INSURANCE COVERAGE
SECTION OF LITIGATION

Spring 2020, Vol. 30 No. 2

Maximizing Coverage amid the Biometric Liability Wave

By Pamela Hans, John Lacey, and Marc Schein

In the last two years, a wave of class action lawsuits alleging violations under the Illinois Biometric Information Privacy Act (BIPA), [1] has flooded state and federal courts in Illinois. In 2008, BIPA was enacted because the Illinois legislature understood the importance of regulating biometric information and preventing that information from getting into the wrong hands. As it turns out, Illinois was ahead of the curve, and now several states are considering following Illinois's lead.

Meanwhile, BIPA remains possibly the most significant piece of legislation regulating biometrics, in part because it is the only current legislation that provides aggrieved individuals a private right of action against businesses that fail to properly handle biometric information. In fact, BIPA provides statutory penalties of up to $5,000 for intentional or reckless violations of the act.

In recent years, biometric technology has exploded. By 2025, the industry is projected to be worth as much as $59 billion. [2] Companies everywhere are using face recognition devices, iris recognition devices, fingerprint scanners, voice recognition devices, and hand geometry applications that capture an individual's biometric information after each use. Biometrics have infiltrated virtually every industry, including automotive, financial services, health care, food and beverage, hospitality, retail, border control, law enforcement, and education. As a result, more and more companies will face potential exposure under current legislation and will face further potential exposure as more states consider whether to implement legislation aimed at regulating the use of biometric information.

The recent wave of BIPA class action lawsuits is, in part, a result of the Illinois Supreme Court's decision in *Rosenbach v. Six Flags Entertainment Corp*., [3] which held that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under [BIPA], in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief." Plaintiffs are now emboldened to bring more class action lawsuits because the plaintiff need not show an actual injury. Rather, a mere technical violation of BIPA will suffice.

Many companies like Google, Facebook, WeWork, Southwest Airlines, and others have found themselves entangled in these lawsuits, and the potential exposure is astronomical. For example, earlier this year, Facebook agreed to settle a class action lawsuit for alleged violations under BIPA for $550 million. The prospect of that level of exposure is alarming.

Therefore, it is critical that all policyholders handling biometric information take the appropriate steps now to protect against massive exposure in the future. These steps include (1) staying abreast of all legislation in this arena; (2) ensuring that internal compliance is up to date; and (3) consulting with insurance brokers, risk managers, and coverage counsel to maximize the potential for coverage in the event a policyholder finds itself named in a BIPA lawsuit.

Background

In 2008, the Illinois legislature recognized that the use of biometrics was growing, in particular within the business and security screening sectors. In passing BIPA, the Illinois legislature determined that (1) biometrics are unique and, when compromised, place individuals at an increased risk for identity theft; (2) biometric technology is new, and "[t]he full ramifications of biometric technology are not fully known"; (3) the public is "weary" of using biometrics in connection with personal information; and (4) regulating biometric collection, use, and storage serves the public interest.[4] To those ends, BIPA prevents any private entity in possession of biometric information from "disclos[ing], redisclos[ing], or otherwise disseminat[ing] a person's . . . biometric identifier or biometric information" unless the person consents to the disclosure or redisclosure.[5]

Private entities in possession of biometric identifiers or biometric information are subject to various requirements; among them, developing a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information and making that schedule available to the public.

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."

As noted, violations of BIPA pack a punch. Namely, any person "aggrieved" by a violation of BIPA may recover for each violation $1,000 "against a private entity

that negligently violates BIPA" or $5,000 "against a private entity that intentionally or recklessly violates [BIPA]."

Similar Legislation

BIPA is among several legislative initiatives aimed at regulating entities that handle biometric information. In the years since Illinois enacted BIPA, several states have enacted, or are considering enacting, legislation similar to BIPA. Currently, Texas, Washington, New York, and just recently, California, have enacted laws aimed at regulating the use and dissemination of biometric information. Other states, like New Jersey and Florida, are considering similar legislation, but that proposed legislation has not yet become law. As technology continues to advance, so too will legislation aimed at regulating companies that handle biometric information. More and more states will continue to pass their own versions of BIPA that will affect the legal landscape nationally.

