/3/16 – Final Approval**

***No. 15-ch-17302 (Circuit Court of Cook County, IL)***

The Court granted final approval of class settlement on behalf of tenants of a Chicago apartment building where the landlords violated the City of Chicago Residential Landlord and Tenant Ordinance by collecting and holding tenant security deposits without paying interest earned.

**Cook v. Bank of America**

**8/2/16 – Final Approval**

***No. 15-cv-07718 (United States District Court for the Northern District of Illinois)***

The Court granted final approval of \$3,250,000 settlement for an Illinois Class and FLSA Collective on behalf of individuals who worked as Treasury Services Advisors and who were misclassified as exempt from earned overtime wages.

**Altnor v. Preferred Freezer Services, Inc.**

**7/18/16 – Final Approval**

***No. 14-cv-7042 (United States District Court for the Eastern District of Pennsylvania)***

The firm's attorneys served as lead counsel in this lawsuit seeking recovery of wages for unpaid meal break work for a class of 80 cold storage warehouse workers.

**Lukas v. Advocate Health Care**

**6/29/16 – Final Approval**

***No. 14-cv-2740 (United States District Court for the Northern District of Illinois)***

The Court granted final approval of a \$4,750,000 settlement for a federal FLSA and Illinois Minimum Wage Law collective class of home health care clinicians who were wrongly classified as "exempt" from federal and state overtime laws.

**Kurgan v. Chiro One Wellness Centers LLC**

**4/27/16 – Final Approval**

***No. 10-cv-1899 (United States District Court for the Northern District of Illinois)***

The Court granted Plaintiffs' motion for Section 216(b) certification of Plaintiffs' FLSA claim, granted Rule 23 certification of Plaintiffs' claims under the Illinois Minimum Wage Law and appointed Stephan Zouras, LLP as counsel for a class of chiropractic technicians and assistants.

FILED DATE: 1/8/2019 2:36 PM 2018CH15233

# STEPHANZOURAS LLP

ATTORNEYS AT LAW

100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1560 | F 312-233-1560  
stephanzouras.com

FILED DATE: 1/18/2019 2:36 PM 2018CH15233

- Heba v. Comcast** **4/6/16 – Final Approval**  
*No. 12-471 (First Judicial District of Pennsylvania Court of Common Pleas of Philadelphia)*  
The Court granted class certification to Customer Account Executives who worked at Comcast's Pennsylvania call centers and were required to work 15 minutes a day before their scheduled start time without pay. As lead counsel, Stephan Zouras, LLP achieved a favorable resolution for over 6,000 class members.
- Johnson v. Casey's General Stores, Inc.** **3/3/16 – Final Approval**  
*No. 15-cv-3086 (United States District Court for the Western District of Missouri)*  
The Court granted final approval on behalf of a certified class of employees of Casey's General Stores, Inc. to redress violations of the Fair Credit Reporting Act (FCRA).
- Fields v. Bancsource, Inc.** **2/3/16 – Final Approval**  
*No. 14-cv-7202 (United States District Court for the Northern District of Illinois)*  
The Court entered an order granted Plaintiffs' motion for Section 216(b) certification of a class of field engineers who were deprived of overtime for hours worked in excess of 40 in given workweeks.
- Elder, et al. v. Comcast Corporation** **1/11/16 – Final Approval**  
*No. 12-cv-1157 (United States District Court for the Northern District of Illinois)*  
The Court granted Plaintiffs' motion for conditional certification and appointed Stephan Zouras, LLP as counsel for a class of cable technicians who allege they were deprived of overtime wages in violation of federal law.
- Posada, et al. v. Continental Home Loans, Inc.** **1/13/16 – Final Approval**  
*15-cv-4203 (United States District Court for the Eastern District of New York)*  
Stephan Zouras, LLP was appointed class counsel and achieved a substantial settlement on behalf of a class of loan officers deprived of minimum and overtime wages.
- Struett v. Susquehanna Bank** **10/27/15 – Final Approval**  
*No. 15-cv-176 (United States District Court for the Eastern District of Pennsylvania)*  
The firm's attorneys served as co-lead counsel in this lawsuit which recovered \$300,000 in unpaid overtime wages for 31 misclassified loan officers.
- Faust, et al. v. Comcast Corporation** **10/11/15 – Final Approval**  
*No. 10-cv-2336 (United States District Court for the Northern District of Maryland)*  
The Court granted Plaintiffs' motion for conditional certification and appointed Stephan Zouras, LLP lead counsel for a class of call center employees.
- Butler, et al. v. Direct Sat** **9/3/15 – Final Approval**  
*No. 10-cv-08747 DKC (United States District Court for the District of Maryland)*  
Stephan Zouras, LLP reached favorable resolution on behalf of a finally-certified collective class of technicians working in DirectSat's Maryland warehouses who were not paid overtime.
- Sosnicki v. Continental Home Loans, Inc.** **7/30/15 – Final Approval**  
*No. 12-cv-1130 (United States District Court for the Eastern District of New York)*  
As lead class counsel, Stephan Zouras, LLP achieved a six-figure settlement on behalf of a collective class of loan officers who were deprived of minimum wages and overtime in violation of federal and state law.
- Bordell v. Gelsinger Medical Center** **4/8/15 – Final Approval**  
*No. 12-cv-1688 (Northumberland Court of Common Pleas)*

