October 2020

ANDERSON KILL
CYBER INSURANCE
ALERT

Identifying Insurance Coverage for Alleged Violations of the Illinois Biometric Information Privacy Act

By Cort T. Malone and Vivian Costandy Michael

In 2008, Illinois passed one of the first biometric privacy laws to take effect in the United States. The Biometric Information Privacy Act[1] (BIPA) did more than usher in a new wave of biometric information privacy protections, it also ushered in a wave of class action lawsuits, with plaintiffs seeking to recover damages per the law's hefty statutory penalties. Companies that collect, store, use or disseminate biometric identifiers or information in Illinois should take stock of their insurance coverage and be aware of potential pitfalls and pressure points in their policies.

Requirements and Rationale of the Biometric Information Privacy Act

The use of biometric technology in day-to-day operations is on the rise. Whether it's a fingerprint scan to clock in and out of work, or a retinal scan to confirm access to a restricted area, companies in virtually every industry are using and storing individuals' biometric information. Consequently, more and more companies will face potential exposure under BIPA and similar legislation in other states, like New York, California, Texas and Washington.

BIPA defines biometric information as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." Biometric identifier means "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." BIPA imposes a number of requirements on private entities possessing biometric identifiers or biometric information, including requirements to:

1. Inform individuals in writing of the specific purpose and length of time for which biometric identifiers or information are being collected, stored and used.
2. Provide a publicly available retention schedule and guidelines for permanently destroying individuals' biometric identifiers or information.
3. Obtain a written release from individuals to collect, store, disseminate or otherwise use their biometric identifiers or information.

ANDERSON KILL
1251 Avenue of the Americas
New York, NY 10020
(212) 278-1000

ANDERSON KILL
1760 Market Street, Suite 600
Philadelphia, PA 19103
(267) 216-2700

ANDERSON KILL
1055 Washington Boulevard, Suite 510
Stamford, CT 06901
(203) 388-7950

ANDERSON KILL
1717 Pennsylvania Avenue, Suite 200
Washington, DC 20006
(202) 416-6500

ANDERSON KILL
One Gateway Center, Suite 1510
Newark, NJ 07102
(973) 642-5858

ANDERSON KILL
Wells Fargo Building
355 South Grand Avenue
Los Angeles, CA 90071
(213) 943-1444

www.andersonkill.com

In enacting BIPA, the Illinois legislature recognized that:

1. Biometrics are unique and, when compromised, place individuals at an increased risk for identity theft.
2. Biometric technology is new, and its ramifications are not yet fully known.
3. The public is wary of using biometrics in connection with personal information.
4. Regulating collection, use and storage of biometric identifiers and information serves the public interest.[2]

The Illinois legislature passed BIPA to codify that any private entity in possession of biometric information cannot "disclose, redisclose, or otherwise disseminate a person's ... biometric identifier or biometric information" unless the person consents to the disclosure or redisclosure.[3]

The Rapid Rise of Class Actions Following Rosenbach

BIPA imposes penalties of up to $5,000 per violation. Unlike most of the biometric privacy acts in effect today, BIPA creates a private right of action for **any** person "aggrieved" by a BIPA violation. Aggrieved persons may recover $1,000 against a private entity that "negligently" violates BIPA, or $5,000 against a private entity that "intentionally or recklessly" violates BIPA. In its much-discussed decision in *Rosenbach v. Six Flags Entertainment Corp.*,[4] the Illinois Supreme Court held that any person alleging a failure to comply with any aspect of BIPA — even in the absence of injury or harm resulting from the violation — is an "aggrieved person" under BIPA. "The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action."[5]

The Illinois Supreme Court's decision was met with a spate of putative class action filings. More than 150 class actions have been filed since Rosenbach, which was only decided in January 2019. The relative ease of asserting a BIPA claim since *Rosenbach*, and the prospect of headline-grabbing settlements, like Facebook's reported $550 million settlement, suggest that BIPA class action claims will continue to proliferate.

Insurance Coverage Considerations

Companies facing BIPA claims should consider a range of options for insurance coverage of defense costs, settlements, judgments and verdicts. BIPA claims allege a negligent or intentional invasion of privacy, often by an employer, involving sensitive personal information and systems utilizing that sensitive information. The nature of BIPA liability makes three types of policies natural contenders for coverage: commercial general liability (CGL), employment practices liability (EPL), and cyber insurance policies.