BIPA Cases

As noted above, BIPA litigation has exploded. As states continue to pass new legislation geared toward regulating the use of biometric information, litigation will indeed increase. Inevitably, coverage litigation will increase, and already certain themes are beginning to take shape.

Set forth below are three recent insurance coverage cases that highlight emerging themes concerning insurance companies' strategy in defending these claims. Two cases involve commercial general liability policies, while the third case involves an employment practices liability policy. The first case involves a coverage dispute concerning two underlying class action suits, each alleging one count for alleged violations of BIPA. The second case involves a coverage dispute concerning an underlying class action suit alleging one count for alleged violations of BIPA and a second count for negligence. The third case involves a coverage dispute concerning an underlying BIPA class action suit. Insurance companies filed all three complaints.

United States Fire Insurance Co. v. Xanitos. *Xanitos* involved two class action complaints. Each underlying complaint contained one count and alleged BIPA violations. After receiving notice of the two underlying complaints, United States Fire Insurance Company (USFIC) disclaimed coverage. The policy at issue was a commercial general liability policy. Thereafter, USFIC filed a complaint against Xanitos, seeking a declaration that it did not owe a duty to either defend or indemnify Xanitos in the underlying claims. In its complaint, USFIC alleged that the underlying claims did not fall within the insuring agreement, but even if they did,

coverage was precluded by several exclusions in the policy. Two of those exclusions will are addressed in turn below.

The first exclusion USFIC relied on was the "Access Or Disclosure Of Confidential Or Personal Information And Data-related Liability" exclusion. That exclusion concerned claims for

> [d]amages arising out of: (1) [a]ny access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of non-public information; or (2) the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

The exclusion defined "electronic data" as "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."

The second exclusion USFIC relied on was in the "personal and advertising injury" coverage. That exclusion concerned claims alleging

> [p]ersonal and advertising injury . . . arising directly or indirectly out of any action or omission that violates or is alleged to violate . . . (4) [a]ny federal, state or local statute, ordinance or regulation, other than the TCPA, CAN-SPAM Act of 2003 or FCRA and their amendments and additions, that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information.

The policy defined "personal and advertising injury" as "injury, including consequential 'bodily injury', arising out of . . . [o]ral or written publication, in any manner, of material that violates a person's right of privacy."

Although the *Xanitos* case remains inactive, the USFIC complaint demonstrates which exclusions insurance companies will rely on in the commercial general liability policy context to side-step their coverage obligations.

Zurich v. Omnicell. On August 30, 2018, Zurich American Insurance Company and American Guarantee & Liability Company filed a complaint against Omnicell, Inc.,

seeking a declaration that they did not owe a duty to defend or indemnify an underlying claim for alleged violations under BIPA. Notably, Zurich agreed to defend Omnicell subject to a reservation of rights before ultimately filing its complaint against Omnicell. Zurich then filed a claim against Omnicell for reimbursement of its defense costs.

The plaintiff in the underlying action alleged, inter alia, that (1) employees of a Chicago-area hospital were required to have their fingerprints scanned by a biometric device in order to gain access to stored materials, i.e., medication dispensing systems, that, in turn, would authorize employees to dispense medications to patients at the hospital; (2) the hospital failed to inform its employees that it discloses employees' fingerprint data to at least two out-of-state vendors, including Omnicell; and (3) Omnicell, the provider of the biometric device, failed to inform the employees of the purposes and duration for which it collects the biometric data.

The insurance companies argued that they owed no duty to defend or indemnify Omnicell in the underlying action because several exclusions barred coverage, including exclusions similar to those relied on in the *Xanitos* case.

On January 29, 2020, Zurich, American Guarantee & Liability, and Omnicell filed a joint notice of settlement indicating the parties had reached a settlement in principle.