# STEPHANZOURAS, LLP

ATTORNEYS AT LAW

100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1560 | F 312-233-1560  
stephanzouras.com

The firm's attorneys served as lead counsel in this lawsuit which challenged Defendant's workweek averaging practices and recovered \$499,000 in unpaid overtime wages for hospital workers.

**Harvey, et al. v. AB Electrolux, et al.**

**3/23/15 – Final Approval**

**No. 11-cv-3036 (United States District Court for the Northern District of Iowa)**

As lead counsel, Stephan Zouras, LLP achieved a six-figure settlement amount on behalf of hundreds of production workers seeking unpaid earned wages.

**Price v. NCR Corporation**

**3/18/15 – Final Approval**

**No. 51-610-908-12 (AAA Arbitration)**

As lead class counsel, Stephan Zouras, LLP achieved a seven figure, arbitrator approved settlement on behalf of thousands of Customer Engineers nationwide who were deprived overtime wages in violation of federal law.

**Frebes, et al. v. Mask Restaurants, LLC**

**1/15/15 – Final Approval**

**No. 13-cv-3473 (United States District Court for the Northern District of Illinois)**

Stephan Zouras, LLP was appointed class counsel and achieved a substantial settlement on behalf of hundreds of servers, bartenders and bussers forced to participate in an illegal "tip pool."

**Jones v. Judge Technical Services Inc.**

**12/15/14 – Final Approval**

**No. 11-cv-6910 (United States District Court for the Eastern District of Pennsylvania)**

As lead class counsel, Stephan Zouras, LLP prevailed on summary judgment and subsequently achieved a seven-figure settlement on behalf of IT workers who were designated under the "Professional Day" or "Professional Week" compensation plan, misclassified as exempt from the FLSA and denied overtime pay.

**Howard, et al. v. Securitas Security Services USA, Inc.**

**5/7/14 – Final Approval**

**No. 08-cv-2746 (United States District Court for the Northern District of Illinois)**

**and Hawkins v. Securitas Security Services USA, Inc.**

**No. 09-cv-3633 (United States District Court for the Northern District of Illinois)**

For settlement purposes, the Court certified a class of approximately ten thousand security guards seeking damages for unpaid wages and overtime under the FLSA and Illinois Minimum Wage Law.

**Thomas v. Matrix Corporation Services**

**2/12/14 – Final Approval**

**No. 10-cv-5093 (United States District Court for the Northern District of Illinois)**

As lead counsel, Stephan Zouras, LLP achieved a six-figure settlement on behalf of a class of hundreds of technicians who allege they were deprived of overtime wages in violation of federal law.

