Labor and Employment Alert: Illinois Employers Face a Wave of Class Actions for Collecting Biometric Data

Related Professionals

Michael J. Ball

Michael C. Griffaton

Related Services

Class Actions

Labor and Employment

CLIENT ALERT | 12.22.2017

Companies are increasingly turning to technology to track customers and employers. For example, employers use fingerprint readers as means of employee timekeeping. Employers doing so in Illinois must take heed of the Illinois Biometric Information Privacy Act (BIPA). Enacted in 2008, BIPA was relatively dormant until recently. But in 2017, more than 25 lawsuits were filed against companies for failing to comply with BIPA when using biometric identifiers like retina scans, voiceprints, fingerprint identification and facial recognition technology to collect biometric information from employees and customers. Biometric information is broadly defined to mean any information, regardless of how it is captured, converted, stored or shared, that is based on an individual's biometric identifier (retina scan, fingerprint, voiceprint, etc.).

BIPA does not prohibit the use of biometric identification technology. Instead, BIPA requires individuals and companies to provide notice and obtain consent before collecting or using biometric data and then ensure the proper storage and disposal of that data. Under BIPA, a private entity that possesses biometric identifiers or biometric information must develop a publicly available, written policy establishing a retention and destruction schedule. The biometric information and identifiers must be destroyed when the initial purpose for collecting or obtaining it has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

A private entity is prohibited from collecting, capturing, purchasing, or otherwise obtaining a person's or a customer's biometric identifier or biometric information unless it first does all of the following:

(1) informs the person in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the person 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, which is defined as “informed written consent” or, in the context of employment, “a release executed by an employee as a condition of employment.”

No private entity may disclose, redisclose or otherwise disseminate a person's biometric identifier or biometric information unless that person consents; the disclosure completes a financial transaction requested or authorized by the person; or the disclosure is required by law, warrant or subpoena. A private entity is further prohibiting from selling, leasing, trading or otherwise profiting from a person's biometric identifier or biometric information.

A private entity must store, transmit and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and store, transmit and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits and protects other confidential and sensitive information.

BIPA provides a private right of action for violations. A prevailing party can recover substantial damages for each violation: $1,000 in liquidated damages or actual damages for negligent violations; $5,000 in liquidated damages or actual damages for reckless violations; and reasonable attorneys’ fees and costs.

Companies in Illinois that use or collect biometric information from customers or employees must take immediate steps to ensure that they are complying with BIPA. At a minimum, this includes preparing a written policy and retention and destruction guidelines, providing the requisite notice, and adopting the appropriate safeguards for storing and transmitting biometric information. Contact your Vorys lawyer if you have questions about the Biometric Privacy Act and best practices for compliance.