



Employers Must Be Aware Of The Illinois Biometric Information Privacy Act

Matthew Kellam

11.01.2017

In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA). BIPA, which governs private entities, addresses the collection, storage and use of “biometric identifiers” of individuals, such as retina or iris scans, fingerprints, voiceprints and scans of hand and face geometry. The purpose of BIPA is to prevent identity theft because biometric information is permanent and, once compromised, leaves the victim with little recourse to recover from identity theft. BIPA, among other measures, requires private entities that use biometric information to develop a written policy, made available to the public, that establishes a retention schedule for permanently destroying biometric information. BIPA also requires private entities to provide written notice to, and receive written releases from, subjects before collecting, capturing or otherwise obtaining their biometric information. Lawsuits filed under BIPA are on the rise, as evidenced by a class action lawsuit recently filed in the Circuit Court of Cook County against a manufacturing company. According to the plaintiffs in that case, their employer violated BIPA by requiring them to scan their fingerprints into its time clock system to record their hours worked without first providing written notice to plaintiffs and receiving their written consent to do so. In certain cases, BIPA imposes a \$5,000 penalty for each violation, in addition to attorneys’ fees. Employers who use biometric information of their employees, customers, vendors, or any other individuals must be aware of BIPA and comply with its notice and consent requirements.

Attorneys

Matthew P. Kellam

Practice Areas

Class Actions / EEOC
Pattern and Practice

Counseling and
Transactional
Employment Counseling
Public Sector