SFGH Sugar Felsenthal Grais & Helsinger LLP

Illinois Biometric Information Privacy Act (BIPA)

Enacted in 2008, the Illinois Biometric Information Privacy Act ("BIPA") (740 ILCS 14/1, *et seq*.) regulates private employer use of biometric identifiers and biometric information. For purposes of BIPA, biometric information is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." Examples are fingerprints, iris scans, voice prints, and facial recognition scans. Local and state governmental employers are specifically exempted from BIPA.

Employer use of biometric information

Employers are not allowed to use retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry for security scanning, time entry, and paying wages or salaries without prior notice or written consent of the employee. BIPA specifically excludes certain personal information from the definition of biometric identifiers, such as writing samples, photographs, human biological samples used for validating scientific testing or screening, demographic data, tattoo descriptions, and physical descriptions.

Protecting employee biometric information

Employers are required to protect biometric identifiers and information using a reasonable standard of care. The means of protection must be at least as protective

as the manner in which the employer protects other confidential and sensitive information.

Employers must refrain from disclosing biometric identifiers or information. Exceptions include employee consent, completion of a financial transaction that the employee authorized, a federal, state, or local law requires disclosure, or a warrant or subpoena requires disclosure. Employers are prohibited from selling or profiting from biometric identifiers and information. Restrictions on selling and disclosing biometric information also applies to third parties that maintain or manage databases consisting of employees' biometric information.

Notice and Consent

Before obtaining or transferring biometric identifiers or biometric information on employees, employers **must:** (1) inform the employee in writing of the applicable time span and specific purpose for collecting, storing, and using the employee's biometric identifier or biometric information; and (2) receive a written release from the employee as a condition of employment for such collection, storage, and use.

Written Policy Requirements

Employers must also have a public written policy which states a schedule for retaining biometric identifiers and biometric information and guidelines for destroying such data when the purposes of collecting it have been satisfied or within

three (3) years of the employee's last interaction with the employer, whichever is earlier.

Compliance

BIPA permits individuals to sue for violations and recover liquidated damages of $1,000 for each violation instance or actual damages, whichever is greater, along with attorney fees and expert witness fees. The liquidated damages amount increases to $5,000 if the violation is intentional or reckless. Courts have applied BIPA to out-of-state employers as long as the violations occurred within Illinois. Violations do not require disclosure of the biometric date. Collection or storage of the information without consent qualifies as a violation, even if the data remains secure.

The Illinois Supreme Court determined that an individual need not suffer actual damages to be a person aggrieved and that any violation of the statute entitles an individual to the available remedies. The 9th Circuit approved a class action lawsuit against Facebook claiming the company's use of biometric data for facial recognition violates BIPA. The lawsuit alleges damages of $1,000 for every negligent violation, and $5,000 for every intentional or reckless violation for affected Facebook users.