ILLINOIS DEFENSE COUNSEL
IDC QUARTERLY

Monograph

Matthew B. Champlin
HeplerBroom LLC, Edwardsville

Georgia L. Joyce
Tressler, LLP, Chicago

Navigating the Maze of Insurance Coverage Issues in Biometric Information Privacy Act Litigation

In 2008, Illinois became the first state in the nation to enact a biometric information privacy law. For several years after its enactment, the Illinois Biometric Information Privacy Act (BIPA) went largely unutilized as a litigation tool, but as time passed and the use of biometric data became more widespread, BIPA litigation increased. Then, in 2019, the Illinois Supreme Court decided *Rosenbach v. Six Flags Entm't Corp.*, in which the court held that an individual need not allege "actual injury or adverse effect" to bring a cause of action under BIPA.[1] Instead, to be entitled to BIPA's liquidated damages and injunctive relief, a plaintiff need only prove "violation of his or her rights under the Act."[2] After *Rosenbach*, BIPA, which provides for statutory damages and attorney's fees, has provided fertile ground for class actions and massive settlements.[3] In late 2022, the first BIPA case went to verdict. That case, *Rogers v. BNSF Ry. Co.*, resulted in a $228 million judgment, based upon a jury finding that the defendant violated BIPA 45,600 times in collecting its truck drivers' fingerprint scans.[4]

Given the volume of pending BIPA claims and the potential for substantial recoveries, insurance coverage disputes abound. Unfortunately, insurance coverage jurisprudence relating to BIPA claims is thus far largely inconsistent and unreliable—to the point where judges of the same court have come to contrary conclusions concerning coverage obligations owed to the same insured.[5] While insurers have been slow to respond with changes to policy language, such changes are undoubtedly coming soon.

This Monograph examines the current state of the law and discusses the arguments for and against defense and indemnity obligations for BIPA claims. While the question of coverage for BIPA claims is most often addressed under commercial general liability (CGL) policies, this article also discusses potential coverage for such claims under directors and officers/professional liability policies, employment practices liability policies, and cyber and media liability policies. At the outset, however, one must have a general understanding of what BIPA is and how, under *Rosenbach* and its progeny, BIPA is applied.

The Illinois Biometric Information Privacy Act

When it enacted BIPA in 2008, the Illinois General Assembly determined that "public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[6] It concluded that legislative action was warranted given the growing use of biometrics in financial transactions and security screenings, and the fact that Chicago and other locations in Illinois had been selected by national corporations for pilot testing of "biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."[7] The legislature noted that an individual's unique

biometric identifiers, once compromised, cannot be changed like social security numbers.[8] Without statutory action, the legislature found individuals were at heightened risk for identity theft and would have no recourse for misuse of their biometric information.[9] Add to this a public wariness toward the use of such technology relating to financial and personal information,[10] and BIPA was born.

The requirements of BIPA apply to private individuals and entities only, and BIPA expressly excludes state or local governmental agencies and state courts from its purview.[11] The Act sets forth five requirements for private entities relating to "biometric identifiers" and "biometric information."[12] A "biometric identifier" is a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[13] "Biometric information" is defined in the Act as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometri identifier used to identify an individual.[14]"

The overarching purpose of BIPA is to protect against unauthorized publication of biometric data before it occurs.[15] To that end, the duties encompassed in BIPA relate to "the collection, retention, disclosure, and destruction of a person's or customer's biometric identifiers or biometric information."[16] Each subsection of Section 15 of the Act imposes a separate and distinct duty, and "a private entity could violate one of the duties while adhering to the others."[17] For example, an entity "would violate section 15(a) by failing to develop a written policy establishing a retention schedule and destruction guidelines," or "section 15(b) by collecting or obtaining biometric data without written notice and release."[18] Section 15(c) prohibits the sale, lease, trade, or profit from biometric data, and section 15(d) "is violated by disclosing or otherwise disseminating such data" absent certain prerequisites.[19] An entity violates section 15(e) "by not taking reasonable care in storing, transmitting, and protecting biometric data."[20]

The Act's statutory damages make it particularly appealing for potential litigants and class action counsel. Specifically, BIPA provides that "[a]ny person aggrieved by a violation" of the Act may recover: (a) "liquidated damages of $1,000 or actual damages, whichever is greater," for a negligent violation; (b) "liquidated damages of $5,000 or actual damages, whichever is greater," for an intentional or reckless violation; (c) attorneys' fees, costs, and expenses; and (d) injunctive relief or other appropriate relief determined by the court.[21]

In *Rosenbach*, the Illinois Supreme Court concluded that the "aggrieved by" language set forth above, by its plain language, does not require an individual to demonstrate "some actual injury or damage beyond infringement of the rights afforded [by the Act]."[22] Post-*Rosenbach*, a plaintiff may assert a BIPA violation and recover liquidated damages and attorneys' fees, despite sustaining no actual injury or damages. A plaintiff may recover these liquidated damages—$1,000 or $5,000 depending on the nature of the defendant's conduct—for *each violation* of the Act.[23]

The question of when a BIPA claim accrues—and the corollary question of how many violations an individual may claim—were important questions recently answered by the Illinois Supreme Court in *Cothron v. White Castle Sys., Inc.*[24] As discussed in detail below in this article, the *Cothron* court held that an action accrues every time a scan or transmission of biometric data occurs, as opposed to simply the first time the biometric information is collected or transmitted.[25] This interpretation is yet another blow to private entities and their insurers. With each scan and transmission being a separate and discreet violation of the Act, the door is now open for exponentially larger class action verdicts and settlements.

The Illinois Supreme Court has also held that that an employee's cause of action under BIPA is not preempted by the Illinois Workers' Compensation Act,[26] that a CGL insurer owed a duty to its insured to defend against a BIPA class action,[27] and that a five-year statute of limitations applies to BIPA claims.[28] Later this year, the court will address whether the Labor Management Relations Act, 29 U.S.C. § 185, preempts BIPA claims brought by collective bargaining unit employees.[29] Similar novel issues are making their way through the Illinois Appellate Court, including the question of whether the collection of biometric information is "dissemination of information to the public" so as to trigger coverage under a media liability policy.[30]

Given the financial stakes involved, and the number and variety of unanswered legal questions surrounding BIPA, it is not surprising that defendants facing BIPA lawsuits aggressively pursue insurance coverage for these claims. Largely, insureds have been successful in securing duty to defend findings against their insurers, but even then, the law is inconsistent. And law relating to an insurer's indemnity obligations for BIPA claims is unestablished.[31]

Insurance Coverage for BIPA Claims

The context in which BIPA-related insurance coverage questions most often arises is where the insured has a commercial general liability (CGL) policy. That said, other types of policies, such as directors and officers/professional liability policies, employment practices liability policies, and cyber and media liability policies, could arguably afford coverage for such claims. Each type of policy—and the current state of the law pertaining to BIPA claims asserted under each—is discussed below. Finally, statutes of limitations, claim accrual, and assessing the number of occurrences will be addressed.

Commercial General Liability Policies

Commercial general liability (CGL) policies provide coverage for "bodily injury," "property damage," and "personal and advertising injury."[32] Standard "personal and advertising injury" covers injury arising from "oral or written publication of material that violates a person's right of privacy."[33]

In *West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, the Illinois Supreme Court examined whether coverage for a BIPA lawsuit was afforded under the "personal and advertising injury" provisions of a CGL policy.[34] The *Krishna* court first addressed whether the underlying plaintiff's complaint alleged a "publication" when she pleaded that Krishna shared her biometric identifiers and information with Krishna's third-party vendor, SunLync.[35] The court noted that the policy itself did not define "publication," so it looked to dictionaries, treatises, and the Restatement to define the term.[36] In so doing, the court concluded that "the term 'publication' has at least two definitions and means both the communication of information to a single party and the communication of information to the public at large."[37] The supreme court therefore concluded that the use of the term publication in West Bend's policy was ambiguous, rejected West Bend's argument that "publication" required communication to the public, and construed the term in favor of providing coverage to Krishna.[38]

The *Krishna* court went on to analyze whether the underlying plaintiff had alleged a violation of her "right of privacy."[39] Similar to "publication," "right of privacy" was not defined in the policy.[40] The court noted that the right of privacy includes two primary interests: (a) secrecy—"the right to keep certain information confidential"; and (b) seclusion—"the right to be left alone and protecting a person from another's prying into their physical boundaries or affairs."[41] The underlying plaintiff in *Krishna* alleged disclosure of her biometric information to SunLync.[42] BIPA codified the plaintiff's right to privacy in that information, and disclosure of the information without her consent necessarily violated her right of privacy.[43] For that reason, the court held that the underlying lawsuit potentially fell within West Bend's coverage.[44]

