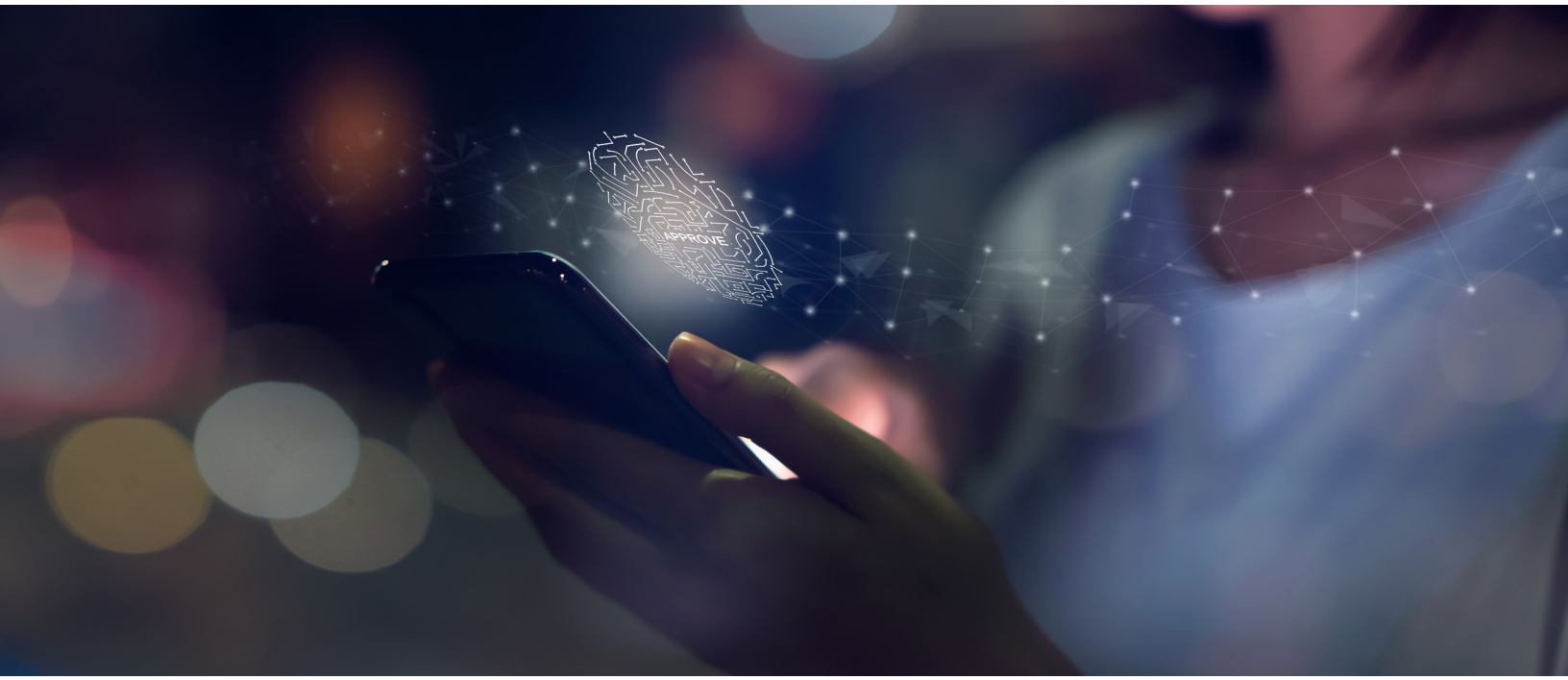
MarshMcLennan Agency

Your future is limitless.℠



Illinois Biometric Information Privacy Act

How to Stay Compliant

Does your organization utilize fingerprints, retina, voice, face scans or other biometric identifiers in its practices? The Illinois Biometric Information Privacy Act (BIPA) is cracking down on biometric use and safekeeping.

In 2008, Illinois enacted a groundbreaking law to help individuals control their own biometric data. BIPA is a bill that regulates the collection, use, safeguarding, handling, storage, retention and destruction of biometric identifiers and information. It requires private employers to inform impacted parties, disclose the purpose and duration of storage and obtain written consent as it relates to the following:

Biometric Identifiers: retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry

Biometric information: any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual

Despite BIPA's exclusion of photographs, a number of putative class action lawsuits have been filed based on the collection and storage of photographs.

Why is this important?

Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers when compromised can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

How has BIPA impacted employers?

Tanning salons have long used fingerprint scanners to sign a customer in. Fast food restaurants have used facial recognition scanners for consumers to access their profile. While these instances may happen a few times throughout the month, an employer's biometric timeclock could be used at least four times a day, five days a week, by a full-time, non-exempt employee. If not compliant, this could subject Illinois employers using biometric identifiers and/or information to lawsuits.

Most recently, BIPA received massive attention when the Illinois Supreme Court unanimously ruled in favor of Stacy Rosenbach (Rosenbach v. Six Flags Entertainment Corp) in January 2019. Stacy sued the amusement park Six Flags after her son's fingerprints were taken without notice and consent when purchasing a season pass. The Illinois Supreme Court held that an individual "does not need to allege actual harm in order to seek liquidated damages and injunctive relief under the Illinois Biometric Information Privacy Act." The plaintiff only needed to allege there was a technical violation of BIPA to be sufficiently "aggrieved" under the Act. The Court's ruling will likely increase the already considerable number of BIPA-related cases throughout Illinois and the country.

How do you remain compliant?

Does your organization currently collect, use, store and/or handle biometric identifiers and information? If the answer is 'yes,' here are a few ways to stay compliant with the Illinois law.

Make Your Policy Public: The policy is required to be made available to the public establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information.

Obtain Written Consent: BIPA requires a written, publicly available policy with a retention schedule and guidelines for “permanently” destroying the data.

Take Reasonable Care: Organizations must protect data in the same manner in which it stores, transmits, and protects other confidential and sensitive information like social security numbers, drivers licenses, etc.

Check Insurance Coverage: Discuss your current operations and practices with your broker. He or she can review if and where insurance coverage might protect your organization in the event of a lawsuit.

What are the legal and financial implications?

Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. Employers can be sued (on top of paying the fines listed below) for the following reasons:

- No policy in place
- No waiver obtained from employees
- No retention/destruction protocols

A prevailing party may recover for each violation:

- $1,000 or actual damages (whichever is greater) for negligent violations
- $5,000 or actual damages (whichever is greater) for intentional or reckless violations

With over $1,000 in damages per violation, employers are being subjected to large class action lawsuits. The most frequent class action lawsuits target employers utilizing biometric timekeeping systems. If an employer is using a biometric timeclock, that could mean over $1,000 in damages times four instances per day times five days per week for just one full-time, non-exempt employee. Now, take that $20,000 per week and times it by the number of employees utilizing that biometric timeclock and for however many weeks it was in place and used.

With over $1,000 in damages per violation, employers are being subjected to large class action lawsuits.

Now what?

The court's interpretation of BIPA will likely encourage lawsuits against employers using biometric identifiers for consumer or employee authentication. It is important to speak with a legal advisor and your insurance broker to ensure your organization is covered in the event of a lawsuit.

Contact your local Marsh McLennan Agency advisor today.

Business Insurance
Employee Health & Benefits
Private Client Services
Retirement Services

MarshMcLennan Agency

A business of Marsh McLennan