CARLTON FIELDS

New York City Creates Right to Sue Over Use of Biometric Data

October 13, 2021

New York City's new biometrics law, NYC Admin. Code §§ 22-1201–1205, went into effect in July 2021. The law creates a new private right of action for persons "aggrieved" by violations. Violations might arise from at least two different requirements. First, the law creates signage requirements for "commercial establishments," which include places of entertainment, retail stores, and food and drink establishments. Second, the law creates a blanket ban on any person or entity selling or "otherwise profit[ing] from" the transaction of biometric identifier information used by a commercial establishment.

A similar Illinois statute (the Biometric Information Privacy Act) has led to significant consumer class action litigation because the Illinois Supreme Court has held that individuals need not suffer an actual, concrete injury to be "aggrieved" and thus have standing to sue. If courts adopt a similar interpretation of New York City's new law, a similar result may follow in the five boroughs.

Covered Information

"Biometric identifier information" is defined as a "physiological or biological characteristic that is used by or on behalf of a commercial establishment … to identify or assist in identifying an individual." The law also gives a nonexclusive list of examples: (i) a retina or iris scan; (ii) a fingerprint or voiceprint; or (iii) a scan of the hand or face geometry, or any other identifying characteristic.

Requirements for Collection, Use, and Retention of Covered Information

The law has two basic requirements: post a sign that discloses what you're doing, and don't sell biometric identifier information.

The disclosure and signage requirement in section 22-1202(a) provides that a commercial establishment that collects, retains, converts, stores, or shares its customers' biometric identifier information must place a clear and conspicuous sign "in plain, simple language" near any customer entrance to notify customers of the collection of their biometric data.

However, the disclosure and signage provision generally does not apply to biometric identifier information "collected through photographs or video recordings," such as security cameras. That is, disclosure and signage are not necessary if: "(i) the images or videos collected are not analyzed by software or applications that identify, or that assist with the identification of, individuals based on physiological or biological characteristics, and (ii) the images or video are not shared with, sold or leased to third-parties other than law enforcement agencies."

In addition, the disclosure and signage provision generally does not apply to "financial institutions," such as banks, credit unions, and brokerage firms. It only applies if those otherwise exempt institutions are primarily engaged in "the retail sale of goods and services to customers" and only provide "limited financial services such as the issuance of credit cards or in-store financing." Thus, a department store that offers a credit card would likely be unable to claim the exemption.

Government agencies, employees, and agents are also exempt from provisions relating to the "collection, storage, sharing or use" of biometric identifier information.

The prohibition on sales in section 22-1202(b) provides that "[i]t shall be unlawful to sell, lease, trade, share in exchange for anything of value or otherwise profit from the transaction of biometric identifier information."

A plaintiff suing under the law might argue that, unlike the disclosure and signage provision, the ban on selling or otherwise profiting from biometric identifier information applies to photographs or video recordings. That is because the applicable exemption is not incorporated into the definition of "biometric identifier information" itself but is instead located within section 22-1204(b), which only expressly mentions the disclosure and signage provision. Thus, a prospective plaintiff might argue that the exemption for photographs and video recordings applies only to the signage provision and not to the ban on sales.

Finally, government agencies, employees, and agents might not be exempt from the rule prohibiting the sale of biometric identifier information.

Private Right of Action

Individuals can bring lawsuits against commercial establishments that have allegedly violated the law. Prospective plaintiffs alleging violations of the signage requirement must provide a 30-day written notice and cure period to the commercial establishment, setting forth the grounds for the allegation, before filing a lawsuit. No prior written notice is required for actions alleging the unlawful sale of biometric identifier information. Recoverable damages are $500 per violation for improper signage, $500 per negligent violation of the ban on the sale of information, and $5,000 per

intentional or reckless violation of the ban on sales. A prevailing party may also recover its reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses.

New York City's step here may not be the last word in New York state. The legislature is still mulling over an even more expansive statewide law, which would further regulate the collection and use of biometrics. The statewide law has been pending since January 2021 and would cover private entities (any individual, partnership, corporation, limited liability company, association, or other group, however organized) and provide for a private right of action.

Key Takeaways

- Covered commercial establishments should place a conspicuous sign at all customer entrances immediately.
- All entities in New York City that "sell, lease, trade, [or] share in exchange for anything of value" or "otherwise profit from" the "transaction of biometric identifier information" should stop doing so immediately.
- If your commercial establishment receives written notice of a signage violation, make sure to cure the violation and inform the claimant in writing within 30 days of receiving notice.

Authored By

Michael L. Yaeger

Related Practices

Cybersecurity and Privacy
Hospitality
Business Transactions
Litigation and Trials
Digital and E-Commerce Engagement and Innovation

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This

publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.