Even assuming, however, that an alleged BIPA violation constitutes a personal and advertising injury, there are still several common exclusions that may operate to preclude insurance coverage. Since *Krishna*, insurers have based denials of coverage on three common CGL exclusions: (1) the recording and distribution of material or information in violation of law exclusion; (2) the access or disclosure of confidential or personal information exclusion; and (3) the employment

practices exclusion. Whereas the insured bears the burden of proving a claim falls within coverage, "the insurer has the burden of proving that the loss was limited or excluded by a contract provision."[45]

Recording and Distribution of Material or Information in Violation of Law Exclusion

In addition to holding that the underlying plaintiff's BIPA claim in *Krishna* fell within West Bend's personal and advertising injury coverage, the Illinois Supreme Court also rejected West Bend's attempted reliance on a recording and distribution of material or information in violation of law exclusion.[46] This exclusion began appearing in CGL policies in 2006 in response to the influx of claims under the Telephone Consumer Protection Act (TCPA) and similar statutes.[47] The version of the exclusion at play in *Krishna* stated:

> This insurance does not apply to:
> DISTRIBUTION OF MATERIAL IN VIOLATION OF STATUTES
> 'Bodily injury', 'property damage', 'personal injury' or 'advertising injury' arising directly or indirectly out of any action or omission that violates or is alleged to violate:
> (1) The Telephone Consumer Protection Act (TCPA) [(47 U.S.C. § 227 (2018))], including any amendment of or addition to such law; or
> (2) The CAN-SPAM Act of 2003 [(15 U.S.C. § 7701 (Supp. III 2004))], including any amendment of or addition to such law; or
> (3) *Any statute, ordinance or regulation, other than the TCPA or CAN-SPAM Act of 2003, that prohibits or limits the sending, transmitting, communicating or distribution of material or information.*[48]

The *Krishna* court began its analysis with the title of the exclusion—"Violation of Statutes that Govern E-Mails, Fax, Phone Calls *or Other Methods* of Sending Material or Information."[49] The court noted that the title of the exclusion only referenced methods of communication.[50] Likewise, the two statutes specifically identified in the exclusion regulate methods of communication; the TCPA pertains to phone calls and the CAN-SPAM Act pertains to e-mails.[51]

The "other than" language contained in sub-paragraph (3) of the exclusion followed the enumeration of words with a specific meaning—the TCPA and the CAN-SPAM Act.[52] For this reason, the court applied *ejusdem generis*.[53] The cannon of construction *ejusdem generis* provides that "where general words follow an enumeration of persons or things, by words of a particular and specific meaning, such general words are . . . to be held as applying only to persons or things of the same general kind or class as those specifically mentioned."[54] For the exclusion at issue, the court held the "other than" language meant "other statutes of the same general kind that regulate methods of communication like the TCPA and the CAN-SPAM Act."[55] Because BIPA does not regulate methods of communication like the TCPA and CAN-SPAM Act, the exclusion could not be read to include BIPA.[56] Finally, to the extent the "other than" language may be ambiguous, the court held it must be construed in favor of finding coverage.[57]

Courts facing recording and distribution exclusions "virtually identical" to the one in *Krishna* have consistently found that the exclusion does not bar coverage for BIPA claims.[58] But the exclusion at issue in *Krishna* was updated by ISO form CG 00 01 04 13, and now includes broader language.[59] Several courts have now confronted the following language:

> "Personal and advertising injury" arising directly or indirectly out of any action or omission that violates or is alleged to violate:
> (1) The Telephone Consumer Protection Act (TCPA), including any amendment of or addition to such law;

> (2) The CAN-SPAM Act of 2003, including any amendment of or addition to such law;
> (3) The Fair Credit Reporting Act (FCRA), and any amendment of or addition to such law, including the Fair and Accurate Credit Transactions Act (FACTA); or
> (4) Any 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.[60]

Other than the addition of FCRA claims to the exclusion, the exclusion remains virtually the same as the one before the supreme court in *Krishna*. Accordingly, several courts have held that the above exclusion does not bar coverage for BIPA claims.[61] Those courts generally reason that BIPA is not the same kind of law as the TCPA or CAN-SPAM Act of 2003, which regulate communication, or the FCRA, which regulates the use of materials such as background reports.[62] These courts resolve what they consider ambiguity in favor of coverage: "[a]t best, it is unclear whether BIPA is sufficiently similar to those other statutes; at worst, as in *Krishna*, BIPA is different in kind."[63]

One court further concluded that reading subsection (4) of the exclusion to broadly encompass BIPA claims could result in that section excluding most statutory claims and would make other policy provisions illusory:

> Most statutes "regulate ... information" to some degree. To interpret the exclusion to cover every statute that concerns a person or entity doing practically anything whatsoever with "information" would make certain coverage provisions illusory, including, for example, those that provide coverage for injuries "arising out of ... [o]ral or written publication, in any manner, of material that violates a person's right of privacy."
>
> * * *
>
> [For example, the] Policy explicitly covers slander and libel claims, false advertising claims, and claims for copyright infringement. These claims also arise under statutes—such as the Illinois Slander and Libel Act, 740 Ill. Comp. Stat. 145/0.01 *et seq.*, the Lanham Act, 15 U.S.C. § 1051 *et seq.*, and the Copyright Act, 17 U.S.C. § 101 *et seq.*—that "regulate the dissemination ... or distribution of material or information." Under [such a] construction, the Statutory Violation exclusion would bar coverage for violations of the very statutes under which slander, libel, false advertising, and copyright claims arise. The Court refuses to adopt such a nonsensical reading of the Policy.[64]

Indeed, until fairly recently, only a district court in North Carolina had applied this exclusion to BIPA claims.[65] But late last year, in *Continental Western Ins. Co. v. Cheese Merchants of Am., LLC*, an Illinois federal court took a different approach in interpreting the exclusion, and the court's analysis hinged upon the FCRA's addition to the exclusion.[66] In *Cheese Merchants*, a former employee filed a putative BIPA class action against his employer stemming from the employer's use of a biometric time tracking system that recorded the backs of employees' hands for authentication.[67] The employer's insurer, Continental Western, sought a declaration that it owed no duty to defend the lawsuit, arguing that the underlying claims were subject to several policy exclusions, including the "violation of law" exclusion.[68]

The U.S. District Court for the Northern District of Illinois noted that "other courts in this district have wrestled with [the] language" of the recording and distribution exclusion and "have landed in the same spot. Each court concluded that the exclusion does not apply to BIPA claims."[69] Recognizing that, the *Cheese Merchants* court, "[a]fter tangling with the language" of the exclusion, arrived at a different conclusion.[70]

The court, like those courts before it, started by addressing *ejusdem generis*. Indeed, recognized the court, "[f]rom a *structural* perspective, the exclusion looks like a good candidate" for the interpretative tool.[71] The problem, however, is "from a *textual* perspective, things look a bit different."[72] The court engaged in a thorough discussion of *ejusdem generis*, noting that that the cannon applies "when there is a general phrase that has a cryptic quality, where there is room for doubt about the sweep of the text."[73]

But sub-part (4) of the exclusion here is "not the type of general provision that cries out for a gap filler to fill in the cracks and give it meaning."[74] Rather "[i]t reads like a provision designed for an all-encompassing scope."[75] Stated otherwise, ". . . the text does not seem particularly ambiguous. Quite the opposite, it seems clear as a bell—and the clear message is that the provision sweeps broadly. The text is undoubtedly broad. But breadth is not the same thing as ambiguity."[76] Because the court found the text unambiguous, it concluded that the cannon of *ejusdem generis* did not apply.[77]

But the more interesting—and persuasive—portion of the court's assessment of *ejusdem generis*'s applicability came next. The court noted that *ejusdem generis* requires a "discernible principle running through all of the specifics"—a common thread.[78] Where the specifics of a list (or here, a coverage exclusion) "are so heterogeneous as to disclose no common ground . . . the canon does not apply."[79]

As the Illinois Supreme Court held in *Krishna*, both the TCPA and the CAN-SPAM Act regulate unauthorized communications that private citizens receive.[80] For that reason, BIPA "stuck out from the crowd" in *Krishna*, and, applying the cannon of *ejusdem generis*, the supreme court found the exclusion did not apply to BIPA claims.[81] But the new version of the exclusion introduces a third, specific newcomer to the mix—FCRA. "FCRA [unlike the TCPA and CAN-SPAM Act] does not govern the method of communications to consumers," but instead promotes "fair and accurate credit reporting" and ensures the safekeeping and privacy of consumers' financial information.[82] Indeed, "[i]f someone asked you about the FCRA, and asked you to name a similar statute, you probably wouldn't pick the TCPA or the CAN-SPAM Act. If you're straining to find a theme, there's probably no theme."[83]

