Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Illinois Biometrics Privacy Suits Bring Insurance Questions

By **Jonathan Schwartz and Colin Willmott**

Jonathan Schwartz

Colin Willmott

In the past two years, we witnessed a wave of putative class action lawsuits filed under Illinois' Biometric Information Privacy Act ("BIPA") (740 ILCS 14/1 et seq.), with the rate of filings increasing exponentially in the past few months. The epicenter of these filings has been Chicago, Illinois, home of the plaintiff-friendly Circuit Court of Cook County and the larger division of the United States District Court for the Northern District of Illinois, where dozens of these suits are now being litigated.

Insurers should take note given the significant potential exposure from these suits and the incentive for policyholders to seek out alternatives to funding their own defense and potential settlement of these suits. Because BIPA class action lawsuits do not fit neatly in any one existing insurance product, insurers can expect policyholders to insist on coverage positions with respect to various policies, including commercial general liability ("CGL"), employment practices liability ("EPLI") and cyber liability insurance policies. This article will generally address insurers' potential coverage obligations under each policy. Since BIPA suits are in their nascent stages, and each defendant likely has a different workplace security system and set of employee disclosures, coverage should be determined on a case-by-case basis — there is no one-size-fits-all approach to these claims.

Why Are There So Many BIPA Class Actions?

BIPA was enacted in 2008 to regulate the manner in which private entities collect and store biometric information. The Illinois legislature passed the statute in response to the increased use of biometrics in the private sector and the reality that if a person's unique biometric information is comprised, "the individual has no resource" and "is at heightened risk for identity theft." 740 ILCS 14/5(a), (c). The specific information regulated by BIPA is, without more, retina or iris scans, fingerprints, voiceprints, and scans of hand or facial geometry. 740 ILCS 14/10.

BIPA places a heavy onus on private entities to develop a publicly available written policy regarding the retention schedule for the collected biometric information and guidelines for permanently destroying the information. 740 ILCS 14/15(a). Critically, BIPA does not allow a private entity to collect, capture, purchase, receive through trade or otherwise obtain a person/customer's biometric information unless it:

1. Informs the subject or subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
2. Informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored and used; and
3. Receives a written release executed by the subject of the biometric identifier of biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b). BIPA also completely prohibits a private entity from selling, leasing, trading or profiting from a person's biometric information. 740 ILCS 14/15(c). BIPA further prohibits the disclosure or dissemination of a person's biometric information absent informed consent, the purpose of completing a financial transaction, and a legal obligation by the private entity to disclose the information. 740 ILCS 14/15(d).

The bulk of the class actions filed under BIPA concern employers' time-keeping systems and the use of fingerprint recognition technology to monitor employees' work hours.[1] Employers created such systems to avoid "buddy punching" (where someone "punches in" for a co-worker who is late) and to improve workplace safety (e.g., it is much more difficult to circumvent a biometric scanner than to steal someone's key card). Employees contend they did not consent to these systems and the collection of their biometric data.

For employees aggrieved by a violation of the statute, BIPA stands alone nationwide in creating a private right of action.[2] In fact, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000 or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20. Thus, the exposure from these rapidly proliferating BIPA class actions is incredible, especially since no court has examined the line between negligent and reckless violations of the statute.

The exposure for businesses whose employees clock in and out every day is even greater. For a business with only 50 employees, the sought-after damages from violations could arguably amount to $100,000 per day. Further, BIPA lacks an express statute of limitations, which leaves businesses uncertain as to their total exposure. Even more disconcerting for policyholders and their insurers, BIPA allows for the recovery of attorneys' fees and costs, including expert witness fees and other litigation expenses. Id. At bottom, the multiple avenues of recovery for classes and their counsel make BIPA highly attractive, which explains in part the recent flurry of putative class actions filed against myriad businesses, including a trucking company, restaurants, hotels, an airline cargo handling company, an ambulance company, a supermarket chain, a video game company and a gas station.[3]

Is There Coverage Available for BIPA Claims?