Church Mutual v. Triad Senior Living, Inc. On November 18, 2019, Church Mutual Insurance Company filed a complaint against Triad Senior Living, Inc., seeking a declaration that it did not owe coverage for an underlying class action suit alleging BIPA violations.

The plaintiff in the underlying action was an employee of Triad. She alleged, among other things, that when Triad hires employees, they are enrolled in a database requiring fingerprint scans to monitor when they clock in and clock out. The plaintiff further alleged that Triad disclosed the fingerprint data to at least one third-party vendor for payroll purposes in violation of BIPA.

Church had issued two multi-peril insurance policies to Triad. Those policies contained various coverage parts, including employment practices liability coverage; directors', officers', and trustees' liability coverage; affiliated entity dispute legal defense coverage; senior living facility liability coverage; and general liability coverage, which included bodily injury and property damage liability coverage and personal and advertising injury liability coverage. Church addressed each of these coverage parts in denying coverage for the underlying claim.

Ultimately, Church filed a notice of voluntary dismissal on February 6, 2020, and the case remains inactive. Nonetheless, the Church complaint provides a comprehensive look into which exclusions insurance companies will rely on to side-step their coverage obligations in connection with underlying BIPA claims. The pertinent exclusions relied on by Church are addressed in turn below.

First, Church argued that two exclusions under the employment practices liability coverage part precluded coverage. The two exclusions relied on by Church were the "Violation of Laws Applicable to Employers" exclusion and the "Dishonest, Criminal or Fraudulent Acts" exclusion.

As to the former, Church, like the insurance companies in *Xanitos* and *Zurich*, relied on broadly worded exclusionary language concerning statutory violations to deny coverage. As to the latter, Church argued the underlying BIPA claim was precluded because the underlying claim was "[a]ny claim based on or attributable to, or arising out of any actual or alleged dishonest, criminal, or fraudulent acts, or the willful failure to comply with any law."

This case provides another example of an insurance company relying on broadly worded exclusionary language concerning statutory violations. Therefore, it is imperative that all policyholders review their policies for these exclusions. And, if the exclusion is not clear, policyholders should consult with their insurance brokers or risk managers immediately.

Second, Church argued that two exclusions under the directors', officers', and trustees' liability coverage part precluded coverage. The two exclusions relied on by Church were, again, a statutory violation exclusion and an employee and employment exclusion that excluded "any claim arising out of injury to an employee of any insured arising out of employment by any insured."

Third, Church argued coverage was excluded under the senior living facility liability coverage part. The exclusion read, in pertinent part, that "[t]his insurance does not apply to . . . injury to . . . [a]n employee of the insured arising out of and in the course of employment by the insured."

Fourth, Church argued coverage was excluded under the personal injury and advertising injury liability coverage part. Namely, Church relied on the following exclusion: "This insurance does not apply to personal injury to an employee of the insured if it occurs in the course of employment by the insured. Personal injury is

defined, in pertinent part, as 'Oral or written publication of material that violates a person's right of privacy.'"

Finally, Church also argued coverage was excluded under a cyber liability exclusion, which modified the general liability coverage part. In relevant part, the cyber liability exclusion provided:

> This insurance does not apply to any of the following: 1) damages arising out of any access to or disclosure of any person's or organization's confidential or personal information; 2) personal injury arising directly or indirectly out of any action or omission that violates or is alleged to violate any federal, state, or local statute, ordinance or regulation.