Recognizing this apparent lack of homogeneity between the three specific laws listed in the exclusion, the court accepted that one could conceivably argue that the common theme between the laws is that they all protect privacy.[84] This would, however, require "a high level of generality" and "[i]f that's what the provision means, it sure took a long and circuitous path to say so."[85] In the end, therefore, the court concluded that the exclusion has either: (1) no theme at all; or (2) a theme with a high level of generality.[86] If it is the former, no limiting principle such as *ejusdem generis* would apply.[87] If it is the latter, the theme would necessarily be so broad as to "sweep in BIPA."[88] That said, either contractual interpretation arrives at the same result as does a plain reading of sub-section (4) of the exclusion: "the exclusion applies to BIPA claims."[89]

In adopting the *Cheese Merchants* court's analysis, the court in *State Auto Property and Casualty Ins. Co. v. Fruit Fusion, Inc.*, similarly concluded that "BIPA is a state statute that 'addresses, prohibits, or limits' the collection, retention, dissemination, and disposal of information."[90] BIPA claims, held the court, therefore fall squarely within the broad language included in sub-section (4) of the recording and distribution exclusion.[91]

While opinions to date offer competing interpretations of the recording and distribution exclusion, the *Cheese Merchants* court's contractual interpretation of the provision is logically attractive. That said, there is a compelling counterargument that the exclusion, if applied so broadly, would conceivably exclude most statutory claims—even those expressly covered elsewhere in CGL policies. While both the *Cheese Merchants* and *Fruit Fusion* courts believe the Illinois Supreme Court would subscribe to their analysis and find the new version of the exclusion to encompass BIPA claims,[92] the future of this approach is less clear.

Access or Disclosure of Confidential or Personal Information Exclusion

Adding even more uncertainty to the mix, courts are evenly divided on whether the access or disclosure of confidential or personal information exclusion applies to BIPA claims. This exclusion eliminates coverage for:

> "Personal or advertising injury" arising out of any 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 nonpublic information.*[93]

On its face, this exclusion eliminates coverage relating to claims arising from the collection or dissemination of information of a confidential, personal, or private nature. To that end, the courts holding that the exclusion applies to BIPA claims note the breadth of this plain language.[94] Indeed, "the word 'any' doesn't suggest a lot of limitations."[95] To this camp of courts, the exclusion is "bookended with breadth," and the text "does not seem ambiguous at all."[96] The fact that the exclusion contains a list of certain types of information does not change this analysis, as the list is prefaced by the word "including," meaning the "whole list is illustrative."[97] Given that BIPA's purpose is to protect privacy interests in biometric information, "[i]t is hard to see how a BIPA claim is not about protecting confidential or personal information."[98]

These courts have rejected insurers' attempts to invoke *ejusdem generis*, instead concluding that the cannon does not apply because the language is unambiguous, items introduced by "including" are not an exclusive list, and *ejusdem generis* only applies when the listed items have a "readily identifiable common thread," which is missing from this exclusion.[99] Similarly, applying *noscitur a sociis*—a broader version of *ejusdem generis* that means "coupling of words denotes they should be understood in the same general sense"—would not, in the opinion of these courts, change the result.[100] To the contrary, the only resemblance between the categories of information in the exclusion (*e.g.*, patents, credit card information, health information) is that they all pertain to information for which individuals and companies "have a heightened interest in keeping from third-parties or the public at large . . .."[101] The information protected by BIPA "certainly falls within this category."[102] In short, given the exclusion's plain language and breadth, half the courts addressing the applicability of this exclusion to BIPA claims conclude that the exclusion bars coverage.[103]

The other half of the courts addressing this question, on the other hand, utilize the cannons of *ejusdem generis* or *noscitur a sociis* and focus on the specific list of confidential or personal information contained in the exclusion.[104] These courts hold that the listed examples in the exclusion are simply not the same type of information as biometric data such as fingerprints or handprints.[105] In *Am. Family Mut. Ins. Co. v. Caremel, Inc.*, for example, the court concluded that "[t]he closest provision that could arguably be interpreted to include fingerprints would be 'health information,'" but doing so "would stretch the definition of health information to include a physical characteristic that has nothing to do with the state of health of an individual."[106] Similarly, the court in *Citizens Ins. Co. of Am. v. Thermoflex*, held that handprints did not share the same attributes of privacy and sensitivity as the types of information listed in the exclusion.[107] The court found support for this conclusion in BIPA's statutory definition of "confidential and sensitive information," which does not include any of the Act's examples of biometric identifiers.[108] These courts reason that at best the exclusion is ambiguous, and applying that ambiguity in favor of the insured, they have held that insurers owe a duty to defend against BIPA claims, despite this exclusion.[109]

In short, and unfortunately, there is little guidance one can glean from cases interpreting the access or disclosure exclusion. The district courts are evenly split on whether the exclusion operates to eliminate coverage for BIPA claims, and absent an appellate court addressing the issue, these conflicting interpretations will likely continue to permeate.

Employment Practices Exclusion

The employment practices exclusion, on the other hand, has been almost uniformly held to not apply to BIPA claims. The employment practices exclusion provides that coverage does not apply to "personal and advertising injury" to a person arising out of "*employment-related practice, policies, acts or omissions,* such as coercion, demotion, reassignment, discipline, defamation, harassment, humiliation or discrimination *directed at that person . . . .*"[110]

In the only published case to conclude that the exclusion barred coverage for BIPA claims, the district court in *Caremel* held that the exclusion applied to BIPA claims brought by Caremel employees relating to their use of a biometric time clock system.[111] There, the insurer argued the exclusion applied to eliminate coverage, because "the requirement that an employee give his fingerprints is an employment related practice."[112] Caremel countered that the exclusion was inapplicable, arguing that *ejusdem generis* applied and that the harms from BIPA are unlike any of the harms listed in the exclusion.[113] Caremel contended that the exclusion applied to practices *directed toward individuals*, and Caremel's fingerprint requirement was directed toward *all employees*.[114]

In rejecting Caremel's arguments, the court noted that the harm addressed by BIPA is one of an individual nature.[115] According to the court, it therefore follows that "a BIPA violation is of the same nature as the exemplar employment-related practices" contained in the exclusion.[116] The court held the insurer owed Caremel a duty to defend it in the underlying lawsuit.[117]

But while the collection of biometric data by employers through fingerprint scans and the like may very well be "a practice or policy, in a colloquial sense,"[118] courts examining the employment related practices exclusion since *Caremel* have universally refused to apply the exclusion to BIPA claims.[119] True, "at first glance, one might think that the exclusion applies to the use of a biometric tracking system. It's a practice at work, after all."[120] But this broad interpretation, as advocated by insurers, would, in the estimation of these courts, result in the exception swallowing the rule. "Interpreting the ERP exclusion to bar coverage for any employment-related practice that could cause harm to an employee would broadly preclude coverage for *any* claim against an employer."[121]

To the contrary, the examples of conduct listed in the employment practices exclusion all relate to *targeted mistreatment of a specific person*, and while the listed conduct "is not *exhaustive*, it is *suggestive*."[122] Indeed, the third clause of the exclusion "expressly describes the excluded conduct as conduct 'directed at that person.'"[123] In short, while using a finger to clock-in and clock-out of work may be an employment practice, "it isn't the type of practice envisioned by the full text of the provision."[124]

Any ambiguity, of course, is resolved in favor of the insured and against the insurer.[125] Absent notable changes to the employment practices exclusion, parties can be reasonably confident that this exclusion will not bar coverage for BIPA claims moving forward.

