No. 129081

In The
Supreme Court Of Illinois

LUCILLE MOSBY, Individually, and on Behalf of All Others Similarly Situated, Plaintiff-Appellee, v. THE INGALLS MEMORIAL HOSPITAL, UCM COMMUNITY HEALTH & HOSPITAL DIVISION, INC., and BECTON, DICKINSON AND COMPANY, Defendants-Appellants.	)	On Appeal from the Circuit Court of Cook County, Illinois, County Department, Chancery Division Case No. 2018-CH-05031 The Honorable Judge Pamela McLean Meyerson, Presiding

YANA MAZYA, Individually, and on Behalf of All Others Similarly Situated, Plaintiff-Appellee, v. NORTHWESTERN LAKE FOREST HOSPITAL and NORTHWESTERN MEMORIAL HEALTHCARE, Defendants-Appellants.	)	On Appeal from the Circuit Court of Cook County, Illinois, County Department, Chancery Division Case No. 2018 CH 07161 The Honorable Judge Alison C. Conlon, Presiding

BRIEF OF THE ILLINOIS CHAMBER OF COMMERCE AND THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AS *AMICI CURIAE* IN SUPPORT OF DEFENDANTS-APPELLANTS

Daniel D. Birk
John K. Adams
EIMER STAHL LLP
224 South Michigan Avenue,
Suite 1100
Chicago, Illinois 60604
(312) 660-7600
dbirk@eimerstahl.com
jkadams@eimerstahl.com

Counsel for Amici Curiae

TABLE OF CONTENTS AND POINTS OF AUTHORITIES

INTEREST OF *AMICI CURIAE*

The Illinois Chamber of Commerce is a nonprofit organization composed of businesses and organizations of all types across Illinois. The Illinois Chamber is the unifying voice of the Illinois business community and represents businesses in all areas of Illinois' economy, including health care. Members consist of many mid-sized businesses as well as large international companies headquartered in this state. The Illinois Chamber works collaboratively with trade organizations on specific policy issues. It is dedicated to strengthening Illinois' business climate and economy for job creators and health care providers. Accordingly, the Illinois Chamber provides businesses with a voice as it works with state lawmakers to make business-related policy decisions. The Illinois Chamber also operates its Amicus Briefs Program to bring attention to specific cases and provide additional information for courts to consider.

The Chamber of Commerce of the United States of America ("the Chamber") is the world's largest business federation. It represents approximately 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and

the courts. To that end, the Chamber regularly files amicus curiae briefs in cases, like this one, that raise issues of concern to the nation's business community.

Amici have substantial experience with the Illinois Biometric Privacy Act, 740 ILCS 14 *et seq*. ("Privacy Act"), and The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 *et seq*. ("HIPAA"). *See, e.g.*, *Cothron v. White Castle System, Inc.*, --- N.E.3d ---, 2023 IL 128004, 2023 WL 2052410, ¶ 10, and *Walton v. Roosevelt University*, --- N.E.3d ---, 2023 IL 128338, 2023 WL 2603868, ¶ 13. Privacy litigation has recently exploded. *See* U.S. Chamber of Commerce, Institute for Legal Reform, *A Bad Match: Illinois and the Biometric Information Privacy Act* 5 (Oct. 2021) ("Institute for Legal Reform"), *available at* https://perma.cc/4AP4-5U49. *Amici* therefore submit this brief to explain why it is crucial to interpret the health care exclusion here in a manner consistent with its plain language, and the broader implications of this case for the Illinois health care system.

SUMMARY OF ARGUMENT

Three justices of this Court recently warned about the threat of "annihilative liability" posed by Privacy Act lawsuits for businesses that use biometric identifiers in their daily operations. *Cothron v. White Castle*

System, Inc., 2023 IL 128004, ¶ 48 (Overstreet, J., dissenting), *petition for rehearing pending*. Indeed, the *Cothron* majority acknowledged that the defendant in that case could be subject to $17 billion in damages for mere technical violations of the Act. *Id.* ¶ 40. The Appellate Court's decision in this case limiting the Privacy Act's "health care exclusion" to patient information now extends the prospect of "annihilative liability" to Illinois health care providers that routinely use biometric identifiers to safeguard sensitive information and medications, in compliance with HIPAA and other federal laws. Affirming the Appellate Court's decision not only will have harsh consequences for Illinois businesses and consumers, it would be contrary to the statutory text. Giving effect to the Act's plain language requires this Court to reverse.