**Ingram v. World Security Bureau**

**12/17/13 – Final Approval**

**No. 11-cv-6566 (United States District Court for the Northern District of Illinois)**

Stephan Zouras secured a class settlement on behalf of several hundred security officers deprived of minimum wages and overtime in violation of federal and state law.

**Sexton v. Franklin First Financial**

**9/30/13 – Final Approval**

**No. 08-cv-04950 (United States District Court for the Eastern District of New York)**

Stephan Zouras, LLP achieved a settlement on behalf of a class of approximately 150 loan officers deprived of minimum wages and overtime in violation of the FLSA.

FILED DATE: 1/8/2019 2:36 PM 2018CH15233



# STEPHANZOURAS, LLP

ATTORNEYS AT LAW

100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1550  
stephanzouras.com

**Outlaw v. Secure Health, L.P.**

**9/24/13 – Final Approval**

**No. 11-cv-602 (United States District Court for the Eastern District of Pennsylvania)**

The firm's attorneys served as lead counsel in this lawsuit seeking recovery of wages for unpaid pre-shift, meal break and uniform maintenance work for a class of 35 nursing home workers.

**Robinson v. RCN Telecom Services, Inc.**

**8/5/13 – Final Approval**

**No. 10-cv-6841 (United States District Court for the Eastern District of Pennsylvania)**

The firm's attorneys served as co-lead counsel in this lawsuit which recovered \$375,000 in unpaid overtime wages for misclassified cable television installers.

**Holland v. Securitas Security Services USA, Inc.**

**7/26/13 – Final Approval**

**No. BC 394708 (Superior Court of California, County of Los Angeles)**

As class counsel, Stephan Zouras, LLP achieved a six figure settlement on behalf of thousands of security officers who allege they were deprived of overtime wages in violation of federal law.

**Jankuski v. Heath Consultants, Inc.**

**7/2/13 – Final Approval**

**No. 12-cv-04549 (United States District Court for the Northern District of Illinois)**

Stephan Zouras, LLP was appointed lead counsel and achieved a settlement on behalf of gas management technicians deprived of minimum wages and overtime in violation of the FLSA.

**Ord v. First National Bank of Pennsylvania**

**6/21/13 – Final Approval**

**No. 12-cv-766 (United States District Court for the Western District of Pennsylvania)**

The firm's attorneys served as co-lead counsel in this consumer fraud lawsuit which recovered \$3,000,000 for consumers who had been made to pay improper overdraft fees.

**Holley v. Erickson Living Management, LLC**

**6/13/13 – Final Approval**

**No. 11-cv-2444 (United States District Court for the Eastern District of Pennsylvania)**

The firm's attorneys served as lead counsel in this lawsuit seeking recovery of wages for unpaid pre-shift and meal break work for a class of 63 nursing home workers.

**Hansen, et al. v. Per Mar Security Services**

**5/15/13 – Final Approval**

**No. 09-cv-459 (United States District Court for the Southern District of Iowa)**

Stephan Zouras, LLP was appointed class counsel and secured a settlement for hundreds of security guards deprived of minimum wages and overtime in violation of federal and state law.

**Pomphrett v. American Home Bank**

**3/14/13 – Final Approval**

**No. 12-cv-2511 (United States District Court for the Eastern District of Pennsylvania)**

The firm's attorneys served as co-lead counsel in this lawsuit which recovered \$2,400,000 in unpaid overtime wages for misclassified loan officers.

**Murphy v. Rayan Brothers, et al.**

**2/22/13 – Final Approval**

**No. 11 CH 03949 (Circuit Court of Cook County, Chancery Division, State of Illinois)**

Stephan Zouras, LLP achieved class wide recovery on behalf of a class of tenants for violations of the Chicago Residential Landlord and Tenant Ordinance (RLTO).