In most cases, a CGL policy is the first place to look for coverage of a class action. The broad duty to defend requires insurance compa-

who's who

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
(212) 278-1382

Vivian Costandy Michael, an attorney in Anderson Kill's New York office, concentrates her practice in insurance recovery. Vivian has helped to recover millions of dollars in insurance assets under liability and property insurance policies sold to banks, government entities, not-for-profits, Fortune 500s, medical practices and small businesses.

vmichael@andersonkill.com
(212) 278-1190

nies to provide a full and complete defense if any allegation in the complaint could conceivably be covered. Many CGL policies promise to pay "all sums" that the policyholder is legally obligated to pay because of "personal and advertising injury," which is often defined to include "publication of material that violates a person's right of privacy." One Illinois appellate court has held that this "publication" clause encompassed a BIPA plaintiff's allegation that fingerprint data was improperly provided to a third party and ruled that the insurance company had a duty to defend its policyholder.[6]

Though this decision is good news for policyholders, they still should expect insurance companies to raise a number of challenges to coverage under CGL policies. Insurance companies have brought declaratory judgment actions citing exclusions for "Access or Disclosure of Confidential or Personal Information and Data-Related Liability," "knowing" violations of rights, and "Recording and Distribution of Material" in violation of law.[7] These exclusions must be carefully analyzed in order to determine their impact on coverage.

Employment practices liability insurance policies are another valuable source of protection for companies facing BIPA liability based on biometric data practices in the workplace. EPL insurance provides coverage to employers for claims made by employees regarding defined sets of wrongful acts. Many claims are brought by employees alleging that their biometric identifiers and information were improperly collected, used or stored by the employer without the employees' written consent. Because this is not the typical fact pattern that EPL insurance companies expect to encounter, and these policies are less standardized than CGL policies, policyholders can expect some resistance to their BIPA-related claims, such as arguments regarding whether plaintiffs meet an EPL policy's definitions of "employee" or "independent contractor." Many EPL policies include "invasion of privacy" in the policy's definition of "wrongful act," which ought to give policyholders a strong argument for coverage of potential BIPA liabilities.

Cyber insurance may also be an avenue for coverage of BIPA claims, depending on the specific terms of the policy. While biometric data should fall squarely within a cyber policy's definition of confidential information or data, cyber insurance policies are not yet standardized and need to be scrutinized carefully. The scope of coverage under a cyber policy may depend on several policy provisions, but policyholders with potential BIPA liabilities should be especially wary of exclusions for claims "alleging, based upon, arising out of or attributable to the unlawful collection" of confidential information.

Third parties may also have a duty to provide insurance for any losses arising from a BIPA claim. Some policyholders hire third-party data companies to maintain their biometric scanning systems. Under the terms of the contract between the policyholder and the third-party data company, policyholders with exposure to BIPA claims may have the benefit of being an additional insured on the data company's insurance policies. Policyholders should request and maintain complete copies of the policies on which they are listed as an additional insured, and confirm that there is adequate insurance for potential future BIPA claims.

Whether a company is already facing BIPA claims, or may face such claims in the future because it collects, uses or stores biometric information, it is critical to understand the possible insurance that may respond and provide valuable coverage. Companies should work with their brokers and experienced insurance recovery counsel to ensure the best protection from this expanding universe of potentially damaging claims.

1 740 ILCS 14/1 et seq.
2 740 ILCS 14/5(c)-(g)
3 740 ILCS 14/15(d).
4 *Rosenbach v. Six Flags Entertainment Corp.*, 129 N.E.3d 1197 (Ill. 2019).
5 *Id.* at 1206.
6 *West Bend Mut. Ins. Co. v. Krishna Schaumburg,* No. 1-19-1834, 2020 IL App (1st) 191834 (Mar. 20, 2020).
7 *See* Complaints in *Westfield Ins. Co. v. Caputo's New Farm Produce, Inc.*, 2019CH00232 (Ill. Cir. Ct.) (Jan. 8, 2019); *Depositors Ins. Co. v. Joliet Hi Hotels, et al.*, No. 1:19-cv-07480 (N.D. Ill.) (Nov. 12, 2019); and *Am. Guar. Liability & Ins. Co. v. Toms King LLC et al.*, 2020CH04472 (Ill. Cir. Ct. June 5, 2020).