Directors and Officers/Professional Liability Policies

As of this writing, the only published opinion to address coverage for BIPA claims under a directors and officers/professional liability policy is *Twin City Fire Ins. v. Vonachen Servs*.[126] The underlying employee-plaintiffs sued Vonachen, alleging BIPA violations associated with the timeclock collection of the employees' fingerprint data.[127] Vonachen's insurer, Twin City, sought a declaration that it did not owe Vonachen a duty to defend the claims under its directors and officers liability coverage or employment practices liability coverage.[128]

The Directors, Officers and Entity Liability coverage provided that "the Insurer shall pay Loss on behalf of an Insured Entity resulting from an Entity Claim first made against such Insured Entity during the Policy Period or Extended Reporting Period, if applicable, for a Wrongful Act by an Insured Entity."[129] "Entity Claim" included any civil proceeding.[130] "Wrongful Act" meant "any actual or alleged: (1) Error, misstatement, misleading statement, act, omission, neglect, or breach of duty committed by an Insured Person in their capacity as such or in their Outside Capacity, or, with regard to Insuring Agreement (C) an Insured Entity."[131]

Twin City argued several exclusions in support of its declination of coverage. First, Twin City argued that an insured versus insured exclusion barred coverage, because the underlying plaintiffs were deemed insureds under the policy.[132] The court rejected this argument, however, finding that the exclusion specifically exempted suits resulting from whistleblowing. While the nature of the underlying plaintiffs' claims would not fall within traditional statutory definitions of whistleblowing, the definition of "whistleblowing" in Twin City's policy was broad:[133]

> "Whistleblowing" means an Insured Person's lawful act of providing information, causing information to be provided, or otherwise assisting in an investigation regarding any conduct which the Insured Person reasonably believes constitutes a violation of any federal, state or foreign law.[134]

Relying on this broad language, the *Vonachen* court concluded that the exception to the exclusion applied and that the insured versus insured exclusion did not eliminate coverage.[135]

However, directors and officers liability coverage was eliminated by Twin City's "Invasion of Privacy Exclusion."[136] This exclusion provided that Twin City "shall not pay for Loss under Insuring Agreement (C) in connection with any Claim *based upon, arising from, or in any way related to any actual or alleged . . . invasion of privacy*."[137] The court rejected Vonachen's argument that a person's right to privacy is only violated under BIPA if the biometric information is "collected surreptitiously or disseminated to third parties without the person's consent."[138] Vonachen's attempt to categorize the claims made by the underlying plaintiffs as merely procedural violations of BIPA was simply unpersuasive to the court, given the wealth of case law holding "that a BIPA violation is an invasion of privacy."[139] Twin City's invasion of privacy exclusion was broad, and it therefore eliminated directors and officers liability coverage.[140]

Employment Practices Liability Policies

The *Vonachen* court also addressed potential coverage under Twin City's employment practices liability coverage. Employment practices liability policies respond to "the dramatic increase in lawsuits arising from the employment relationship," and typically provide coverage for "claims arising as a result of discrimination, sexual harassment, wrongful termination, and other workplace torts."[141]

In *Vonachen*, the employment practices liability policy defined the wrongful acts for which it provided coverage as including "a breach of any oral, written, or implied employment contract, including, without limitation, *any obligation arising from a personnel manual, employee handbook*."[142] Vonachen's employee handbook required its employees to use the designated time-keeping system which allegedly violated BIPA, threatened discipline if the employees failed to do so, and provided that Vonachen would "comply with all applicable laws and regulations."[143] Vonachen argued that because the underlying BIPA complaint alleged breach of obligations required in its employee handbook, employment practices liability coverage was triggered.[144]

In response, Twin City argued that the handbook contained a disclaimer that it did not create contractual obligations, and the underlying complaint therefore "did not implicate the [h]andbook or a breach of contract claim."[145] According to

Twin City, Vonachen's interpretation of the policy assumed "that *any* lawsuit alleging *any* violation" would breach the handbook, and it argued that "no insurance company would knowingly write a policy that would enable the insured to trigger coverage any time it wanted a windfall."[146]

The court, recognizing that it was "a close call as to whether the underlying actions are within the EPL [c]overage," nevertheless found that the alleged conduct "potentially falls within the EPL coverage."[147] The court found that in its policy Twin City notably included coverage for breach of contract, including "*without limitation, any obligation arising from* a personnel manual, employee handbook, or policy statement."[148] In other words, the policy itself contemplated that a handbook could give rise to a contractual obligation.[149] And the policy was silent as to whether these requirements apply to the employer or employee.[150] "A plain reading of the provision would indicate that the obligations could be imposed on either."[151]

While the court declined to decide if the handbook created an employment contract, it found that a state court could conceivably conclude that it did create a contract.[152] Therefore, held the court, "the conduct alleged in the complaint is potentially or at least arguably within one or more of the categories of wrongdoing" covered by the policy.[153] If an insurer, such as Twin City, wanted to avoid assuming risks it was not willing to cover, it could have "reviewed an employee handbook prior to providing EPL coverage to employers."[154] Twin City owed a duty to defend Vonachen under the employment practices liability policy.[155]

In *Church Mut. Ins. Co. v. Prairie Village Supportive Living, LLC*, the court also assessed potential insurance coverage for BIPA claims under an employment practices liability policy.[156] The insurer, Church Mutual, sought a declaratory judgment that it owed no duty to defend or indemnify Prairie Village Supportive Living in a putative BIPA class action filed by a former Prairie Village employee.[157]

The employment liability coverage at issue provided that Church Mutual would "pay for 'loss' arising from any claim of injury arising out of a 'wrongful employment practice' to which this insurance applies."[158] "Wrongful employment practice" was defined in the policy as including "any actual or alleged . . . [e]mployment related false arrest, wrongful detention or imprisonment, malicious prosecution, libel, slander, defamation of character, or *invasion of privacy*."[159] The policy also included the following exclusion for "Violations of Laws Applicable to Employers," which excluded coverage for ERISA claims, state and local laws similar to ERISA, and:

> (3) *Any claim based on, attributable to, or arising out of any violation of any insured's responsibilities or duties required by any other federal, state, or local statutes, rules, or regulations, and any rules or regulations promulgated therefor or amendments thereto.* However this exclusion does not apply to: Title VII of the Civil Rights Act of 1964, the Americans With Disabilities Act, the Age Discrimination in Employment Act, the Equal Pay Act, the Pregnancy Discrimination Act of 1978, the Immigration Reform and Control Act of 1986, the Family and Medical Leave Act of 1993, and the Genetic Information Nondiscrimination Act of 2008 or to any rules or regulations promulgated under any of the foregoing and amendments thereto or any similar provisions of any federal, state, or local law.[160]

Church Mutual conceded that the BIPA claim alleged a "wrongful employment practice" under the policy.[161] It instead argued that the italicized language above from the Violation of Laws exclusion operated to eliminate coverage.[162] Prairie Village contended, on the other hand, that BIPA was more akin to the statutes expressly exempted from the exclusion.[163] Prairie Village argued that BIPA, like the exempted statutes, "protects employee rights," and was therefore "aligned" with those statutes.[164]

The court rejected Prairie Village's argument, noting that all of the statutes expressly exempted from the exclusion "proscribe discrimination in one form or another," and "BIPA has nothing to do with discrimination."[165] If one were to include BIPA in the list of laws exempted by the exclusion, "it would stick out like a sore thumb."[166] Because BIPA is "categorically different" from the exempted statutes, and because a BIPA claim constitutes a "claim based on, attributable to, or arising out of any violation of any insured's responsibilities or duties required by any other federal, state, or local statutes," the Violation of Laws exclusion barred coverage for the underlying lawsuit.[167]

Cyber Liability and Media Liability Policies

Finally, coverage may exist for BIPA claims under cyber liability or media liability policies. While cyber liability policies are designed to protect from loss associated with data breaches, they may cover BIPA claims depending upon the language of the policy. "The availability of coverage for a BIPA claim under a cyber liability policy will turn on how the term 'confidential information' is defined in a given policy. . . ."[168] If a policy's definition of "confidential information" includes personally identifiable information, including biometric data, BIPA claims may be covered.[169] Similarly, absent a policy definition of "confidential information" excluding biometric data, or an applicable policy exclusion for such claims, a cyber liability policy could provide coverage.[170]

Media liability coverage may be included in a cyber liability policy, or it may be provided in a freestanding policy.[171] Under a media liability policy, coverage extends to certain "wrongful acts," such as defamation or invasion of privacy.[172] "'Wrongful acts' is generally broadly defined . . . including, but not limited to, personal injury, invasion of privacy, and breach of any agreement to maintain the confidentiality of a source or any information."[173] Because of the broad definition of wrongful acts in media liability policies, it is quite possible that certain BIPA violations may be covered under these policies.

In addressing BIPA claims under a media liability policy, at least one trial court held that the media liability policy in question did not provide coverage for BIPA claims. In dismissing a coverage claim in *Remprex, LLC v. Certain Underwriters at Lloyd's, London, Syndicates 2623/623*, the Circuit Court of Cook County, Illinois held that the insured failed to demonstrate that the dissemination of fingerprint scan information was "to the public," as required for coverage under the media liability policy.[174] The insured appealed, the Illinois Appellate Court First District heard oral argument in *Remprex* on January 12, 2023, and a decision is pending.[175]

In short, there is very limited case law addressing coverage for BIPA claims under cyber liability or media liability policies. Given that the coverage provided by and language included in such policies may substantially vary from insurer to insurer, close examination should be given to these policies in assessing potential coverage. Counsel should also consider whether the existing case law concerning insurance coverage of BIPA claims under other types of polices may bolster arguments for or against coverage under a cyber or media liability policy.