FILED DATE: 1/8/2019 2:36 PM 2018CH15233

**STEPHANZOURAS LLP**  
ATTORNEYS AT LAW

100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1560  
stephanzouras.com

**Glatts v. Crozer-Keystone Health System**

**2/6/13 – Final Approval**

*No. 0904-1314 (Philadelphia Court of Common Pleas)*

The firm's attorneys served as co-lead counsel in this lawsuit which challenged Defendant's workweek averaging practices and recovered \$1,200,000 in unpaid overtime wages for hospital workers.

**Chambers v. Front Range Environmental, LLC**

**1/23/13 – Final Approval**

*No. 12-cv-891 (United States District Court for the Northern District of Illinois)*

Stephan Zouras, LLP was appointed as class counsel and resolved this action on behalf of a class of maintenance workers.

**Piehl v. Baytree National Bank**

**1/3/13 – Final Approval**

*No. 12-cv-1364 (United States District Court for the Northern District of Illinois)*

Stephan Zouras, LLP was appointed class counsel and resolved this action on behalf of a class of Indiana loan officers who were paid on a commission-only basis and deprived of earned minimum wage and overtime in violation of the FLSA.

**Searson v. Concord Mortgage Corporation**

**11/19/12 – Final Approval**

*No. 07-cv-3909 (United States District Court for the Eastern District of New York)*

Stephan Zouras, LLP achieved a settlement on behalf of a class of 80 loan officers deprived of minimum wages and overtime in violation of the FLSA.

**Ellenbecker, et al. v. North Star Cable Construction, Inc., et al.**

**11/14/12 – Final Approval**

*No. 09-cv-7293 (United States District Court for the Northern District of Illinois)*

Stephan Zouras, LLP obtained Rule 23 certification, were appointed lead counsel, and achieved a significant monetary resolution for a class of several hundred cable technicians seeking unpaid overtime wages and the recovery of improper deductions from their pay.

**Williams, et al. v. Securitas Security Services USA, Inc.**

**11/8/12 – Final Approval**

*No. 10-cv-7181 (United States District Court for the Eastern District of Pennsylvania)*

As lead class counsel, Stephan Zouras, LLP achieved a settlement on behalf of a class of Pennsylvania security guards who were not paid for all time spent in training and orientation.

**Lacy, et al. v. The University of Chicago Medical Center**

**11/6/12 – Final Approval**

*No. 11-cv-5268 (United States District Court for the Northern District of Illinois)*

As lead class counsel, Stephan Zouras, LLP achieved a FLSA settlement for a collective class of hospital respiratory therapists.

**Molyneux, et al. v. Securitas Security Services USA, Inc.**

**11/5/12 – Final Approval**

*No. 10-cv-588 (United States District Court for the Southern District of Iowa)*

As lead class counsel, Stephan Zouras achieved a settlement on behalf of a class of Iowa and Wisconsin security guards who were not paid for all time spent in training and orientation.

**Davis v. TPI Iowa, LLC**

**9/6/12 – Final Approval**

*No. 11-cv-233 (United States District Court for the Southern District of Iowa)*

As class counsel, Stephan Zouras, LLP achieved a settlement on behalf of a collective class of production employees.

**Kernats, et al. v. Comcast Corporation**

**5/28/12 – Final Approval**

*No. 09-cv-3368 (United States District Court for the Northern District of Illinois)*

FILED DATE: 1/18/2019 2:36 PM 2018CH15233

**STEPHANZOURAS LLP**  
ATTORNEYS AT LAW

100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1560  
stephanzouras.com

As lead class counsel, Stephan Zouras, LLP achieved a seven-figure settlement on behalf of over 7,500 Customer Account Representatives (CAEs) for unpaid wages in a Rule 23 class action brought under Illinois wage law.

**Garcia, et al. v. Loffredo Fresh Produce Co., Inc.**

**5/24/12 - Final Approval**

*No. 11-cv-249 (United States District Court for the Southern District of Iowa)*

As class counsel, Stephan Zouras, LLP achieved a settlement on behalf of a collective class of produce processing employees.