Takeaways from the BIPA Cases

Several key takeaways arise from *Xanitos*, *Zurich*, and *Triad*. First, as with all potential claims, policyholders should always immediately provide notice under all potentially applicable insurance policies, even if the possibility of coverage under those policies is remote. Second, if an insurance company seeks to disclaim coverage based on statutory violations (such as BIPA violations), it is imperative that policyholders closely examine their current insurance policies and ask their insurance brokers or risk managers how those policies would respond to BIPA claims. Third, any private entity sued for alleged BIPA claims should carefully review the underlying complaint. Generally, insurance companies have a broad duty to defend. In other words, even if the complaint primarily alleges statutory violations, the allegations in the complaint may not necessarily fall squarely within the statutory violation exclusion. In that case, insurance companies are generally required to defend a policyholder. Most jurisdictions require that exclusions be construed narrowly and against the insurance company as the drafter. Fourth, policyholders should inquire into the available market for these types of claims. As usage of biometric technology continues to increase, so too will the potential for massive exposure. Finally, the settlement of the *Zurich* case is significant. Policyholders should always challenge coverage positions taken by insurance companies particularly where, as in *Zurich*, an insurance company disclaims coverage based on statutory violations. Finally, in providing notice under all potentially applicable insurance policies, a policyholder may find coverage in unexpected places. For Omnicell, pushing back against its insurance company apparently paid off and resulted in a settlement.

A Risk Management Perspective

The privacy and network security marketplace has more than doubled in the last five years. Marsh USA found that in 2015 roughly 19 percent of its clients procured privacy and network SimCity insurance (cyber insurance). In 2019, Marsh USA found that its clients procuring cyber insurance increased to 38 percent. As of today, there are over 200 carriers offering stand-alone cyber insurance policies. This increase in capacity has driven costs down in the middle market space. This is due to supply-side economics: The demand has not crossed the equilibrium point so that a supply-side economics issue exists. Consequently, the global accounts marketplace is now facing a hardening market as carriers are less willing to offer the large towers they previously were willing to offer. This is happening for several reasons—reinsurance treaties, the rise in ransomware claims, large breaches, and new regulatory legislation.

Oftentimes clients will ask how their cyber insurance policy would respond to a BIPA complaint. As in most answers in insurance, it depends. Many times, clients are not aware that their employment practices liability policy may respond as well. It's through this holistic coordination that an insured may be able to find coverage when looking to both the employment practices liability insurance and the cyber policy to respond. This may change as the employment practices liability insurance marketplace does not currently contemplate this type of biometric exposure in its pricing model. An astute insurance broker would assume that the employment practices liability insurance companies will either start to exclude this coverage or start to charge an additional premium for this exposure (or both).

Conclusion

As the BIPA wave continues to wreak havoc on companies that use biometric information, it is critical that all companies handling biometric information take preemptive measures now to prevent potentially massive exposure in the future. These same measures may be taken with respect to all legislation that regulates the use of biometric information, including the California Consumer Privacy Act, which just recently went into effect. Companies can take proactive measures in a myriad of ways, but the first step should be to verify compliance with existing legislation. Companies should also keep abreast of developing legislation and, in particular, legislation that may mirror BIPA. Finally, companies should immediately consult their insurance brokers or risk managers to ascertain how their current insurance program would respond to a BIPA claim. Beware of the exclusions that preclude statutory violations, and if the scope of such an exclusion is unclear, the company should consult its insurance broker or risk manager for clarification.

If a company finds itself subject to a BIPA suit, it should immediately provide notice under all potentially applicable insurance policies, even if the possibility of coverage is remote. As BIPA claims continue to increase, coverage litigation will also increase. It is important for all policyholders to maximize the potential for coverage of these claims by taking the appropriate steps sooner rather than later.

Pamela D. Hans is a shareholder at Anderson Kill, P.C., where she is managing partner of its Philadelphia office. John Lacey is an associate in Anderson Kill's Newark office. Both represent policyholders in insurance coverage disputes. Marc D. Schein, CIC, CLCS, is national cochair of the Marsh & McLennan Agency's cyber center of excellence. He specializes in assisting clients qualify and quantify the costs potential of a data incident.

[1] 740 Ill. Comp. Stat. 14/1 et seq.

[2] "9 Industries Biometrics Technology Could Transform," *CB Insights*, Dec. 12, 2019.

[3] *Rosenbach v. Six Flags Entm't Corp.*, 432 Ill. Dec. 654, 662, 129 N.E.3d 1197, 1205 (2019).

[4] 740 Ill. Comp. Stat. 14/5(c)-(g).

[5] 740 Ill. Comp. Stat. 14/15(d).