Statute of Limitations, Accrual, and Assessing the Number of Occurrences

Under any of the aforementioned policies, one examining insurance coverage must also assess issues pertaining to the statute of limitations, accrual of claims, and the number of occurrences. Until very recently, the law in these areas relating to BIPA claims was unsettled. Earlier this year, however, the Illinois Supreme Court issued a pair of opinions settling—at least for the time being—these issues.

Statute of Limitations

In *Tims v. Black Horse Carriers, Inc.*, the Illinois Supreme Court examined whether the one-year limitations period in § 13-201 of the Illinois Code of Civil Procedure or the five-year period in § 13-205 of the Code applied to BIPA claims.[176]

In *Tims*, Black Horse argued that the one-year limitations period contained in § 13-201 for "[a]ctions for slander, libel or for publication of matter violating the right of privacy" should apply to BIPA claims.[177] Because claims under § 15 of BIPA are for privacy violations, Black Horse argued § 13-201 should govern BIPA claims. Conversely, the plaintiffs argued that the five-year "catchall" limitations period in § 13-205 of the Code should apply. Section 13-205 provides, in relevant part, that ". . . all civil actions not otherwise provided for, shall be commenced within 5 years next after the cause of action accrued."[178]

The supreme court began its analysis by noting that "[o]ne of the purposes of a limitations period is to reduce uncertainty and create finality and predictability in the administration of justice."[179] Giving the statutory language of BIPA its plain and ordinary meaning, the supreme court noted that "the Act was enacted to help regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[180] The court further noted there was no dispute that the fingerprint data collected by Black Horse constituted biometric identifiers subject to regulation under BIPA, and that the electronically stored version of the fingerprint data constituted biometric information within the meaning of BIPA.[181]

The supreme court analyzed all five subsections contained in § 15 of the Act and concluded that, based on the Act's plain language, all five subsections prescribed rules to regulate the collection, retention, disclosure, and destruction of biometric identifiers and biometric information.[182] The supreme court agreed with the appellate court's interpretation that subsections 15(a), 15(b), and 15(e) of BIPA "contained no words that could be defined as involving publication," and therefore, those three subsections would not fall within the one-year limitations period in § 13-201 of the Code as "publication of matter" violating a privacy right.[183] Instead, the supreme court held subsections (a), (b), and (e) are subject to the five-year catchall limitations period codified in § 13-205 of the Code.[184]

However, the supreme court went further than the appellate court. The appellate court had held that because subsections 15(c) and 15(d) contained the words "sell," "lease," "trade," "disclose," "redisclose," and "disseminate," they could be construed as involving publication and "would fall within the purview" of the one-year limitation period in § 13-201 as "publication of matter" violating a privacy right.[185] Although the supreme court agreed that the terms used in subsections (c) and (d) could be construed as involving "publication" based on the court's interpretation of that term in *Krishna*, the supreme court concluded that "it would be best" to apply the five-year catchall limitations period in § 13-205 of the Code.[186]

In reaching this conclusion, the court considered the fact that there is no limitations period set forth in BIPA, and it recognized the "goal of ensuring certainty and predictability in the administration of limitations periods that apply to causes of action under the Act."[187] In addition, the court found that the five-year limitations period contained in § 13-205 of the Code would allow a party "sufficient time to discover the violation and take action," and therefore, "would comport with the public welfare and safety aims of the General Assembly."[188] Accordingly, the supreme court held that the five-year limitations period contained in § 13-205 of the Code applies to all BIPA claims.[189]

Accrual and Number of Occurrences

In *Cothron v. White Castle Sys., Inc.*, the Illinois Supreme Court recently issued its opinion on the certified question asking: "Do section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?"[190] In a split opinion, the supreme court held "that a separate claim accrues under the Act each time a private entity scans or transmits an individual's biometric identifier or information in violation of section 15(b) or 15(d)."[191]

Cothron initially filed a proposed class action lawsuit in 2018 in the Circuit Court of Cook County on behalf of all Illinois employees of defendant White Castle Systems, Inc., and its third-party vendor, Cross Match Technologies. Cross Match Technologies removed the case to federal court under the Class Action Fairness Act of 2005, where Cothron later voluntarily dismissed Cross Match Technologies from her action and proceeded against White Castle.[192]

According to her complaint, Cothron is a manager of a White Castle restaurant in Illinois, where she has worked since 2004.[193] Cothron alleged that, not long after she began working there, White Castle introduced a system that required its employees to scan their fingerprints to access pay stubs and computers.[194] A third-party vendor verified each scan and authorized the employee's access.[195]

Cothron alleged that White Castle implemented this biometric collection system and did not seek her consent to acquire her fingerprint data until 2018, more than a decade after BIPA took effect in 2008.[196] Accordingly, Cothron asserted that White Castle unlawfully collected and disclosed her biometric data in violation of sections 15(b) and 15(d) of BIPA.[197]

Section 15(b) of BIPA provides:

> (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
> (1) informs the subject * * * in writing that a biometric identifier or biometric information is being collected or stored;
> (2) informs the subject * * * in writing of the specific purpose and length of time 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 or biometric information.[198]

Section 15(d) of BIPA provides:

> (d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> > (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure.[199]

White Castle argued that the phrase "unless it first" in section 15(b) means that claims can accrue only once—when the biometric data is initially collected or disclosed. The supreme court did not agree with White Castle that the active verbs "collect, capture, purchase, receive, and obtain" used in section 15(b), which mean to gain control, can only happen once.[200]

Similarly, White Castle argued that under section 15(d), which requires consent in order for a private entity to "disclose, redisclose or otherwise disseminate" an individual's biometrics, occurs only on the first instance of disclosure or dissemination. White Castle also argued that disclosure or dissemination means "by one party to a new, third party" who has not previously possessed the biometric information.[201]

Cothron argued, to the contrary, that "the plain meaning of the statutory language demonstrates that claims under section 15(b) and 15(d) accrue every time a private entity collects or disseminates biometrics without prior informed consent" and "consistent with the plain meaning of the statutory language, gives effect to every word in the provision, and directly reflects legislative intent to provide an individual with a meaningful and informed opportunity to decline the collection or dissemination of their biometrics."[202]

Cothron further argued that the word "first" in section 15(b) modifies the words "informs" and "receives," and therefore, "an entity violates section 15(b) when it collects, captures, or otherwise obtains a person's biometrics without prior informed consent."[203] Similarly, Cothron argued that section 15(d) prohibits the disclosure, redisclosure, or dissemination of biometrics by a private entity "unless" that entity receives prior consent. Thus, according to Cothron, a claim accrues each time biometric identifiers or information are collected or disseminated by a private entity without prior informed consent.[204]

The supreme court began its analysis by focusing on the plain and ordinary language of BIPA to ascertain the intent of the legislature.[205] The supreme court agreed with the federal district court that "[a] party violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection."[206]

The supreme court rejected White Castle's suggestion that the "unless it first" phrase in section 15(b) refers only to the first collection of biometric information. "Contrary to White Castle's position, the 'unless it first' phrase refers to the private entity's statutory obligation to obtain consent or a release," not to the triggering actions.[207]

Similar to section 15(b), the supreme court held that "section 15(d) mandates consent or legal authorization before a specific action is taken."[208] Section 15(d) provides that "[n]o private entity * * * may disclose, redisclose, or otherwise disseminate * * * biometric information unless" it obtains informed consent to disclose that information.[209] The supreme court rejected White Castle's argument that a disclosure is something that can happen only once.[210] Focusing on the terms "disclose" and "redisclose," the supreme court concluded that the term "disclose" means "to make known" or "to reveal . . . something that is secret or not generally known."[211] The supreme court further noted that the term "redisclose" as used in section 15(d) could include repeated disclosures of the same biometric data to the same third party, as opposed to White Castle's interpretation of "redisclose" as "a downstream disclosure carried out by a third party to whom information was originally disclosed."[212] Finding that it did not "have to specifically determine the meaning of 'redisclose' in section 15(d) because the other terms in that section are broad enough to include repeated transmissions to the same party," the court concluded that "a claim accrues upon each transmission of a person's biometric identifier or information without prior informed consent."[213] Accordingly, the supreme court held that "the plain language of section 15(b) and 15(d) demonstrates that such violations occur with every scan or transmission."[214]

Finally, the supreme court considered other "nontextual" arguments made by White Castle in support of its single-accrual interpretation of BIPA and "was not persuaded."[215] White Castle argued that, under Illinois law, "a claim accrues when a legal right is invaded and an injury inflicted," and that the supreme court's decisions interpreting BIPA define a "right to secrecy in and control over biometric data" and define the "injury" as loss of control or secrecy.[216] Citing *Rosenbach*, White Castle argued that BIPA allows a claim for an individual's loss of the "right to control" biometric

information and that, "once an individual loses control over the secrecy in his or her biometric information, it cannot be recreated, resulting in the loss of any confidentiality."[217]