**Larsen, et al. v. Clearchoice Mobility, Inc., et al.**

**3/21/12 - Final Approval**

*No. 11-cv-1701 (United States District Court for the Northern District of Illinois)*

Stephan Zouras, LLP achieved an FLSA settlement on behalf of a collective class of retail sales consultants.

**Etter v. Trinity Structural Towers**

**1/26/12 - Final Approval**

*No. 11-cv-249 (United States District Court for the Southern District of Iowa)*

As class counsel, Stephan Zouras, LLP achieved a settlement on behalf of a collective class of production employees.

**Petersen, et al v. Marsh USA, Inc. et al.**

**9/21/11 - Final Approval**

*No. 10-cv-1506 (United States District Court for the Northern District of Illinois)*

Stephan Zouras, LLP achieved a six-figure settlement on behalf of over 30 analysts who claimed they were misclassified under the FLSA.

**Thompson v. World Alliance Financial Corp.**

**8/5/11 - Final Approval**

*No. 08-cv-4951 (United States District Court for the Eastern District of New York)*

Stephan Zouras, LLP were appointed lead counsel and achieved a settlement on behalf of a class of over one hundred loan officers deprived of minimum wages and overtime in violation of federal and state law.

**Vaughan v. Mortgage Source LLC, et al.**

**6/16/11 - Final Approval**

*No. 08-cv-4737 (United States District Court for the Eastern District of New York)*

Stephan Zouras, LLP were appointed lead counsel and achieved a settlement on behalf of a class of loan officers deprived of minimum wages and overtime in violation of federal and state law.

**Harris, et al. v. Cheddar's Casual Cafe, Inc.**

**6/1/11 - Final Approval**

*No. 51 460 00557 10 (AAA Arbitration)*

Stephan Zouras served as lead counsel in six-figure class settlement on behalf of over 100 restaurant workers deprived of minimum wages and overtime.

**Turner v. Mercy Health System**

**4/20/11 - Final Approval**

*No. 0801-3670 (Philadelphia Court of Common Pleas)*

The firm's attorneys served as co-lead counsel in this lawsuit which challenged Defendant's workweek averaging practices and, in a case of first impression, recovered \$2,750,000 in unpaid overtime wages for hospital workers.

**Brown et al. v. Vision Works, et al.**

**3/4/11 - Final Approval**

*No. 10-cv-01130 (United States District Court for the Northern District of Illinois)*

As lead class counsel, Stephan Zouras, LLP achieved a settlement on behalf of retail store managers improperly classified as exempt from overtime.

FILED DATE: 1/8/2019 2:36 PM 2018CH15233

# STEPHANZOURAS, LLP

ATTORNEYS AT LAW

100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1560  
stephanzouras.com

**Havard v. Osceola Foods, Inc., et al.**

**2/28/11 - Final Approval**

**No. LA CV 0111290 (Iowa District for Clarke County, Iowa)**

As lead class counsel, Stephan Zouras, LLP achieved a class settlement on behalf of meat processing plant employees who were not properly paid for donning and doffing activities performed before their shifts, during meal breaks and after their shifts.

**Lagunas v. Cargill Meat Solutions Corp.**

**1/27/11 - Final Approval**

**No. 10-cv-00220 (United States District Court for the Southern District of Iowa)**

Stephan Zouras, LLP served as co-lead counsel in class settlement on behalf of meat processing plant employees who were not properly paid for donning and doffing activities performed before their shifts, during meal breaks and after their shifts.

**Anderson v. JCG Industries, Inc.**

**9/2/10 - Final Approval**

**No. 09-cv-1733 (United States District Court for the Northern District of Illinois)**

As lead class counsel, Stephan Zouras, LLP achieved a six-figure settlement on behalf of meat processing plant employees who were not properly paid for time worked before their shifts, during meal breaks and after their shifts.

**Cedeno, et al. v. Home Mortgage Desk, Corp., et al.**

**6/15/10 - Final Approval**

**No. 08-cv-1168 (United States District Court for the Eastern District of New York)**

Stephan Zouras, LLP along with co-counsel was appointed lead counsel and achieved a six-figure settlement on behalf of a Section 216(b) collective class of loan officers deprived of overtime wages.

