SANDBERG PHOENIX

EMPLOYER LAW BLOG

EMPLOYER ALERT: Illinois Federal Court Refuses to Dismiss Franchisor and Out-of-State, Third-Party Technology Vendor in BIPA Suit

AUTHOR: JAMES KEANEY

CONTRIBUTOR: PHILIP GRAHAM

The case—Ronquillo v. Doctor's Associates, LLC and HP, Inc.—is pending before the United States District Court for the Northern District of Illinois. It involves claims by an employee of a Subway franchisee that the franchisor and its vendor violated BIPA by collecting and obtaining her biometric information without the required consent.

In this case, the plaintiff employee alleged the technology vendor—Hewlett-Packard ("HP")—leased point-of-sale software and hardware to the franchisor (while HP still maintained ownership of the hardware), and the franchisor—in turn—required franchisees to use the software and hardware with its employees, like the plaintiff.

The plaintiff alleged the franchisor uses this software and hardware to create "reference templates" of workers' fingerprints—that is, copies of the fingerprints that the systems use to identify workers whenever they clock in or out or unlock registers.

Both the franchisor and vendor moved to dismiss the employee's claims on several grounds.

First, as many courts have recognized, they argued BIPA requirements do not apply based solely on possession of biometric data alone; rather, to be subject to BIPA, the company must "take active steps to collect, capture, or otherwise obtain" biometric information.

The court did not necessarily disagree. But it found the employee's allegations, at the initial stage of the lawsuit, sufficient to show both the franchisor and vendor "took an active step" to "obtain" her fingerprints.

Second, the defendants argued it would lead to absurd results if the court applied BIPA to non-employers like the technology vendor and franchisor in this case. The court disagreed, relying primarily upon the broad language used in the statute itself.

Finally, HP urged the court BIPA does not and should not apply to a non-resident of Illinois like HP. Once again, the court disagreed. The court concluded it should apply because "the alleged BIPA violations took place 'primarily and substantially in Illinois.'" The court based this conclusion on the plaintiff's allegation the fingerprint scans occurred via HP-owned hardware located at a Subway store in Illinois.

So, what are the takeaways from this case?

At least one is that technology vendors across the country—especially companies offering point-of-sale software and hardware—should carefully review with counsel their contracts and policies, including indemnity agreements, to ensure steps are taken to protect against or minimize any liabilities or exposure to liabilities under BIPA.