Biometric Information Privacy Act in Illinois: How Can You Protect Yourself?

Knowledge is power. As we identify exposures that your business may face, we wanted to take a moment to provide some information regarding biometric information privacy laws and what we know that may help protect your business.

Recent court rulings have put a spotlight on how businesses are or are not complying with the Illinois Biometric Information Privacy Act (BIPA). This statute regulates how this information is collected, used, stored and destroyed, as well as assesses statutory damages for non-compliance. The provisions that have caused the litigation rush are those that created a private right of action and imposed statutory damages of $1,000 per violation and $5,000 if intentional or reckless. Moreover, the Illinois Supreme Court has held that the plaintiff in a BIPA case need not show any actual injury — just a violation of the statute.

What is biometric information?

Biometric information includes physical characteristics that can identify a person, such as retina or iris scans, fingerprints, voiceprints or facial geometry. BIPA prohibits the collection of such data from employees, customers, vendors, residents or other third parties without their written authorization and without a public policy for the handling and use of such information.

What can I do to try to comply with the law?

Assess your Risk

- Determine if and what biometric information is being collected
  - Only collect such information if absolutely necessary. New technologies such as a timeclock using biometric data come with unintended consequences
- If biometric information must be collected, determine how it is collected, stored, and used
- Create and share your written biometric data storage policy (including purpose for collecting biometric information, disclosure/non-disclosure, duration of storage and method of destruction) that complies with the law
- Test your systems to ensure they are working appropriately
- Determine reasonable accommodations for disabilities and religious beliefs
- Make sure you don't sell, lease, trade, or otherwise profit from the biometric information
- Do not disclose, re-disclose, or otherwise disseminate biometric information unless consent is obtained or the disclosure is required for specific purposes (e.g., the disclosure is necessary to complete a financial transaction, required by law, or pursuant to a valid warrant or subpoena)
- Review your vendor contracts; don't assume that using a vendor to provide services such as biometric payroll systems relieves you of liability under the law
- Keep an eye on state and federal laws and legal developments

Give Written Notice and Obtain Proper Authorization

- A written notice should include a disclosure about the information being collected, what purpose it will be used for, how it could be shared, and how and when it will be destroyed
- Obtain written consent for the collection, storage and use of the biometric information

Train Your People

- Make sure your employees are aware of these regulations and there is a process in place to help maintain compliance

---