**Perkins, et al. v. Specialty Construction Brands, Inc.**

**11/15/09 - Final Approval**

**No. 09-cv-1678 (United States District Court for the Northern District of Illinois)**

As lead class counsel, Stephan Zouras, LLP achieved a six-figure wage and hour settlement on behalf of a collective class of plant employees for claims of unpaid overtime, including time worked before the start of their shifts, during breaks and after the end of their shifts.

**Wineland, et al. v. Casey's General Stores, Inc.**

**10/22/09 - Final Approval**

**No. 08-cv-00020 (United States District Court for the Southern District of Iowa)**

Stephan Zouras, LLP along with co-counsel was appointed lead counsel and achieved a seven-figure settlement on behalf of a Section 216(b) collective class and Rule 23 class of over 10,000 cooks and cashiers for unpaid wages, including time worked before and after their scheduled shifts and while off-the-clock.

**Jones, et al. v. Casey's General Stores, Inc.**

**10/22/09 - Final Approval**

**No. 07-cv-400 (United States District Court for the Southern District of Iowa)**

Stephan Zouras, LLP along with co-counsel was appointed lead counsel and achieved a seven-figure settlement on behalf of a Section 216(b) collective class and Rule 23 class of assistant store managers for unpaid wages, including time worked before and after their scheduled shifts and while off-the-clock.

**Stuart, et al. v. College Park, et al.**

**12/11/07 - Final Approval**

**No. 05 CH 09699 (Circuit Court of Cook County, Chancery Division, State of Illinois)**

The firm's partners served as co-lead counsel in this case brought on behalf of a class of tenants who were seeking the refund of their security deposits. As a result of their efforts, Mr. Stephan and Mr. Zouras helped achieve a six-figure settlement on behalf of a class of over 100 tenants.

FILED DATE: 1/18/2019 2:36 PM 2018CH15233

# STEPHANZOURAS, LLP

ATTORNEYS AT LAW

100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1560  
stephanzouras.com

## **Huebner et al. v. Graham C Stores**

**11/15/07 - Final Approval**

***No. 06 CH 09695 (Circuit Court of Cook County, Chancery Division, State of Illinois)***

Ryan Stephan of Stephan Zouras, LLP served as co-lead counsel in this wage and hour case involving claims for unpaid wages by a class of gas station employees. Mr. Stephan helped achieve a six-figure settlement for over 100 employees.

## **Perez, et al. v. RadioShack Corporation**

**9/14/07 - Final Approval**

***No. 02-cv-7884 (United States District Court for Northern District of Illinois)***

The firm's partners served as co-lead counsel in this nationwide Fair Labor Standards Act ("FLSA") overtime action brought on behalf of 4,000 retail store managers. Plaintiffs claimed they were improperly classified as exempt from the FLSA and owed overtime compensation for all hours worked in excess of 40 each week. In a case of first impression, the Court granted summary judgment in favor of a sub-class of Plaintiffs who did not "regularly and customarily" supervise at least 80 hours of subordinate time per week at least 80% of the time as required by the executive exemption of the FLSA. The reported decision is *Perez v. RadioShack Corp.*, 386 F. Supp. 979 (N.D. Ill. 2005). As a result of the efforts of Plaintiffs' counsel, Plaintiffs obtained a nearly \$9 million settlement on the eve of trial.

## **Reinsmith, et al. v. Castlepoint Mortgage**

**4/3/07 - Final Approval**

***No. 05-cv-01168 (United States District Court, Eastern District of Massachusetts)***

The firm's partners served as co-lead counsel in this action brought on behalf of a collective class of loan officers seeking to recover unpaid overtime. Mr. Stephan and Mr. Zouras helped achieve a seven-figure settlement on behalf of over 100 loan officers in this case.

