

ILR BRIEFLY



A BAD MATCH: ILLINOIS AND THE BIOMETRIC INFORMATION PRIVACY ACT

“*The Illinois Biometric Information Privacy Act is a prime example of a misdirected law that has led to more litigation abuse than consumer protection.*”

A Bad Match: Illinois and the Biometric Information Privacy Act†

Policymakers across states are grappling with whether and how to regulate the collection, use, and sharing of biometric identifiers—such as fingerprints or facial scans. A few states have adopted stand-alone biometric privacy laws that create notice, consent, and other requirements for biometric data in certain circumstances, while others have adopted omnibus privacy laws that sweep in biometric data as a subset of protected data.¹

Of the three states that have stand-alone biometric privacy laws—Illinois, Texas, and Washington—the Illinois law is the only one that authorizes a private right of action (PRA).

One huge concern with biometric privacy laws in general is that they can create unintended consequences. Such laws can incentivize lawsuits over routine practices with no consumer harm, resulting in big awards for plaintiffs' attorneys, litigation burdens on well-meaning companies, and no net benefit for consumers. The Illinois Biometric Information Privacy Act (BIPA) is a prime example of a misdirected law that has led to more litigation abuse than consumer protection.²

Understanding and avoiding the pitfalls of BIPA will help

policymakers considering biometric privacy laws to avoid unfairly punishing businesses, promoting frivolous lawsuits, and stifling the immense practical benefits of utilizing biometric data for purposes such as authentication and security.³

BIPA: A LUCRATIVE TARGET

Enacted in 2008, BIPA is a biometric privacy law that regulates the collection, retention, disclosure, and destruction of biometric identifiers (e.g., retina or iris scans, fingerprint, voiceprint, or scans of hand or face geometry) and biometric information.⁴ The requirements for entities that possess this data are complex and technical,⁵ including providing written notice (of the "specific purpose and length of term for which a biometric identifier or

biometrics information is being collected, stored, and used")⁶ and obtaining written release.

Aside from the substantive requirements around a company's biometric data practices, what makes BIPA stand out from other state biometric privacy laws is its PRA and overall lack of commonsense enforcement procedures to protect companies attempting good faith compliance with the law, which have opened the floodgates to abusive litigation. Notably, as the mapping in the Appendix shows, BIPA fails to incorporate meaningful procedural protections needed⁷ to prevent unintended and harmful consequences of state privacy legislation, making it a poster child for litigation abuse.

BIPA'S PRA AND LOW HURDLE TO BRING SUIT ALLOW RAMPANT ABUSE

The most important way to protect consumers' privacy, avoid inconsistent and unfair application of laws, and stem the growing tide of litigation abuse is to explicitly preclude a PRA in privacy legislation and to vest enforcement authority solely in the hands of experts with discretion (i.e., state attorneys general). Unfortunately, BIPA does

neither of these things. Instead of precluding a PRA, it authorizes one. Instead of vesting enforcement authority with the Illinois Attorney General, it leaves litigation completely up to private plaintiffs and lawyers.

BIPA's PRA is exacerbated by the lack of a need to show any actual harm to consumers. In January 2019, the Illinois Supreme Court found in *Rosenbach v. Six Flags* that simply violating the statute,

without showing any actual harm or adverse effect, was enough to state a claim under the law.⁸ Together, the PRA and the incredibly low hurdle to bringing a lawsuit—allowing for litigation based on mere procedural violations—has inevitably fueled a torrent of lawsuits, with plaintiffs' attorneys seemingly motivated by the promise of large cash settlements filing boilerplate complaints.⁹

“ Together, the PRA and the incredibly low hurdle to bringing a lawsuit—allowing for litigation based on mere procedural violations—has inevitably fueled a torrent of lawsuits, with plaintiffs' attorneys seemingly motivated by the promise of large cash settlements filing boilerplate complaints. ”