The supreme court reasoned that *Rosenbach*, contrary to White Castle's position, "does not stand for the proposition that the 'injury' for a section 15 claim is predicated on, or otherwise limited to, an initial loss of control or privacy."[218] Instead, the supreme court stated that *Rosenbach* and subsequent decisions in *Krishna* and *McDonald* recognized that a claim under the Act is a private cause of action based exclusively on a statutory violation, which itself is the "injury" for purposes of a claim under BIPA, but rejected the argument that a claim under section 15 should be limited to the first time that a private entity scans or transmits a party's biometric identifier or biometric information.[219]

The supreme court also rejected White Castle, and *amici* supporting White Castle's conclusion, that construing section 15(b) and 15(d) to mean that a claim accrues for each scan or transmission of biometric information in violation of BIPA "could potentially result in punitive and 'astronomical' damage awards that would constitute 'annihilative liability' not contemplated by the legislature and possibly be unconstitutional."[220] The court noted White Castle's estimate that "if plaintiff is successful and allowed to bring her claims on behalf of as many as 9500 current and former White Castle employees, class-wide damages in her action may exceed $17 billion."[221] The court held that because "the statutory language clearly supports plaintiff's position, * * * it must be given effect, 'even though the consequences may be harsh, unjust, absurd or unwise.'"[222]

The supreme court discussed the balance between giving private entities "the strongest possible incentive to conform to the law" and the "financial destruction of a business," and concluded that "policy-based concerns about potentially excessive damage awards under the Act are best addressed by the legislature."[223] The supreme court, therefore, "respectfully suggest[ed] that the legislature review these policy concerns and make clear its intent regarding the assessment of damages under the Act."[224]

Relying upon the plain language of the Act, the supreme court concluded "that a claim accrues under the Act with every scan or transmission of biometric identifiers or biometric information without prior informed consent."[225]

Three justices dissented, finding that the "majority's interpretation cannot be reconciled with the plain language of the statute, the purposes behind [BIPA], or this court's case law, and it will lead to consequences that the legislature could not have intended."[226] The dissenting opinion mirrors many of the issues discussed by the Seventh Circuit in its decision certifying this case to the supreme court.[227]

Among the compelling points raised, the dissent agreed with White Castle that "Plaintiff's injury under [section] 15(b) occurred, if at all, the first time that her biometrics were collected by White Castle without her consent, not each subsequent time that her finger was rescanned."[228] The dissent found that "[t]here is only one loss of control or privacy, and this happens when the information is first obtained. * * * The majority tellingly never explains how there is any additional loss of control or privacy with subsequent scans that are used to compare the employee's fingerprint with the fingerprint that White Castle already possesses."[229]

The dissent further concluded that the analysis should be the same for section 15(d) claims requiring consent before a private entity may "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information."[230] The dissent concluded that a disclosure of biometric information "can happen only once. You can tell someone your middle name an unlimited number of times, but you can disclose it to them only once."[231] When something is "redisclosed" or "disclosed again," it necessarily must be to a different party such as downstream disclosures to third parties.[232]

In short, according to the dissent, "[t]he legislature's intent was to ensure the safe use of biometric information, not to discourage its use altogether," noting that the "construction of a statute that leads to an absurd result must be avoided."[233] The dissent discussed two significant negative consequences that could result from construing BIPA under

the majority's interpretation. First, "plaintiffs would be incentivized to delay bringing their claims as long as possible. If every scan is a separate, actionable violation, qualifying for an award of liquidated damages, then it is in a plaintiff's interest to delay bringing suit as long as possible to keep racking up damages."[234] Second, "the majority's construction of the Act could easily lead to annihilative liability for businesses."[235]

From an insurance coverage perspective, one has to question why an insurer should be obligated to provide coverage for multiple violations of BIPA, after the first disclosure of biometric data, or for continuous voluntary disclosure of biometric data that did not comport in advance with BIPA's disclosure requirements. The argument that a "one and done" violation rule will encourage further non-compliance with BIPA arguably means that the insurer should not be expected to provide coverage for subsequent "intentional" violations of BIPA.

In summary, the supreme court's decision in *Tims* clarified that the five-year limitations period contained in § 13-205 of the Code applies to all BIPA claims. And, for the time being, under *Cothron*, a separate claim accrues under BIPA each time a private entity scans or transmits an individual's biometric identifier in violation of section 15(b) or 15(d). The legislature has been invited to appropriately address this question and concerns raised by the *Cothron* dissent through legislative amendment. Unless and until that happens, however, the potential for astronomical damage awards in BIPA cases is as high as it has ever been, and battles over insurance coverage for such claims will be more important than ever.

The Future of Insurance Coverage for BIPA Claims

No doubt this year has already been one in which many questions of first impression concerning the interpretation and application of BIPA's provisions were answered. The holdings in *Tims*, *Cothron*, and anticipated decisions in several other pending cases may very well impact the common coverage disputes discussed in this article. Presumably—and hopefully—insureds and insurers will also receive further guidance this year from state and federal appellate courts or the Illinois Supreme Court relating to the application of common policy language to BIPA claims. Until then, insureds and insurers have little certainty as to whether coverage will be found by a court to exist.

It can also be expected that insurers, in an attempt to insulate themselves from the large settlements and verdicts generated by BIPA lawsuits, will rewrite policies and exclusions to eliminate or substantially reduce the likelihood for coverage for such claims. Much like the insurance industry responded to the TCPA and similar statutes through the recording and distribution exclusion, it seems inevitable that a clearer exclusion for biometric information privacy claims is forthcoming.

With that in mind, it appears the best protection for an insured is a focus upon education and compliance with BIPA's requirements. With each new multi-million-dollar settlement and verdict, the incentivization of employers, technology companies, and other private entities to comply with BIPA provisions only increases. Absent widespread and uniform compliance with BIPA, however, these lawsuits will continue to proliferate, and both defense and coverage counsel must keep abreast of the myriad new decisions on BIPA claims and the coverage questions arising therefrom.

(Endnotes)

1 *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 40.

2 *Rosenbach*, 2019 IL 123186, ¶ 40.

[3] *See*, *e.g.*, *Patel v. Facebook, Inc.*, 3:15-cv-03747 (N.D. Cal.) ($550 million class settlement); *Rivera v. Google LLC*, 2019-CH-990 (Cir. Ct. Cook County, Ill.) ($100 million class settlement); *In re: TikTok Inc. Consumer Privacy Litig.*, 1:20-cv-04699 (N.D. Ill.) ($92 million class settlement); *Boone v. Snap Inc.*, 2022-LA-708 (Cir. Ct. DuPage County, Illinois) ($35 million class settlement).

[4] *Rogers v. BNSF Ry. Co.*, 1:19-cv-03083 (N.D. Ill. Oct. 12, 2022).

[5] *See, e.g., Citizens Ins. Co. of Am. v. Thermoflex Waukegan, LLC*, 588 F. Supp. 3d 845 (N.D. Ill. March 1, 2022) (holding insurer owed duty to defend); *Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc.*, 595 F. Supp. 3d 677 (N.D. Ill. March 30, 2022) (holding insurer did not owe duty to defend); *Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc.*, 21-C-788 (N.D. Ill. Jan. 19, 2023) (holding insurer owed duty to defend under umbrella policy once primary insurance limits are exhausted).

[6] 740 ILCS 14/5(g).

[7] 740 ILCS 14/5(a) and (b).

[8] 740 ILCS 14/5(c).

[9] *Id.*

[10] 740 ILCS 14/5(d).

[11] 740 ILCS 14/10.

[12] *See* 740 ILCS 14/15.

[13] 740 ILCS 14/10.

[14] *Id.*

[15] *Rosenbach*, 2019 IL 123186, ¶¶ 36-37.

[16] *Tims v. Black Horse Carriers, Inc.*, 2021 IL App (1st) 200563, ¶ 25.

[17] *Tims*, 2021 IL App (1st) 200563, ¶ 30.

[18] *Id.* ¶ 31; 740 ILCS 14/15.

[19] *Id.* ¶¶ 31-32; 740 ILCS 14/15.

[20] *Id.* ¶ 31; 740 ILCS 14/15.

[21] 740 ILCS 14/20.

[22] *Rosenbach,* 2019 IL 123186, ¶ 38.

[23] 740 ILCS 14/20.

[24] *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004.

[25] *Cothron*, 2023 IL 128004, ¶ 45.

[26] *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶¶ 44-45, 50.

[27] *West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, 2021 IL 125978, ¶ 62.

[28] *Tims*, 2023 IL 127801, ¶ 42.

[29] *Walton v. Roosevelt Univ.*, 2022 IL App (1st) 210011, *appeal allowed*, No. 128338, 2022 WL 1738484 (Ill. May 25, 2022).

