Management Alert

Illinois Biometrics Act Enacted

Though it may conjure images of a futuristic James Bond movie, employers and businesses have already begun using "biometric information"—such as fingerprints, retina scans and voice prints—for identification purposes. Businesses are turning to biometric data to make financial transactions more efficient and employers are using it to ensure that access to sensitive locations and private or confidential information is appropriately restricted. In October 2008, Illinois became the latest state to protect biometric information from possible identity theft with the enactment of the Biometric Information Privacy Act (the "Act"), 740 ILCS 14/1. The Act regulates private entities' collection, use, storage, retention, and destruction of biometric information. Private employers who collect and/or use biometric information for *any* purpose may be covered by the Act.

What Is Biometric Information?

Biometric information includes retina or iris scans, fingerprints, voice prints, and the scan of face geometry. As science continues to develop, other types of biometric information may also become available. Biometric information does not include: writing samples, photographs, tattoo descriptions, or physical descriptions such as weight, hair color, or eye color. It also does not include information captured from a patient in a health care setting or stored for healthcare treatment.

Common examples where companies already use biometric information include: hand scanners to control the entrance into a building or worksite; the collection of thumbprints for use as a means of payment (such at a grocery store check out counter or paying at the pump at a gas station); obtaining fingerprints from job applicants as part of the background screening process; and/or the use of iris or retina scans, or voice prints as a means to control access to sensitive information or locations, among others.

Why The Need For The Law?

Biometrics are increasingly used by Illinois businesses and employers as a means of restricting unauthorized people from accessing sites or information and also in private financial transactions as a means of streamlining and expediting processes and limiting access to sensitive data. Additionally, many employers collect biometric information from employees for employment purposes, such as fingerprints used for background screening. In recent months, an increasing number of Illinois businesses have begun allowing customers to pay for goods or services by using thumb-print scans and other types of biometric devices. It is also becoming increasingly common for businesses in Illinois to replace traditional employee identification and security access cards with biometric information readers.

While the use of biometric information may be attractive to businesses, employers, customers, and employees alike because of its ease of use and the greater efficiencies it presents (no cards to lose or money to carry), it also poses a heightened risk of identity theft. Unlike traditional identifying information, biometric information is particularly sensitive because it is *biologically unique* to the individual. If such information is stolen or otherwise compromised, the individual has no recourse and remains at heightened risk for identity theft. By contrast, if a social security number is compromised, it can be corrected or changed.

What Do Employers Need To Do To Comply With The Biometric Information Privacy Act?

The Act's requirements for any private entity that possesses biometric information are identical whether the intended use is for employment, security, financial, or other purposes. For employers, biometric information is most likely to be relevant in two areas: hiring and access. Employers should carefully review their hiring procedures to determine whether they include the collection, use, or retention of fingerprints or other biometric data. As a further point of caution, even if an outside agency performs the background check, an employer may be subject to the Act if it receives copies of the fingerprints or other biometric information as part of the hiring process. The second way employers are likely to use biometric information is to control employees' access to certain locations or information, such as by requiring hand scans for entrance to a work site, or by using voice prints to ensure that individuals seeking access to sensitive data have appropriate authorization.

Five Key Components of the Law

1. Written policy

Any private entity in possession of biometric information must develop a written policy, made available to the public, regarding its use of biometric information. The policy must establish a retention schedule for the information and contain guidelines for permanently destroying biometric information when the initial purpose for obtaining the information has been satisfied or within three years of the individual's last interaction with the private entity—whichever occurs first.

2. Collection

No private entity may collect, purchase, receive through trade, or otherwise obtain biometric information unless it first:

a. Informs the subject (or his or her legally authorized representative) in writing that it is being collected;
b. Indicates the purpose for collecting the biometric information and length of time for which it is being collected, stored, and used; and
c. Receives a written release from the subject (or his or her legally authorized representative) of the biometric information.

3. Sale

Once collected, the biometric information cannot be sold, leased, or traded.

4. Disclosure

Any private entity that possesses biometric information cannot disclose or disseminate it unless:

a. It first obtains consent by the subject;
b. The disclosure completes a financial transaction authorized by the subject;
c. Disclosure is required by state or federal law; or
d. Disclosure is required pursuant to a valid warrant or subpoena.

5. Storage

A private entity in possession of biometric information shall store, transmit, and protect from disclosure using the reasonable standard of care within the private entity's industry, and by using a method that is the same or more protective than that in which the private entity stores and protects other sensitive information.

What Are The Risks Of Noncompliance?

Entities that fail to comply with the Act may be subject to a private suit filed by individuals whose biometric data is compromised. Damages for noncompliance include: the greater of liquidated or actual damages (liquidated damages are $1,000 for a negligent violation or $5,000 for an intentional or reckless violation), injunctive relief, and attorneys' fees and costs.

Conclusion

Employers should review their policies and procedures to determine if they currently use biometric information, and are thus subject to the Act's requirements. Before implementing any new biometric information program, employers should insure that they have a written policy in place that complies with all aspects of the Act, and should consult with counsel regarding any questions or concerns.

For more information, please contact the Seyfarth attorney with whom you work, or any Labor and Employment attorney on our website (www.seyfarth.com/LaborandEmployment).

SEYFARTH ATTORNEYS SHAW LLP

Breadth. Depth. **Results.**

www.seyfarth.com