## **Kutcher, et al. v. B&A Associates**

**11/20/06 - Final Approval**

***No. 03 CH 07610 (Circuit Court of Cook County, Chancery Division, State of Illinois)***

The firm's partners served as co-lead counsel in this case brought on behalf of a class of tenants who were seeking damages based on alleged security deposit violations. As a result of their efforts, Mr. Stephan and Mr. Zouras helped achieve a six-figure settlement on behalf of a class of over 100 tenants.

## **Ciesla, et al. v. Lucent Technologies, Inc.**

**7/31/06 - Final Approval**

***No. 05-cv-1641 (United States District Court for the Northern District of Illinois)***

The firm's partners served as co-lead counsel in this breach of contract class action against a high-tech communications company. Mr. Stephan and Mr. Zouras helped obtain a seven-figure settlement on behalf of the class.

## **Casale, et al. v. Provident Bank**

**7/25/05 - Final Approval**

***No. 04-cv-2009 (United States District Court for the District of New Jersey)***

The firm's partners served as co-lead counsel in this case brought on behalf of a collective class of over 100 loan officers who were seeking damages based on wage and hour violations of the FLSA. As a result of their efforts, Mr. Stephan and Mr. Zouras helped achieve a seven-figure settlement on behalf of the Plaintiffs.

## **Corbin, et al. v. Barry Realty**

**3/22/05 - Final Approval**

***No. 02 CH 16003 (Circuit Court of Cook County, Chancery Division, State of Illinois)***

The firm's partners served as co-lead counsel in this case brought on behalf of a class of tenants who were seeking the refund and interest on their security deposits as called for by the Chicago Residential Landlord Tenant Ordinance. As a result of their efforts, Mr. Stephan and Mr. Zouras helped achieve a six-figure settlement on behalf of a class of over 100 tenants.

FILED DATE: 1/8/2019 2:36 PM 2018CH15233





100 North Riverside Plaza, Suite 2150  
Chicago, Illinois 60606  
P 312-233-1550 | F 312-233-1560  
stephanzouras.com

## BIOMETRIC INFORMATION PRIVACY CLASS ACTION LAWSUITS

Our firm is at the forefront of BIPA litigation to protect the biometric data and privacy of employees and consumers. We have brought numerous class action lawsuits against employers and other retail businesses who have collected biometric data without consent and without instituting the proper safeguards including;

- **Doporczyk, et al. v. Mariano's**  
*No. 17-cv-05250 (United States District Court for the Northern District of Illinois)*
- **Dixon, et al. v. Smith Senior Living**  
*No. 17-cv-08033 (United States District Court for the Northern District of Illinois)*
- **Fields, et al. v. Abra Auto Body & Glass**  
*No. 17-CH-12271 (Circuit Court of Cook County, Chancery Division, State of Illinois)*
- **Goings, et al. v. Applied Acoustics**  
*No. 17-CH-14954 (Circuit Court of Cook County, Chancery Division, State of Illinois)*
- **Liu, et al. v. Four Seasons**  
*No. 17-CH-14949 (Circuit Court of Cook County, Chancery Division, State of Illinois)*
- **Mims, et al. v. Hilton**  
*No. 17-CH-15781 (Circuit Court of Cook County, Chancery Division, State of Illinois)*
- **Morris, et al. v. Wow Bao**  
*No. 17-CH-12029 (Circuit Court of Cook County, Chancery Division, State of Illinois)*
- **Ogen, et al. v. Wyndham Hotels & Resorts**  
*No. 17-CH-15626 (Circuit Court of Cook County, Chancery Division, State of Illinois)*
- **Watts, et al. v. Chicago Lakeshore Hospital**  
*No. 17-cv-07713 (United States District Court for the Northern District of Illinois)*
- **Williams, et al. v. Rockford Tool**  
*No. 17-CH-000770 (Circuit Court of Winnebago County, Chancery Division, State of Illinois)*

FILED DATE: 1/8/2019 2:36 PM 2018CH15233

# **EXHIBIT 3**





[Department of State](#) / [Division of Corporations](#) / [Search Records](#) / [Detail By Document Number](#) /

## Detail by Entity Name

Foreign Profit Corporation

CROSS MATCH TECHNOLOGIES, INC.