[30] *Remprex, LLC v. Certain Underwriters at Lloyd's, London, Syndicates 2623/623*, No. 1-21-1097, *argued*, (1st Dist. Jan. 12, 2023).

[31] Of course, "[i]n Illinois, an insurer's duty to defend is 'much broader' than its duty to indemnify." *Twin City Fire Ins. v. Vonachen Servs.*, 567 F. Supp. 3d 979, 990 (C.D. Ill. Oct. 19, 2021).

[32] *See*, *e.g., Krishna*, 2021 IL 125978, ¶ 7.

[33] *See id.* ¶ 36.

[34] *Krishna*, 2021 IL 125978.

[35] *Id.* ¶¶ 38-43.

[36] *Id.* ¶ 43.

[37] *Id.*

[38] *Id.*

[39] *Id.* ¶ 45.

[40] *Id.*

[41] *Id.*

[42] *Id.* ¶ 46.

[43] *Id.*

[44] *Id.* ¶ 51.

[45] *Citizens Ins. Co. of Am. v. Wynndalco Enterprises, LLC*, *et. al.*, No. 20 C 3873 (N.D. Ill. Mar. 30, 2022).

[46] *Krishna*, 2021 IL 125978, ¶ 59.

[47] Rosa M. Tumialán, Erin S. Johnson, and So Young (Anna) Lee, *BIPA Class Actions: The Next Generation of Data Privacy Liability Coverage*, 61 No. 5 DRI FOR DEF. 50 (May 2019).

[48] *Krishna*, 2021 IL 125978, ¶ 9 (emphasis added).

[49] *Id. Id.* ¶ 58 (emphasis in original).

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.* ¶ 57 (quoting BLACK'S LAW DICTIONARY 517 (6th ed. 1990)).

[55] *Id.* ¶ 58.

[56] *Id.*

[57] *Id.* ¶ 59.

[58] *See Am. Family Mut. Ins. Co. v. Caremel, Inc.*, No. 20 C 637, 2022 WL 79868, at *4 (N.D. Ill. Jan. 7, 2022) (finding exclusion inapplicable as it was "virtually identical" to that in *Krishna*); *Am. Fam. Mut. Ins. V. Carnagio Enters.*, No. 20 C 3665, 2022 WL 952533 (N.D. Ill. Mar. 30, 2022) ("BIPA is not like the TCPA and the CAN-SPAM ACT, because BIPA protects a different kind of privacy and uses a different method to do so.").

[59] Deborah W. Yue, *Duty to Defend a Biometric Information Privacy Act Violation*, 23 No. 4 TORTSOURCE 18 (Summer 2021).

[60] *See, e.g.*, *Thermoflex Waukegan, LLC*, 588 F. Supp. 3d at 853; ISO form CG 00 01 04 13, at pp. 5-6 (2012).

[61] *Citizens Ins. Co. of Am. v. Thermoflex Waukegan, LLC*, 588 F. Supp. 3d 845 (N.D. Ill. Mar. 1, 2022); *Citizens Ins. Co. of Am. v. Highland Baking Co.*, No. 20-CV-04997, 2022 WL 1210709 (N.D. Ill. Mar. 29, 2022); *Citizens Ins. Co. of Am. v. Wynndalco Enterprises, LLC*, 595 F. Supp. 3d 668 (N.D. Ill. 2022); *Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc.*, No. 21 C 788, at p. 18 (N.D. Ill. Jan 19, 2023).

[62] *Thermoflex Waukegan, LLC*, 588 F. Supp. 3d at 854.

[63] *Id.*

[64] *Wynndalco Enterprises,* 595 F. Supp. 3d at 673–74 (internal citations omitted).

[65] *Mass. Bay. Ins. Co. v. Impact Fulfillment Svcs., LLC*, No. 1:20CV926, 2021 WL 4392061, at *7 (M.D. N.C. Sept. 24, 2021) (identified statutes contained in the exclusion, much like BIPA, are broadly intended to protect privacy; exclusion operates to exclude coverage for BIPA claims).

[66] *Cont'l W. Ins. Co. v. Cheese Merchants of Am., LLC*, No. 21-CV-1571, 2022 WL 4483886 (N.D. Ill. Sept. 27, 2022).

[67] *Cheese Merchants*, 2022 WL 4483886, at *1.

[68] *Id.*

[69] *Id.* at *9.

[70] *Id.* at *10.

[71] *Id.* (emphasis in original).

[72] *Id.* (emphasis in original).

[73] *Id.*

[74] *Id.* at *11.

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.* (citing A. SCALIA & B. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 209 (2012)).

[80] *Id.* at *12.

[81] *Id.* at *14.

[82] *Id.* at *12.

[83] *Id.* at *13.

[84] *Id.*

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *State Auto Prop. and Cas. Ins. Co. v. Fruit Fusion, Inc.*, 2022 WL 4549824, at *6 (S.D. Ill. Sept. 29, 2022) (adopting analysis of *Cheese Merchants*).

[91] *Fruit Fusion*, 2022 WL 4549824, at *6.

[92] *See id.*; *Cheese Merchants*, 2022 WL 4483886, at *16.

[93] *Cheese Merchants*, 2022 WL 4483886, at *4; ISO form CG 04 37 05 14, at p. 1 (2013) (emphasis added).

[94] *See Carnagio*, 2022 WL 952533; *Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc.*, 595 F. Supp. 3d 677 (N.D. Ill. Mar. 30, 2022); *Cheese Merchants*, 2022 WL 4483886.

[95] *Cheese Merchants,* 2022 WL 4483886, at *5.

[96] *Id.* at *8.

[97] *Id.* at *7.

[98] *Id.* at *8.

[99] *Carnagio*, 2022 WL 952533, at *8; *Mitsui Sumitomo Ins. USA, Inc.*, 595 F. Supp. 3d at 682-83.

[100] *Carnagio*, 2022 WL 952533, at *9; *Mitsui Sumitomo Ins. USA, Inc.*, 595 F. Supp. 3d at 684.

[101] *Mitsui Sumitomo Ins. USA, Inc.*, 595 F. Supp. 3d at 684.

[102] *Id.*

[103] *Carnagio*, 2022 WL 952533; *Mitsui Sumitomo Ins. USA, Inc.*, 595 F. Supp. 3d 677 (N.D. Ill. March 30, 2022); *Cheese Merchants*, 2022 WL 4483886.

[104] *See Caremel*, 2022 WL 79868, at *3; *Citizens Ins. Co. of Am. v. Thermoflex Waukegan, LLC*, 588 F. Supp. 3d 845 (N.D. Ill. Mar. 1, 2022); *Highland Baking*, 2022 WL 1210709.

[105] *Caremel,* 2022 WL 79868, at *3; *Citizens Ins. Co. of Am. v. Thermoflex Waukegan, LLC*, 588 F. Supp. 3d 845, 855-56.

[106] *Caremel,* 2022 WL 79868, at *3.

[107] *Citizens Ins. Co. of Am. v. Thermoflex Waukegan, LLC*, 588 F. Supp. 3d at 855.

[108] *Id.* at 856.

[109] *Caremel*, 2022 WL 79868, at *3; *Citizens Ins. Co. of Am. v. Thermoflex Waukegan, LLC*, 588 F. Supp. 3d 845; *Highland Baking*, 2022 WL 1210709.

[110] *See, e.g., Caremel*, 2022 WL 79868, at *3 (emphasis added).

[111] *Id.* at *4.

[112] *Id.* at *3.

[113] *Id.*

[114] *Id.*

[115] *Id.* at *4.

[116] *Id.*

[117] *Id.*

[118] *State Auto Mut. Ins. Co. v. Tony's Finer Foods Enterprises, Inc.*, 589 F. Supp. 3d 919, 930 (N.D. Ill. 2022).

[119] *See Thermoflex Waukegan, LLC*, 588 F. Supp. 3d 845; *Tony's Finer Foods*, 589 F. Supp. 3d 919; *Highland Baking*, 2022 WL 1210709; *Carnagio*, 2022 WL 952533; *Cheese Merchants*, 2022 WL 4483886; *Fruit Fusion,* 2022 WL 4549824.

[120] *Cheese Merchants*, 2022 WL 4483886, *4.

[121] *Fruit Fusion*, 2022 WL 4549824, *5 (emphasis in original)

[122] *Tony's Finer Foods*, 598 F. Supp. 3d at 928.

[123] *Carnagio*, 2022 WL 952533, at *5 (applying cannon of *noscitur sociis*, fingerprinting does not fall within scope of ERP exclusion).

[124] *Tony's Finer Foods*, 589 F. Supp. 3d at 930.

