CLIENT ALERTS & INSIGHTS

Illinois Amends Biometric Information Privacy Act to Reign in Liquidated Damages and Permit Electronic Signatures

AUGUST 12, 2024

The amendments clarify that a plaintiff is only entitled to liquidated damages for up to one violation per person. Businesses had previously faced steep settlements or damage awards into the billions of dollars.

On August 2, Illinois Governor J.B. Pritzker signed a bill amending the Biometric Information Privacy Act ("BIPA"). The amendments address what many businesses viewed as excessively harsh financial penalties wrought by previous court precedent.

Under recent Illinois court precedent, a business was viewed to have violated the act each time a biometric information data point was collected. The amendments instead narrow the "per violation" definition attached to the liquidated damages set forth in BIPA to just a single violation where an individual's information was collected in violation of the statute, no matter how many times their information was collected improperly. Additionally, businesses will be permitted to rely on electronic consent and signatures under the amendments, lowering the implementation hurdles faced by businesses implementing consent mechanisms.

Courts previously left unanswered the question of whether electronic signatures or online consents were permitted or would be sufficient to adhere to BIPA's strict consent requirement. The new amendments allow for and clearly incorporate the concept of electronic signatures.

Of course, the biggest headline with the BIPA amendments is still the liquidated damage reform. The Illinois legislature addressed what businesses had indicated could amount to "annihilative liability." Courts previously held that businesses were liable for violations of the law-and subject to additional fines-each time a business collected biometric information, even where it collected information from single individuals multiple times. In today's technological day and age, where information is collected from the same individuals on a daily basis, the number of violations could, in theory, be astronomical.

These new BIPA amendments address this concern, while also attempting to thread the needle of maintaining the law's privacy protections. Importantly, the amendment maintains that a business can still be liable for multiple violations with respect to the same person's biometric information collected through more than one biometric information collection technology.

Definitions; Old & New

Under BIPA, businesses are prohibited from collecting biometric information without first providing comprehensive notice to-and obtaining affirmative express consent from-an individual. This includes

biometric information collection as it relates to consumers, as well as employees and independent contractors.

"Biometric information" is generally defined as information that is captured, collected, or processed based on an individual's biometric identifiers for the purpose of identifying the individual. "Biometric identifiers" are subsequently defined to include the following examples of biometric data points:

- Retina or iris scans
- Fingerprints
- Voiceprints
- Palmprints
- Face geometry / facial recognition

One important exclusion to keep in mind under BIPA is that the definition of "biometric identifiers" does not include "***information collected, used, or stored for health care treatment, payment, or operation under the Federal Health Insurance Portability and Accountability Act of 1996***." In a recent Illinois Supreme Court case, the court determined that this exemption extended to the collection of employee biometric information that was collected for such employees to access medicine cabinets at hospitals.

With respect to obtaining an individual's consent prior to collecting or otherwise using their biometric information, businesses are required to obtain a "written release." A "written release" was previously defined as "***informed written consent, or, in the context of employment, a release executed by an employee as a condition of employment***."

The "written" aspect of this consent has been the subject of scrutiny from practitioners and businesses alike but courts have thus far shied away from clarifying whether the original definition required a "wet" signature or whether electronic consent or signature also sufficed. Implementing physical signatures proved easier in the employee-employer relationship, as it can be included in onboarding processes. However, businesses had struggled to ascertain the risk of relying on electronic consent in the consumer context-with electronic consent mechanisms proving far more practical and convenient for both businesses and consumers in today's technological world.

The Illinois legislature previously pushed for amendments making clear electronic signatures satisfy the consent requirements-but all previous efforts failed to pass. These new amendments finally enact such clarification and introduce the new BIPA concept of "electronic signature", which is defined to mean "***an electronic sound, symbol, or process attached to or logically associated with a record executed or adopted by a person with the intent to sign the record***." Electronic signatures are also now affirmatively incorporated into the definition of "written release" giving businesses far more flexibility in their implementation of consent mechanisms and processes.

BIPA Liquidated Damage Reform

In the landmark *Cothron v. White Castle Sys., Inc.* case, the Illinois Supreme Court held that liquidated damages under BIPA accrue every time a business collected, used, or otherwise processed

biometric information in violation of the law's requirements-whether or not the business had previously already collected the same information from the same individual. While the court acknowledged this could ballon the potential damages into the billions of dollars, they ruled that the plain meaning of the law made clear that a business was liable each time it violated BIPA's consent requirements, not just for each person whose information was improperly collected or disclosed.

Essentially, "per violation" meant per instance biometric information was collected or disclosed without consent-regardless of who the information related to or how many times that individual's information was collected.

BIPA imposes liquidated damages of $1,000 per violation and $5,000 per "reckless or intentional" violations. Under the *White Castle* precedent, a business was potentially liable for damages every time a biometric information data point was collected or disclosed without consent.

The new amendments state that when a business collects or otherwise processes biometric information about "***the same person***" in more than one instance but "***using the same method of collection***", the business can only be liable for a single violation of BIPA. The amendments essentially equate to "per violation" meaning "per person," which has the potential to lower the number of damages plaintiffs seek under BIPA. Damage claims in BIPA cases had ballooned in recent years to hundreds of millions of dollars and even into the billions.

However, one important point of caution for businesses that leverage biometric information technology: the amendments make clear this narrowing of "per violation" only applies where the information was collected from the same person **using the same technology**. If, for example, the business collects the same biometric information about a consumer using two different technologies-for example, in the employee context through a timekeeping system **and** through on-premises facial recognition security cameras-the business would be liable for more than one violation.

As more states continue to implement their own variations of data protection laws and businesses juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.