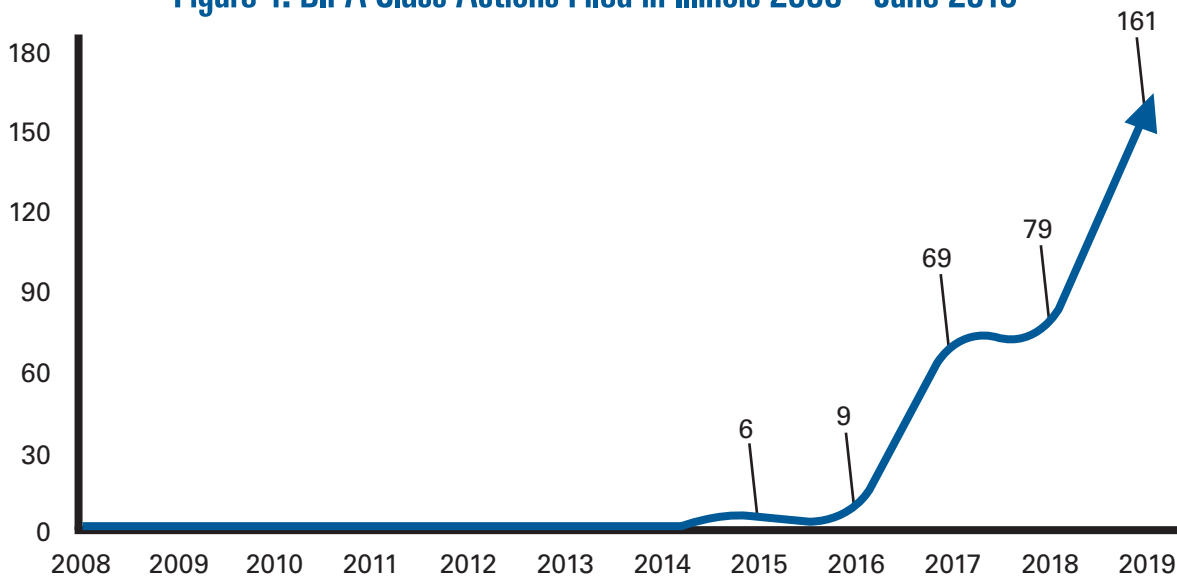
Exponential Growth in Litigation

By the numbers, there has been exponential growth in BIPA litigation. Since BIPA was enacted in 2008 through 2016,

there were only 15 BIPA class actions filed in Illinois,¹⁰ with the first class-wide settlement approved in 2016 for \$1.5

million.¹¹ Litigation began to grow thereafter, as the below graph shows.¹²

Figure 1: BIPA Class Actions Filed in Illinois 2008 - June 2019*



Source: *Biometric Privacy Class Actions By The Numbers: Analyzing Illinois' Hottest Class Action Trend*, available at <https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/>.

*Filing numbers cited in Figures 2 and 3 may not sum to yearly filing totals in this chart due to differing methodologies.

Then in January 2019, the Supreme Court of Illinois found in *Rosenbach* that a plaintiff could seek liquidated damages and injunctive relief under the state privacy statute without proof of actual damages.

This decision spurred a massive wave of class actions: from that decision in January 2019 to June of the same year, there was a total of 151 class actions filed in Illinois, which was “approximately a rate of

an additional case filed every day.”¹³ 2019 closed out with close to 300 BIPA lawsuits filed in Illinois—almost four times the number of cases filed the year before.¹⁴

“ 2019 closed out with close to 300 BIPA lawsuits filed in Illinois—almost four times the number of cases filed the year before. ”

Figure 2: BIPA Cases Filed in Illinois State Court 2015 - Q1 2021

2015	2016	2017	2018	2019	2020	Q1 2021	Total
4	3	58	74	286	95	13	533

Source: *Biometric Proposals May Provide Relief to Employers and Courts*, available at <https://www.hklaw.com/en/insights/publications/2021/04/biometric-proposals-may-provide-relief-to-employers-and-courts>.

Suits are rampant—and growing—at the federal level as well: one study shows that plaintiffs have filed 370 BIPA-related cases in federal district courts since 2015, including

outside of Illinois.¹⁵ While 2020 saw 153 BIPA-related federal cases, the first quarter of 2021 alone saw over a third of that amount: 53 cases.¹⁶

All told, according to a search of court filings, plaintiffs’ lawyers had filed over 900 cases alleging BIPA violations through September 2021.