[125] *Id.*

[126] *Twin City Fire Ins. v. Vonachen Servs.*, 567 F. Supp. 3d 979 (C.D. Ill. Oct. 19, 2021).

[127] *Id.* at 984.

[128] *Id.* at 984-85.

[129] *Id.* at 986.

[130] *Id.*

[131] *Id.* at 987.

[132] *Id.* at 996.

[133] *Id.*

[134] *Id.* at 987.

[135] *Id.* at 998.

[136] *Id.*

[137] *Id.* (emphasis added).

[138] *Id.* at 998, 1001.

[139] *Id.* at 998, 1000-01.

[140] *Id.* at 1002.

[141] *Id.*

[142] *Id.* (emphasis in original).

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.* at 1004 (emphasis in original).

[149] *Id.*

[150] *Id.* at 1005.

[151] *Id.*

[152] *Id.* at 1005-06.

[153] *Id.* at 1005-06.

[154] *Id.* at 1004.

[155] *Id.* at 1011.

[156] *Church Mut. Ins. Co. v. Prairie Village Supportive Living, LLC*, 2022 WL 3290686 (N.D. Ill. Aug. 11, 2022).

[157] *Id.* at *1.

[158] *Id.*

[159] *Id.* (emphasis in original).

[160] *Id.* at *1-2 (emphasis added).

[161] *Id.* at *3.

[162] *Id.* at *4.

[163] *Id.*

[164] *Id.*

[165] *Id.*

[166] *Id.* (quoting *Tony's Finer Foods,* 2022 WL 683688, at *7).

[167] *Id.* at *1, 4.

[168] Rosa M. Tumialán, *et. al*, *supra* note 47.

[169] *Id.*

[170] *Id.*

[171] *Id.*

[172] *Id.*

[173] *Id.*

[174] *Remprex, LLC v. Certain Underwriters at Lloyd's, London, Syndicates 2623/623*, No. 2020-CH-05507 (Cir. Ct. Cook County, Ill. Feb. 28, 2022).

[175] *Remprex, LLC v. Certain Underwriters at Lloyd's, London, Syndicates 2623/623*, No. 1-21-1097, *argued*, (1st Dist. Jan. 12, 2023).

[176] *Tims*, 2023 IL 127801; 735 ILCS 5/13-201; 735 ILCS 5/13-205.

[177] 735 ILCS 5/13-201.

[178] *Tims*, 2023 IL 127801, ¶ 24.

[179] *Id.* ¶ 18 (citing *Sundance Homes, Inc. v. County of Du Page*, 195 Ill. 2d 257, 266 (Ill. 2001)).

[180] *Id.* ¶ 27; 740 ILCS 14/5(g).

[181] *Id*.

[182] *Id.* ¶ 29; *see also Rosenbach*, 2019 IL 123186, ¶ 20.

[183] 735 ILCS 5/13-201; *Tims*, 2023 IL 127801, ¶ 30.

[184] *Tims*, 2023 IL 127801, ¶ 30.

[185] *Id.* ¶¶ 31-33.

[186] *Id.* ¶ 32; *Krishna*, 2021 IL 125978, ¶ 43. In *Krishna*, the supreme court found that the tanning salon's collection of the plaintiff's fingerprints and disclosure to a third-party vendor to be used to gain access to tanning salons "was potentially a publication that violated Sekura's right to privacy" in violation of BIPA.

[187] *Tims*, 2023 IL 127801, ¶ 32; *Sundance Homes*, 195 Ill. 2d at 265-66.

[188] *Tims*, 2023 IL 127801, ¶ 40; 740 ILCS 14/5(g).

[189] *Tims*, 2023 IL 127801, ¶ 42.

[190] *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004, ¶ 1.

[191] *Cothron*, 2023 IL 128004, ¶ 12.

[192] *Id.* ¶ 3.

[193] *Id.* ¶ 4.

[194] *Id.*

[195] *Id.*

[196] *Id.* ¶ 5. Cothron's argument focuses on the plain text of subsections 15(b) and 15(d) of BIPA. The text, according to Cothron, leads to only one conclusion—each time White Castle collected and disseminated Cothron's biometric information without prior informed consent, White Castle violated BIPA, even though she voluntarily agreed that White Castle could use her biometric information to allow access to the computer system.

[197] *Id.* ¶ 6.

[198] 740 ILCS 14/15(b).

[199] 740 ILCS 14/15(d)(1).

[200] *Cothron*, 2023 IL 128004, ¶ 16.

[201] *Id.* ¶ 17.

[202] *Id.* ¶ 18.

[203] *Id.* ¶ 19 (noting the plaintiff's observation that the appellate court reached the same conclusion in *Watson v. Legacy Healthcare Fin. Serv., LLC*, 2021 IL App (1st) 210279, ¶ 53).

[204] *Id.*

[205] *Id.* ¶ 20.

[206] *Id.* ¶ 24 (quoting *Cothron v. White Castle Sys., Inc.*, 477 F. Supp. 3d 723, 732 (N.D. Ill. 2020)). The supreme court further noted that "the appellate court reached the same conclusion, determining that 'the plain language of [section 15(b)] establishes that it applies to each and every capture and use of plaintiff's fingerprint or hand scan. Almost every substantive section of the Act supports this finding.'" (quoting *Watson*, 2021 IL App (1st) 210279, ¶ 46).

[207] *Id.* ¶ 25 (citing 740 ILCS 14/15(b)). Noting that the appellate court correctly determined the "unless it first" phrase "modifies the entity's obligations, not the triggering actions." (quoting *Watson*, 2021 IL App (1st) 210279, ¶ 53).

[208] *Id.* ¶ 27.

[209] *Id.* ¶ 27 (citing 740 ILCS 14/15(d)).

[210] *Id.* ¶ 28.

[211] *Id.* (citing WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 645 (1993)).

[212] *Id.*

[213] *Id.* ¶ 29.

[214] *Id.* ¶ 30.

[215] *Id.* ¶ 32.

[216] *Id.*

[217] *Id.* ¶ 33 (citing *Rosenbach*, 2019 IL 123186, ¶¶ 33-34; *West Bend*, 2021 IL 125978, ¶ 46 (explaining that the Act protects a "secrecy interest"); and *McDonald*, 2022 IL 126511, ¶ 24 (reiterating that the Act protects an individual's "'right to privacy in and control over their biometric identifiers and biometric information'").

[218] *Id.* ¶ 38.

[219] *Id.* ¶ 39.

[220] *Id.* ¶ 40.

[221] *Id.*

[222] *Id.* (citing *Cothron*, 477 F. Supp. 3d at 734).

[223] *Id.* ¶ 42 (citing *McDonald*, 2022 IL 126511, ¶¶ 48-49).

[224] *Id.* ¶ 43.

[225] *Id.* ¶ 45.

[226] *Id.* ¶ 48.

[227] *See Cothron v. White Castle Sys. Inc.*, 20 F. 4th 1156 (7th Cir. 2021).

[228] *Cothron*, 2023 IL 128004, ¶ 54.

[229] *Id.* ¶ 55.

[230] *Id.*

[231] *Id.* ¶ 56.

[232] *Id.* ¶¶ 57-58.

[233] *Id.* ¶¶ 65-66-58.

[234] *Id.* ¶ 60.

[235] *Id.* ¶ 61.

About the Authors

Matthew B. Champlin is a partner at *HeplerBroom LLC*, in Edwardsville. He focuses his practice on personal injury defense. Mr. Champlin received his J.D. from the University of Missouri-Columbia School of Law, where he was inducted in the *Order of the Coif*. He is admitted to practice in Illinois, Missouri, the Southern District of Illinois, and the Eighth Circuit Court of Appeals. Prior to joining *HeplerBroom LLC*, Mr. Champlin clerked for the Honorable Duane Benton on the Missouri Supreme Court and the Eighth Circuit Court of Appeals.

Georgia L. Joyce is an attorney with *Tressler LLP* in Chicago where she concentrates her practice in insurance coverage litigation. Her work includes the preparation of coverage opinions and the handling of all phases of litigation of coverage suits in state and federal courts. She represents insurance carriers in a broad range of coverage matters involving

commercial general liability policies and their application to personal injury and property damage lawsuits. Ms. Joyce is a graduate of Chicago-Kent College of Law (J.D.), De Paul University (M.B.A. Finance), and University of Illinois at Urbana-Champaign (B.S. Finance).

About the IDC

The Illinois Defense Counsel (IDC) is the premier association of attorneys in Illinois who devote a substantial portion their practice to the representation of business, corporate, insurance, professional and other individual defendants in civil litigation. For more information on the IDC, visit us on the web at www.IDC.law or contact us at PO Box 588, Rochester, IL 62563-0588, 217-498-2649, 800-232-0169, admin@IDC.law.