Policyholders can be expected to seek coverage for BIPA claims under their CGL, EPLI and cyberliability policies. CGL policies represent an uphill battle. First, it is unclear how BIPA claims satisfy the "publication" element of the privacy offense under Coverage B's definition of "personal and advertising injury." To satisfy the privacy offense, BIPA claims must set forth the "oral or written publication, in any manner, of material that violates a person's right of privacy." Absent dissemination of an employee's biometric information to a third party, it would stand to reason that the "publication" element would not be met. Second, a host of exclusions should bar coverage entirely for BIPA claims, whether brought under Coverage A's bodily injury coverage or Coverage B's personal and advertising injury coverage. They include the Recording and Distribution of Material or Information in Violation of Law Exclusion ("violation of law exclusion"), which applies to the collecting, recording, transmitting and distributing of information; the Employment-Related Practices Exclusion, which applies to employment-related practices, policies, actions or omissions; and the Access or Disclosure of Confidential or Personal Information and Data-Related Liability Exclusion ("disclosure of confidential information exclusion"), which applies to disclosure of a person's confidential or personal information. In sum, reliance on commercial general liability policies, including those issued before the addition of the disclosure of confidential information exclusion in 2013, would be mistaken under these circumstances.

The availability of coverage under EPLI policies presents more of an unknown in contrast to CGL policies. EPLI policies are not standardized, so the availability of coverage should come down to the exclusions included in the policy. Importantly, many EPLI policies provide coverage for workplace invasions of privacy under the definition of "wrongful act." And, only some EPLI policies contain provisions similar to the violation of law exclusion.

While cyber liability coverage may be available for some policyholders, it should not be available for most, depending on the allegations of the complaint in the class action. Policyholder lawyers opine that the clearest path to coverage for BIPA violations may be a specialty cyber insurance policy.[4]

Admittedly, cyber insurance policies do cover privacy breaches under certain circumstances, and biometric information could theoretically satisfy the policy definition of confidential or personal information protected from disclosure to the public. And, these authors have found one cyber liability policy that might respond to BIPA class actions based on the mere unlawful collection of biometric information. Yet, these authors found four cyber liability policies that would not respond to BIPA class actions based on the mere unlawful collection of biometric information. Those policies either exclude claims based on the unauthorized collection of data, contain an exclusion akin to the violation of law exclusion, or exclude employee claims where their personal information was not allegedly disseminated. At bottom, although cyber insurance, like EPLI, is not standardized and can be customized to a policyholder's needs, based on these authors' canvassing of available cyber insurance policy wordings, it would seem that cyber insurers did not intend to cover claims resulting from BIPA class actions.

Nonetheless, a recent development could make cyber insurance a more realistic option for policyholders facing BIPA class actions. That is, putative BIPA classes are now alleging that employers hire third parties to maintain their biometric scanning systems and disclose to or share with them their employees' biometric information. Whether true or not, policyholders would point to this allegation as dispositive of a cyber insurer's duty to defend the employer. Depending on the truth of the allegation and the actual relationship between the employer and the third party, this could have a significant impact on a cyber insurer's duty to indemnify the employer, as well. Therefore, paying close attention to the specific allegations of these BIPA class action complaints is a must.

With the number of BIPA lawsuits still increasing unabated, insurers with tech-savvy policyholders who do business in Illinois should be mindful of the continuing deluge of BIPA class actions. Although, these cases are in their nascent stages, with courts still determining fundamental jurisdiction and enforcement questions, including whether BIPA class actions support federal subject matter jurisdiction and whether BIPA applies extraterritorially. Hence, whether these claims are entirely defensible is yet to be seen. Likewise, whether there is coverage for these claims under EPLI and cyber insurance policies will depend on both the exact wording of the policy and complaint. One thing we can all be certain of in light of the rapid proliferation of BIPA class actions and the resultant unsettled coverage questions, litigation over coverage for these BIPA claims is just over the horizon.

Jonathan L. Schwartz is a partner in the global insurance services practice group of Goldberg Segalla LLP, residing in the firm's Chicago office. Colin B. Willmott is an associate in the firm's Chicago office.

[1] While the vast majority of class actions filed under BIPA involve workplace privacy claims, there are also high profile class actions pending against Facebook, Google, Shutterfly and others, which were brought by consumers in response to these companies' use of facial recognition technology and other like technologies that rely on biometric information.

[2] For instance, Texas and Washington have biometric information protection statutes, but neither statute contains a private right of action. Tex. Bus. & Com. Code Ann. § 503.001; Wash. Rev. Code Ann. § 19.375.

[3] Some commentators more hopefully attribute the new wave of class actions to heightened consumer awareness of data privacy and security, especially following the Equifax data breach. Other than the obvious financial incentive associated with these lawsuits, a more likely reason for the rise in these suits is that implementing a biometric-based system is much more affordable now than in 2008, which has led companies to avail themselves of the security benefits associated with these more precise systems.

[4]Sistrunk, Jeff, "A Guide To Insurance Coverage for Biometric Privacy Suits," Law360, November 6,

2017.