Figure 3: BIPA Cases Filed in Federal Court 2015 - Q1 2021

	2015	2016	2017	2018	2019	2020	Q1 2021	Total
USDC, N.D. Illinois	7	7	29	16	67	114	42	282
USDC, N.D. California	4	3	3	11	3	17		41
USDC, S.D. Illinois			1		8	13	6	28
USDC, C.D. Illinois			1		4	9	5	19
Grand Total	11	10	34	27	82	153	53	370

Source: *Biometric Proposals May Provide Relief to Employers and Courts*, available at <https://www.hklaw.com/en/insights/publications/2021/04/biometric-proposals-may-provide-relief-to-employers-and-courts>.

“ All told, according to a search of court filings, plaintiffs’ lawyers had filed over 900 cases alleging BIPA violations through September 2021. ”



Plaintiffs' Lawyers, Not Consumers, Reap the Benefits

Another feature of BIPA that makes it a particular target for plaintiffs' attorneys is that it establishes uncapped liquidated damages and allows for unlimited attorneys' fees. Rather than imposing reasonable total limits on damages, the law allows plaintiffs to seek liquidated damages of \$1,000 or \$5,000 per violation, depending on whether the violation is negligent or intentional/reckless.¹⁷

In practice, these liquidated damages provisions increase liability exposure beyond actual damages—given that actual damages are typically negligible and the statute states that recovery may occur on a per violation basis.¹⁸ Further, BIPA authorizes attorneys' fees without any caps—allowing for “reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses.”¹⁹ This only serves to increase litigiousness.

These features—liquidated damages and attorneys' fees, both uncapped—have resulted in astronomical dollar figures from BIPA litigation, with

“*These features—liquidated damages and attorneys' fees, both uncapped—have resulted in astronomical dollar figures from BIPA litigation, with attorneys getting huge sums and class members getting relatively little compared to attorneys.*”

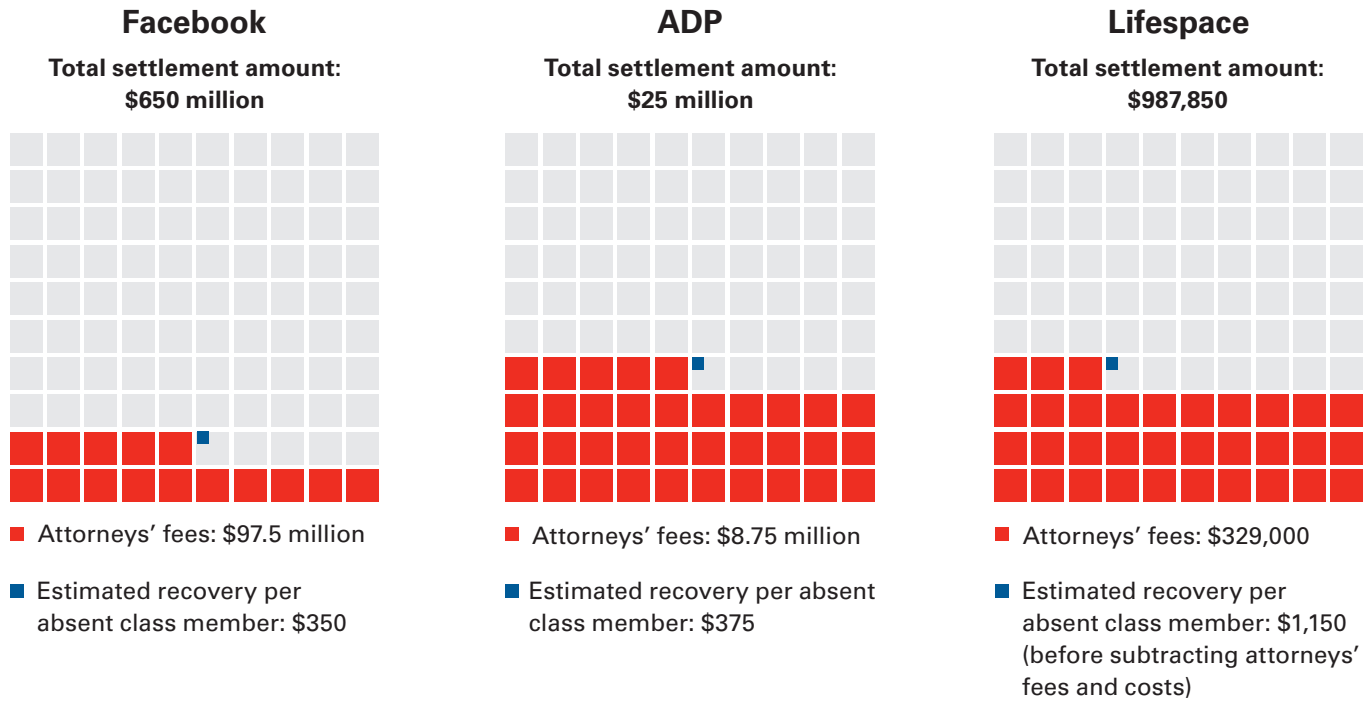
attorneys getting huge sums and class members getting relatively little compared to attorneys. For example:

- In the landmark *Facebook* settlement involving the company's facial recognition technology, a federal judge in February 2021 approved a \$650 million settlement fund, \$97.5 million of which goes to attorneys' fees, with class members receiving around \$350 each.²⁰

- In April 2021, an Illinois judge approved a \$25 million BIPA class action settlement between ADP and its employees. While the individuals who filed claims under the settlement will receive about \$375 each according to the terms of the settlement (with the class representatives receiving \$7,500 each), the class counsel was awarded \$8.75 million, or more than one-third of the total settlement fund.²¹

- In May 2021, an Illinois judge approved a nearly \$1 million settlement in the *Lifespace* BIPA case between a senior living chain and its employees. While the employee class members received \$1,150, before subtracting attorneys' fees and costs, the attorneys were granted almost \$329,000.²²

Figure 4: Attorneys' Fees as a Proportion of BIPA Settlements²³



BIPA TARGETS BUSINESSES BOTH BIG AND SMALL

Contrary to typical media reports, it is not just tech giants and large employers that are bearing the brunt of BIPA litigation abuse. According to the Illinois Chamber of Commerce, it is mostly small companies in the state facing lawsuits.²⁴

In *Kirby v. Gurtler Chemicals, Inc.*,²⁵ a class action suit

was filed against a family-run company based in South Holland, Illinois that has a total of 65 employees. The suit discusses unrelated data breaches—including the 2015 Office of Personnel Management breach—but does not allege actual harm.²⁶ Instead, it alleges only technical violations of the law, including an alleged failure to provide a publicly available retention schedule, among other things,

where the small business used a biometric time clock to clock employees in and out.²⁷

In *Truss v. Four Seasons Heating & Air Conditioning*,²⁸ the same attorney and law firm brought a nearly identical complaint just six days later against another small business in Illinois—this time a heating and air conditioning company.²⁹

“ According to the Illinois Chamber of Commerce, it is mostly small companies in the state facing lawsuits. ”

BIPA PUNISHES TECHNICAL VIOLATIONS INSTEAD OF ADDRESSING ACTUAL INJURY

Following the decision in *Rosenbach*, the lack of any requirement to show actual injury under BIPA has resulted in businesses being targeted for high-dollar lawsuits under the statute as a result of technical missteps.

In *Rapai v. Hyatt Corp*, the defendant hotel collected fingerprints of employees who used a biometric time and attendance system, allowing those employees to accurately punch in and out.³⁰ The automated time entry solution helped employees accurately get paid for time worked, but plaintiffs held that it did not technically comply with the law. Amidst the uncertainty surrounding the scope of BIPA

liability, Hyatt settled the class action claims for \$1.5 million.³¹

In another suit, a proposed class is seeking damages from an audio recognition company whose software helps consumers issue voice commands to trigger hands-free features, such as changing stations, volume control, or interactive requests—a clear benefit to help prevent distractions and increase convenience.³² However, the suit alleges that the company did not obtain written permission or make certain technical disclosures.³³

There is even a trend targeting entities that are helping students and schools adapt to remote learning during the global COVID-19 pandemic. For example, Respondus Inc.—a company that offers

remote proctoring software with biometric features—was hit with three lawsuits from students at three different schools between November 2020 and April 2021.³⁴

Some privacy laws attempt to protect against punishing technical violations that do not result in actual harm by allowing for reasonable notice and cure periods or establishing safe harbor provisions for companies. However, BIPA does neither of these things—leading to unfair and very costly consequences. While there have been efforts to reform BIPA—including HB 559, a bill proposed in the 2021 Illinois legislative session that would have, among other things, established a 30-day notice and cure period before initiating actions—none have yet succeeded.³⁵

“Some privacy laws attempt to protect against punishing technical violations that do not result in actual harm by allowing for reasonable notice and cure periods or establishing safe harbor provisions for companies. However, BIPA does neither of these things—leading to unfair and very costly consequences.”

