

March 27, 2019

Illinois Biometric Policy Law Does Not Require Proof of Actual Damages



Private: Mark Brookstein

Human Resources & Employment

Attention businesses operating in Illinois: If you use a person's "biometric" data for things like timekeeping or security, you *must* have a written policy under which you: (1) obtain written consent, (2) store the data confidentially and (3) destroy the data no later than three years after the last interaction with the person.

If you fail to do so, you face statutory penalties of \$1,000 (negligently) or \$5,000 (recklessly/intentionally) *per person per violation* – even if the employee suffered no actual damages (such as identity theft, etc.). You will also be paying the person's attorneys' fees and litigation expenses (including expert witnesses).

That was the Illinois Supreme Court's ruling in *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, a case involving an amusement park scanning customer fingerprints for use with entry passes. The park did not obtain consent or provide any information about its use of the fingerprints. The potential damages based on millions of customers visiting the park each year is staggering.

It is therefore vital for companies operating in Illinois to understand their obligations when it comes to biometric data.

What is "biometric" data?

The Illinois biometric law (BIPA) breaks down biometric data into two categories. *First*, a "biometric identifier" includes a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. *Second*, "biometric information" includes a biometric identifier in any form—like an uploaded photograph converted into geometric facial measurements or other mathematical representation. In other words, if there is any way to use information to establish a biometric identifier, that information is covered.

What do I do if my business uses biometric data?

BIPA covers companies "in possession" of biometric data, which means to "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data. An easy example is employers who use employee fingerprints for timekeeping rather than punch cards. Such employers must have a written policy that complies with BIPA, which includes obtaining written consent.

Given the expanded reach of BIPA under the *Rosenbach* case, employers and other companies doing business in Illinois should review whether they are properly using biometric data.

The HR attorneys at Gould & Ratner are available to discuss any questions or other issues involving BIPA and its requirements as discussed here. Please do not hesitate to contact us for further information.