THE
NATIONAL LAW REVIEW

Illinois Experiences Surge of Lawsuits Regarding Biometric Information Privacy

Wednesday, November 1, 2017

Employers continue to incorporate the use of biometric information for several employee management purposes, such as in systems managing time keeping and security access that use fingerprints, handprints, or facial scans. Recently, Illinois state courts have encountered a substantial increase in the amount of privacy class action complaints under the Illinois Biometric Information Privacy Act ("BIPA"), which requires employers to provide written notice and obtain consent from employees (as well as customers) prior to collecting and storing any biometric data. Under the BIPA, the employer must also maintain a written policy identifying the "specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used." 740 ILC 14/15(b)(2).

Although the BIPA was enacted almost 10 years ago, individuals did not start filing lawsuits until 2015. Since September 2017, there have been over twenty-five new filings in Illinois state courts including class actions against prominent international hotel and restaurant chains. These lawsuits tend to target employers utilizing finger print recognition machines as part of their time keeping systems. Where the employer uses a third-party supplier for its time-tracking system, the claims have also included allegations that the employer improperly shared the biometric information with the supplier without obtaining the proper consent. In these cases, the claims generally allege that the employer failed to provide proper notice.

Article By Nathaniel M. Glasser
Adam S. Forman Maxine Adams
Epstein Becker & Green, P.C.
Technology Employment Law
Litigation / Trial Practice
Communications, Media & Internet
Labor & Employment
Illinois

Though there is no definitive reason for the increase in filings over the past months, the claims may be related to the increased use of biometric information in the workplace since the initial case filings in 2015.
While Texas and Washington also have laws governing employer use of biometric information, Illinois is the only state that currently provides a private right of action, including class actions. Additionally, potential damages associated with BIPA violations, particularly for class actions, can be extensive, including liquidated damages of $1,000 per negligent violation (or the amount of actual damages, whichever is greater), liquidated damages of $5,000 per intentional or reckless violation (or the actual damages, whichever is greater) and attorney's fees.

What Can Employers Do?

- Prior to collecting or storing biometric data, employers in Illinois should: (1) create a written policy regarding the retention and destruction of biometric data; (2) obtain written acknowledgment and release from the employees; and (3) store the biometric information securely, similar to other confidential information, such as personal health information or personally identifiable information.
- Employers who use a third party to assist with the collection or storage of biometric data should include the third party in the acknowledgement and release, which employees execute.
- Employers also should be aware that most states, including Illinois, have legislation governing how

employers respond to data breaches and the required notifications to employees. If a data breach occurs, employers are advised to immediately contact counsel to devise and implement a response plan.

- In the event of litigation, employers should remove BIPA cases to federal courts when possible, particularly where the allegations focus on notice and consent issues, as employers can argue that plaintiffs cannot establish the necessary harm to establish standing as required by the Supreme Court case *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (requiring more than a "bare procedural violation" to establish harm). Because employees likely will have difficulty establishing actual harm where the biometric data was stored in a confidential and secure manner, employers may be successful in getting such claims dismissed.

As the laws regulating biometric data continues to evolve, employers should monitor this issue closely and consult with counsel as further developments occur to ensure compliance with any relevant regulations.