Conclusion

LOOKING AHEAD, BIPA SHOULD NOT BE THE BLUEPRINT FOR BIOMETRICS REGULATION

The BIPA legal landscape continues to evolve, which may provide clarity on some important legal questions and lead to different litigation trends. For example, as of this writing, the Seventh Circuit is set to answer whether BIPA claims accrue with each alleged violation or only once.³⁶ And in light of recent U.S. Supreme Court precedent holding that only plaintiffs concretely

harmed by a statutory violation have Article III standing,³⁷ defendants may have a path to challenge BIPA suits filed in federal courts on procedural grounds.

But amid the evolving landscape, one thing is clear: BIPA's PRA—coupled with the law's many other failings, including unfettered liquidated damages, lack of a need to show consumer harm, and lack of notice and cure periods—has had disastrous effects. The lawsuits themselves

have provided little benefit to consumers and failed to remedy concrete harms, while the law has punished businesses operating in good faith and inevitably deterred them from adopting biometric-based technology that will benefit businesses and consumers alike.

As other states consider legislative approaches to biometric privacy, they should view BIPA not as a blueprint, but as a lesson in what not to do.

“As other states consider legislative approaches to biometric privacy, they should view BIPA not as a blueprint, but as a lesson in what not to do.”

Appendix: BIPA's Lack of Commonsense Procedural Protections

Recommended Protection	Importance of Protection	Corresponding Deficiency in BIPA
<p>Preclude Private Rights of Action (PRAs)</p>	<p>Privacy bills should preclude private litigants from bringing lawsuits for violations. Enforcement by experts with discretion—not plaintiffs’ lawyers—will best protect consumers.</p>	<p>Rather than precluding a PRA, BIPA is the only state biometric privacy law that authorizes one.³⁸ By contrast, Washington’s biometric privacy law “may be enforced solely by the attorney general” and under Texas’ biometric privacy law, only “[t]he attorney general may bring an action to recover the civil penalty.”³⁹</p>
<p>Vest Exclusive Enforcement Authority with the Attorney General</p>	<p>Exclusive enforcement authority should be vested with the state’s attorney general, who is best positioned to enforce complex and technical laws. Dividing enforcement authority amongst other actors—like private plaintiffs and their attorneys—risks inconsistent and unfair application of the laws.</p>	<p>BIPA only authorizes private enforcement—it does not look to the Illinois Attorney General for consistent and fair enforcement.</p>
<p>Cap Damages and Civil Penalties</p>	<p>State privacy legislation should impose reasonable caps on damages and civil penalties for violations. Enormous damages and punitive civil penalties are not needed to ensure that businesses comply with privacy laws.</p>	<p>Rather than providing reasonable caps, BIPA’s liquidated damages—\$1,000 or \$5,000 (depending on whether the violation is negligent or intentional/reckless)⁴⁰—can lead to company-ending results. In practice, the liquidated damages provisions increase liability exposure beyond actual damages—given that actual damages are typically negligible and the statute states that recovery may occur on a per violation basis.⁴¹</p>
<p>Limit Attorneys’ Fees</p>	<p>While states should not authorize private enforcement of privacy laws, in the event they do, states should at a minimum limit attorneys’ fees. Without such limits, the potential for astronomical attorneys’ fees encourages litigiousness.</p>	<p>BIPA allows for “reasonable attorneys’ fees and costs, including expert witness fees and other litigation expenses.”⁴² These fees and costs, too, are uncapped by the statute.</p>
<p>Establish Notice and Cure Periods</p>	<p>Even companies with the best intentions may err in applying complex and technical requirements in real-world scenarios. Notice and cure periods allow companies to course correct, which saves enforcement resources and promotes compliance.</p>	<p>BIPA provides no such provision.</p>
<p>Offer Safe Harbors</p>	<p>Privacy bills should include reasonable safe harbors for compliance, which will encourage best practices, protect well-meaning companies from “gotcha”-style liability, and reserve enforcement resources for true bad actors.</p>	<p>BIPA does not establish any safe harbors.</p>

