CLIENT ALERTS & INSIGHTS

First Ever BIPA Trial Results in a $228 million Judgement Against Railway Company that Relied on Third Party Vendor to Collect Employee Fingerprints

OCTOBER 24, 2022

The judgement, which came down last week, exemplifies the risk of biometric information collection in Illinois and the risk that can result from relying solely on third party vendors.

On October 12, 2022, a jury found that BNSF Railway Company-which operates in Illinois-did indeed violate Illinois Biometric Information Protection Act ("**BIPA**") when its employees' fingerprints were scanned prior to their entry into the railyard the employees worked in.

This case represents a major milestone in BIPA litigation as the first ever trial in the law's 14 year history-which thus far has been marked with large settlements and consistent appeals by businesses attempting to mitigate the law's broad applicability.

Throughout the case, BNSF attempted to avoid trial and liability by making various arguments, including, that (1) BNSF's third party vendor who supplied and supported the fingerprint scanning had violated BIPA-implying BNSF had not directly violated BIPA; (2) Federal law preempted BIPA in this instance; and (3) that the statute of limitations had run on at least some, if not all, of the plaintiff's claims.

The United States District Court in the Northern District of Illinois, however, was not swayed by the arguments, consistently siding with the plaintiffs. Throughout the course of the case, the court allowed in evidence implying vicarious liability (e.g., that BNSF was responsible for its third party vendor's actions) and rejected claims that Federal law or statute of limitations applied.

The court's acceptance of arguments that BNSF could be liable for the actions-and lack of BIPA compliance-of its third party vendors is perhaps the most important aspect of this case. As crime has become a top concern for individuals and businesses in the United States, security and verification technology and software has increased exponentially. Many of these services include forms of biometric information collection, whether it be fingerprints as was the case here, retina scans, facial recognition software, or palm prints. Businesses entering into engagements for such services will need to heavily scrutinize their potential third party vendors and ensure the applicable contracts include proper protections and risk allocations as BIPA litigation becomes more and more common.

BIPA Standards and Requirements

BIPA prohibits a business from collecting, capturing, purchasing, or otherwise obtaining an individual's biometric information unless they receive the specific individual's prior written consent. Prior to obtaining that consent, businesses must also properly inform the individual in writing (1) that biometric information is collected (i.e., notice) and (2) the applicable time period for which the biometric information is retained.

Businesses are also generally prohibited from disclosing or otherwise disseminating biometric information-even where they originally obtained the consent described above. Instead, a business can only disclose biometric information in the following cases: (1) the individual gave a separate consent, specific to disclosure of their biometric information; (2) disclosure is necessary to complete a financial transaction requested or authorized by the individual; (3) disclosure is required by law; or (4) disclosure is required by applicable court order.

BIPA also requires business that collect biometric information to develop and maintain a written policy that is publicly available-akin to a website privacy policy-the establishes a specific retention period and guidelines on how the biometric information is destroyed after that retention period lapses. Generally, the retention period needs to be for the length of time necessary for the initial purpose the information was collected for, or 3 years after the individual's last interaction with the applicable business. Meaning, the longest a business can retain biometric information is 3 years.

Biometric information, under BIPA, can include retina or iris scans, fingerprints, voiceprints (e.g., voice recognition technology), or scans of the hand or face geometry (e.g., facial geometry or mapping technology).

Private Right of Action and Penalties

BIPA includes and expressed private right of action against those businesses who have violated the law's requirements.

If a plaintiff can prove that the business **negligently** violated the law, the liquidated damages are set to $1,000 per violation or the actual damages, whichever is greater. If a plaintiff can prove that the business **intentionally or recklessly** violated the law, the liquidated damages are set to $5,000 per violation or the actual damages, whichever is greater.

It is important to not the qualifier that the these penalties are **per violation** meaning the fine damages awarded-if the business is collecting thousands of biometric identifiers in violation of the law as was the case in the BNSF case-could rise into the millions.

BIPA Considerations and Risks

This latest case, and first ever trial, in BIPA's decade plus history establishes that the business **using** technology or software that collects biometric information can be held liable for BIPA violations-regardless of whether the actual technology or software is developed, provided, supported, and/or operated by a third party vendor.

Moving forward, businesses need to seriously scrutinize their engagement with biometric technology and software service providers to ensure BIPA compliance is in place both in their own business

processes, but also the business processes of the applicable vendor, and that proper contractual protections are in place.

As more technology and software bring biometric information collection into scope, and BIPA compliance and litigation continue to evolve, 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.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.