### Filing Information

<b>Document Number</b>	F02000002124
<b>FEI/EIN Number</b>	65-0637546
<b>Date Filed</b>	04/29/2002
<b>State</b>	DE
<b>Status</b>	ACTIVE
<b>Last Event</b>	CANCEL ADM DISS/REV
<b>Event Date Filed</b>	11/14/2006
<b>Event Effective Date</b>	NONE

### Principal Address

3950 RCA BOULEVARD, SUITE 5001  
PALM BEACH GARDENS, FL 33410

Changed: 02/01/2005

### Mailing Address

3950 RCA BOULEVARD, SUITE 5001  
PALM BEACH GARDENS, FL 33410

Changed: 02/01/2005

### Registered Agent Name & Address

CORPORATION SERVICE COMPANY  
1201 HAYS STREET  
TALLAHASSEE, FL 32301-2525

Name Changed: 04/06/2006

Address Changed: 04/06/2006

### Officer/Director Detail

#### **Name & Address**

Title SECRETARY, VICE PRESIDENT

HUTTON , KATHRYN  
3950 RCA BOULEVARD, SUITE 5001  
PALM BEACH GARDENS, FL 33410

Title CEO, Director

Agostinelli, Richard  
3950 RCA BOULEVARD, SUITE 5001  
PALM BEACH GARDENS, FL 33410

Title CFO

Cahill, Jerry  
3950 RCA BOULEVARD, SUITE 5001  
PALM BEACH GARDENS, FL 33410

#### **Annual Reports**

<b>Report Year</b>	<b>Filed Date</b>
2016	05/03/2016
2017	05/31/2017
2018	05/21/2018

#### **Document Images**

<a href="#">05/21/2018 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">05/31/2017 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">05/03/2016 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">03/23/2015 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">04/28/2014 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">04/24/2013 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">05/08/2012 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">04/14/2011 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">02/22/2010 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">01/14/2009 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">04/01/2008 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">03/05/2007 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">11/14/2006 -- REINSTATEMENT</a>	<a href="#">View image in PDF format</a>
<a href="#">04/06/2006 -- Reg. Agent Change</a>	<a href="#">View image in PDF format</a>
<a href="#">02/01/2005 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">02/17/2004 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">02/25/2003 -- ANNUAL REPORT</a>	<a href="#">View image in PDF format</a>
<a href="#">04/29/2002 -- Foreign Profit</a>	<a href="#">View image in PDF format</a>

# **EXHIBIT 4**



### CORPORATION FILE DETAIL REPORT

<b>File Number</b>	71748871		
<b>Entity Name</b>	WHITE CASTLE SYSTEM, INC.		
<b>Status</b>	ACTIVE		
<b>Entity Type</b>	CORPORATION	<b>Type of Corp</b>	FOREIGN BCA
<b>Qualification Date (Foreign)</b>	09/05/2018	<b>State</b>	OHIO
<b>Agent Name</b>	CORPORATE CREATIONS NETWORK IN	<b>Agent Change Date</b>	09/05/2018
<b>Agent Street Address</b>	350 S NORTHWEST HIGHWAY #300	<b>President Name &amp; Address</b>	ELIZABETH K INGRAM 555 W GOODALE ST COLUMBUS OH 43215
<b>Agent City</b>	PARK RIDGE	<b>Secretary Name &amp; Address</b>	R ANTHONY JOSEPH 555 W GOODALE ST COLUMBUS OH 43215
<b>Agent Zip</b>	60068	<b>Duration Date</b>	PERPETUAL
<b>Annual Report Filing Date</b>	00/00/0000	<b>For Year</b>	

[Return to the Search Screen](#)

[Purchase Certificate of Good Standing](#)

(One Certificate per Transaction)

[BACK TO CYBERDRIVEILLINOIS.COM HOME PAGE](#)

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [White Castle Hit with Class Action Over Alleged Violations of Illinois Biometric Privacy Law](#)

---