Endnotes

- † This edition of *ILR Briefly* was prepared by Megan L. Brown, Duane C. Pozza, Kathleen E. Scott, and Tawanna D. Lee of Wiley Rein LLP.
- 1 Additionally, several states have included biometric data as an element that triggers reasonable security requirements and/or notifications in the case of a breach.
 - 2 740 Ill. Comp. Stat. § 14/1 et seq.
 - 3 For example, the National Institute of Standards and Technology (NIST) explains that “easily and accurately ascertaining the identity of individuals is what biometrics systems are all about,” noting that biometrics are used to manage identities in a range of settings, from “first responders at the scene of a natural disaster” to “soldiers in theater.” See *Key to Security, Biometric Standards*, NIST, https://cdn.napisek.kaltura.com/index.php/extwidget/preview/partner_id/684682/uiconf_id/31013851/entry_id/1_genwk6mj/embed/dynamic; Biometrics, NIST, <https://www.nist.gov/programs-projects/biometrics>.
 - 4 See generally 740 Ill. Comp. Stat. § 14/1 et seq.
 - 5 See *Ill-Suited: Private Rights of Action and Privacy Claims* at 10, U.S. Chamber Institute for Legal Reform (July 2019), <https://instituteforlegalreform.com/research/ill-suited-private-rights-of-action-and-privacy-claims/> (“*Ill-Suited*”) (generally explaining that BIPA “(1) regulates the retention and destruction of biometric information; (2) prohibits the collection, retention, or disclosure of biometric information without providing certain information to data subjects in writing and receiving written consent; (3) prohibits selling, leasing, trading, or otherwise profiting from biometric information; and (4) restricts the disclosure of biometric information.”).
 - 6 See 740 Ill. Comp. Stat. § 14/15(b)(2).
 - 7 *Ill-Suited*, generally.
 - 8 *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186 (Jan. 25, 2019).
 - 9 *Ill-Suited* at 10–11.
 - 10 *Biometric Privacy Class Actions by the Numbers: Analyzing Illinois’ Hottest Class Action Trend*, Seyfarth Shaw LLP (June 28, 2019), <https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/> (“*Biometric Privacy Class Actions by the Numbers*”).
 - 11 *Ill-Suited* at 10.
 - 12 See *Biometric Privacy Class Actions by the Numbers*.
 - 13 *Id.*
 - 14 Veronica L. Canton, *Biometric Proposals May Provide Relief to Employers and Courts*, Holland and Knight Cybersecurity Privacy Blog (Apr. 20, 2021), <https://www.hklaw.com/en/insights/publications/2021/04/biometric-proposals-may-provide-relief-to-employers-and-courts/> (“*Biometric Proposals May Provide Relief to Employers and Courts*”).
 - 15 *Biometric Proposals May Provide Relief to Employers and Courts*, <https://www.hklaw.com/en/insights/publications/2021/04/biometric-proposals-may-provide-relief-to-employers-and-courts>.
 - 16 *Id.*
 - 17 See 740 Ill. Comp. Stat. § 14/20(1)-14/20(2) (authorizing “liquidated damages of \$1,000 or actual damages, whichever is greater” or “liquidated damages of \$5,000 or actual damages, whichever is greater”).
 - 18 See *id.* at § 14/20 (“A prevailing party may recover for each violation ...”).
 - 19 *Id.* at § 14/20(3).
 - 20 Lauren Berg, *\$650M Facebook Privacy Deal OK’d, \$110M Atty Fees Trimmed*, Law 360 (Feb. 26, 2021), <https://www.law360.com/articles/1359569/-650m-facebook-privacy-deal-ok-d-110m-attys-fees-trimmed>.
 - 21 See Peter S. Lubin and Patrick Austermeuhle, *Judge Grants Final Approval to \$25M Settlement in BIPA Class Action against ADP*, Chicago Business Litigation Lawyer Blog (Apr. 15, 2021), <https://www.chicagobusinesslitigationlawyerblog.com/judge-grants-final-approval-to-25m-settlement-in-bipa-class-action-against-adp/>.
 - 22 Lauraann Wood, *Attys Score \$328K Payday After \$1M BIPA Deal Gets Final OK*, Law360 (May 13, 2021), <https://www.law360.com/articles/1384387/attys-score-328k-payday-after-1m-bipa-deal-gets-final-ok>.
 - 23 The blue portions of squares in the three charts below are not accurate proportional representations of estimated recoveries per absent class member. Actual estimated recoveries per absent class member are too small to represent at scale in these charts. The blue portions seen here are thus over-representations for illustrative purposes.



