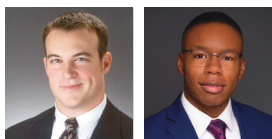


ANDERSON KILL

## Policyholder Alert

# Insurance Coverage Implications for New York City's New Biometric Information Law



By **Cort T. Malone** and  
**James A. Goodridge**

### *Key points:*

**New York City's new Biometric Identifier Information Law went into effect July 9**

**While the New York City law bans the sale of biometric data, it is less onerous than Illinois' Biometric Information Privacy Act**

**As long as notice is posted properly, New York City businesses may collect biometric information without violating the new law**

New York City's **Biometric Identifier Information Law** (the "BII Law"), which went into effect on July 9, 2021, bans the sale of biometric data and imposes notice requirements on covered businesses that use biometric identifying technology in their establishments. While comparisons have been made to the Illinois Biometric Information Privacy Act ("BIPA"), New York City's new BII Law — providing a cure period for certain violations and permitting collection of biometric data without written consent — is far less stringent and is not expected to produce the maelstrom of litigation precipitated by BIPA. That said, policyholders still should be aware of the BII Law's requirements and consider potential insurance coverage implications.

### **Background**

The new BII Law imposes two main requirements. First, covered businesses may not sell, lease, share for value, or otherwise profit from the transmission of biometric identifier information. Second, covered businesses that collect, retain, convert, store, or share biometric identifier information must post



conspicuous signage at all customer entrances disclosing that such information is being collected.

The BII Law defines "biometric identifier information" as any "physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan; (ii) a fingerprint or voiceprint; (iii) a scan of hand or face geometry; or (iv) any other identifying characteristic."

The new BII Law applies to "commercial establishments" in New York City, defined as places of entertainment, retail stores, and food and drink es-

tablishments. Financial institutions are exempt from the posting requirement, while government entities, employees, and agents are exempt entirely.

Notably, as long as notice is posted, businesses may collect biometric information without violating the BII Law. Written consent is not required before collecting such information. Moreover, a business may use CCTV systems that collect biometric information, as long as the footage is (i) not analyzed to identify persons based on “biological characteristics” (e.g., with facial recognition software), and (ii) not sold or shared with third parties.

## Violations

The BII Law provides a private right of action to parties “aggrieved” by violations, but includes a 30-day cure period for businesses accused of violating the posting requirement. Further, any party alleging a posting violation must provide written notice to the business before bringing its claim. Importantly, however, written notice is not required before bringing claims for the illegal sale or sharing of biometric information, and there is no cure period for such claims. Prevailing claimants can recover \$500 per posting violation, \$500 per negligent selling violation, and \$5,000 per intentional or reckless selling violation.

## Coverage Implications

While claims involving the BII Law have yet to be litigated, one important insurance concept involved is that of invasion of privacy. The Personal and Advertising Injury Coverage within general liability policies includes coverage for invasion of privacy. This insurance applies to “personal injury,” which typically is defined as “injury,

other than ‘bodily injury’, arising out of . . . [o]ral or written publication of material that violates a person’s right of privacy.”

The first round of Illinois insurance coverage decisions under BIPA, including *West Bend Mutual Ins. Co. v. Krishna Schaumburg Tan*, 2021 IL 125978 (2021), favored policyholders and provided precedent that coverage for violations of the BII Law should be available under similar general liability policy language.

Biometric measures are regularly used in various work environments, and many employee biometric claims have been brought under BIPA. These claims may be covered under employment practices insurance policies. Claims under the BII Law may also trigger coverage under Directors’ and Officers’ and cyber policies. It will be critical for policyholders to examine all potentially responsive insurance in the face of claims under New York City’s BII Law.

The biggest hurdles for companies seeking insurance coverage for biometric liability, under any type of policy, are potential exclusions for disclosure of confidential information and data-related liabilities. Many insurance companies have begun adding these exclusions to their policies in recent years. Business owners should be aware of these exclusions as they renew or place coverage, especially if their business collects biometric information.

## Conclusion

New York City has joined jurisdictions across the country in attempting to safeguard the use of biometric information. While the new BII Law provides a private right of action, several caveats differentiate it from the more

***Written notice is not required before bringing claims for the illegal sale or sharing of biometric information, and there is no cure period for such claims.***

onerous BIPA. New York City business owners collecting biometric information should review their insurance policies and consider potential exposure under the new BII Law when renewing or placing coverage. ▲

**CORT T. MALONE** is a shareholder in the New York and Stamford, Connecticut, offices of Anderson Kill and practices in the Insurance Recovery and the Corporate and Commercial Litigation departments. He is an experienced litigator, focusing on insurance coverage litigation and dispute

resolution, with an emphasis on commercial general liability, directors and officers, employment practices liability, advertising injury, and property insurance issues.

[cmalone@andersonkill.com](mailto:cmalone@andersonkill.com)  
(212) 278-1382

**JAMES A. GOODRIDGE** is an attorney (admission pending) in Anderson Kill's New York office. He focuses his practice on commercial litigation, employment law, and insurance recovery on behalf of Policyholders.

[jgoodridge@andersonkill.com](mailto:jgoodridge@andersonkill.com)  
(212) 278-1042

***We are interested in your feedback on topics for future articles and seminars. Please email us.***

## ***About Anderson Kill***

Anderson Kill practices law in the areas of Insurance Recovery, Commercial Litigation, Environmental Law, Estates, Trusts and Tax Services, Corporate and Securities, Antitrust, Banking and Lending, Bankruptcy and Restructuring, Real Estate and Construction, Foreign Investment Recovery, Public Law, Government Affairs, Employment and Labor Law, Captive Insurance, Intellectual Property, Corporate Tax, Hospitality, and Health Reform. Recognized nationwide by Chambers USA, and best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes – with no ties to insurance companies and has no conflicts of interest. Clients include Fortune 1000 companies, small and medium-sized businesses, governmental entities, and nonprofits as well as personal estates. The firm has offices in New York, NY, Denver, CO, Los Angeles, CA, Newark, NJ, Philadelphia, PA, Stamford, CT, and Washington, D.C.

*This publication was prepared by Anderson Kill P.C. to provide information of interest to readers. Distribution of this publication does not establish an attorney-client relationship or provide legal advice. Prior results do not guarantee a similar outcome. Future developments may supersede this information. We invite you to contact the authors with any questions. © 2020 Anderson Kill P.C.*