- 24 Grace Barbic, *Lawmakers revisit data collection privacy laws*, The Courier (Mar. 10, 2021), <https://www.lincolncourier.com/story/news/politics/2021/03/10/biometric-information-privacy-act-protect-small-businesses/6944810002/>.
- 25 See Gurtler Industries, Inc., About Us (visited Aug. 23, 2021), <https://www.gurtler.com/laundry-chemical-manufacturer/> (highlighting the three generations of the Gurtler family behind the business); Gurtler Industries, Dun & Bradstreet Company Profile (visited Aug. 23, 2021), https://www.dnb.com/business-directory/company-profiles.gurtler_chemicals_inc.38460515a1de358a356d9b3861c1efc2.html (listing 65 total employees across all of the company's locations).
- 26 *Kirby v. Gurtler Chemicals, Inc.*, Class Action Complaint, Case No. 2019-CH-09395 (Ill. Cir. Ct., Cook Cty. Aug. 14, 2019).
- 27 *Id.*
- 28 *Truss v. Four Seasons Heating & Air Conditioning, Inc.*, Class Action Complaint, Case No. 2019-CH-09633 (Ill. Cir. Ct., Cook Cty. Aug. 20, 2019).
- 29 See Four Seasons Heating and Air Conditioning, About Us (visited Aug. 23, 2021), <https://www.fourseasonsheatingcooling.com/about-us/>.
- 30 Complaint, *Rapai v. Hyatt, Corp*, 2017 WL 5015841 (Ill. Cir. Ct., Cook Cty. Oct. 30, 2017) at ¶ 2.
- 31 Celeste Bott, *Hyatt To Pay \$1.5 M To Resolve Biometric Privacy Suit*, Law 360 (Jul. 14, 2021), <https://www.law360.com/articles/1403093/hyatt-to-pay-1-5m-to-resolve-biometric-privacy-suit>.
- 32 See *Carpenter v. Soundhound, Inc.* Class Action Complaint, No. 2021CH03346 (Ill Cir. Ct., Cook Cty. July 9, 2021); Celeste Bott, *Audio Co. Sued Over Software Used in Pandora's 'Voice Mode,'* Law360 (July 14, 2021), <https://www.law360.com/articles/1403034/audio-co-sued-over-software-used-in-pandora-s-voice-mode>.
- 33 See *Carpenter v. Soundhound, Inc.* Complaint ¶¶ 34-35.
- 34 Lauraann Wood, *More Students Hit Testing Software Co. Over Facial Scans*, Law 360 (Apr. 5, 2021), <https://www.law360.com/classaction/articles/1371876/more-students-hit-testing-software-co-over-facial-scans>.
- 35 See HB 559, Ill. General Assembly, <https://www.ilga.gov/legislation/BillStatus.asp?DocNum=559&GAID=16&DocTypeID=HB&SessionID=110&GA=102>.
- 36 See *Cothron v. White Castle System Inc.*, Brief and Required Short Appendix of Defendant-Appellant White Castle System, Inc., No. 20-3202 (7th Cir. Aug. 13, 2020) (“Whether, when conduct that allegedly violates BIPA is repeated, that conduct gives rise to a single claim under Sections 15(b) and 15(d) of BIPA, or multiple claims.”)
- 37 See *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190 (2021); see also *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016).
- 38 740 Ill. Comp. Stat. § 14/20 (“Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party.”).
- 39 Wash. Rev. Code § 19.375.030(2); Tex. Bus. & Com. Code § 503.001(d).
- 40 See 740 Ill. Comp. Stat. § 14/20(1) (authorizing “liquidated damages of \$1,000 or actual damages, whichever is greater” or “liquidated damages of \$5,000 or actual damages, whichever is greater”).
- 41 See *id.* at § 14/20. (“A prevailing party may recover for each violation ...”).
- 42 *Id.* at § 14/20(3).



U.S. CHAMBER
Institute for Legal Reform

202.463.5724 main
202.463.5302 fax

1615 H Street, NW
Washington, DC 20062

instituteforlegalreform.com