Amici agree with Defendants-Appellants and Presiding Justice Mikva that straightforward rules of statutory interpretation compel the conclusion that the legislature intended to exclude *all* "information collected, used, or stored for health care treatment, payment, or operations" from the Privacy Act's purview, regardless of whether that information is collected from a patient or an employee. *See* 740 ILCS 14/10. Under the "nearest reasonable referent" (also referred to as the "rule of the last antecedent") and "series qualifier" canons, the modifier "under [HIPAA]"

refers to "health care treatment, payment, or operations," and is best understood as meaning "as those terms are defined by HIPAA" or "in accordance with HIPAA."

This straightforward interpretation is also consistent with a presumption that the legislature was aware that the federal government encourages health care providers to comply with HIPAA by using biometric identifiers to safeguard private health care information in their daily operations and to use biometric identifiers to limit access to controlled medications. Compliance with HIPAA already imposes significant costs on health care providers. It thus would have been eminently reasonable for the legislature to exclude biometric identifiers used in health care treatment, payment, or operations from private lawsuits under the Privacy Act in order to avoid further increasing health care costs or interfering with HIPAA compliance. By contrast, affirming the Appellate Court's decision will threaten imposing ruinous liability on health care providers and increase the already high costs of health care for the citizens of the State.

ARGUMENT

I. ESTABLISHED RULES OF STATUTORY CONSTRUCTION REQUIRE REVERSAL OF THE APPELLATE COURT'S DECISION

In its recent decisions construing the Privacy Act, this Court has emphasized the importance of faithfully applying the plain language of the Act as written, without "reading into it exceptions, limitations, or conditions the legislature did not express" or "add[ing] provisions not found in the law." *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 24; *McDonald v. Symphony Bronzeville Park, LLC*, 2022 IL 126511, ¶ 49 ("It is the province of the legislature to draw the appropriate balance. It is not our role to inject a compromise, but, rather, to interpret the acts as written.") (internal citation and quotation marks omitted). Moreover, this Court has emphasized in its Privacy Act decisions that courts should employ "[a]ccepted principles of statutory construction," including fundamental "canons of construction," when interpreting the statutory text. *Rosenbach*, 2019 IL 123186, ¶¶ 28–29.

In the decision below, however, the *Mosby* majority ignored these rules and principles and instead inserted an unwritten, policy-motivated limitation into the plain language of the Privacy Act's exclusion, "while overcomplicating a more straightforward reading of [the] exclusion." *Mosby v. The Ingalls Memorial Hosp.*, 2022 IL App (1st) 200822, ¶ 74

(Mikva, P.J., dissenting).

That straightforward reading is clear. The health care exclusion provides: "Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under [HIPAA]." 740 ILCS 14/10. The qualifier "under [HIPAA]" appears directly after three terms— "healthcare treatment, payment, and operations"—that are specifically referred to in and defined by HIPAA and its implementing regulations. *See, e.g.*, 45 C.F.R. § 164.501 (defining "health care operations," "payment," and "treatment"). As Presiding Justice Mikva explained, "health care treatment, payment, and operations" are terms of art that appear throughout HIPAA. *Mosby*, 2022 IL App (1st) 200822, ¶¶ 79–80 (citing 45 C.F.R. §§ 164.501, 164.502, 164.504, 164.506, 164.508, 164.514, 164.522, 164.528, 170.210, 170.315).

Thus, the natural implication is that "under [HIPAA]" refers to this triumvirate and means that "[b]iometric identifiers do not include . . . information collected, used, or stored for health care treatment, payment, or operations" *in accordance with (or pursuant to)* HIPAA's definition of those terms. *See* Webster's New Universal Unabridged Dictionary, *Under* (2003) ("in accordance with: *under the provisions of the law*"); Macmillan Dictionary, https://perma.cc/SD2N-VURX, under ("according to a

particular law, agreement, or system <Under the terms of the agreement, our company will receive 40% of the profits.> <The boy is considered a minor under British law.>"); Cambridge Dictionary, https://perma.cc/3EPD-XZ59, under ("in the process of, influenced or controlled by, or according to . . . Under current law, stores in this town can't do business on Sunday."). As Presiding Justice Mikva noted, it is common for legislatures in general, and the Illinois legislature in particular, to employ "under" to incorporate statutory definitions by reference in this manner. *Mosby*, 2022 IL App (1st) 200822, ¶ 81 (noting that 210 ILCS 25/2-134, 2-136, and 2-137 provide that each of the terms "health care operations," "payment," and "treatment" "has the meaning ascribed to it *under HIPAA*").

The majority opinion overcomplicates this straightforward reading by positing that "under" means "protected by" and "under [HIPAA]" modifies "information," such that the exclusion applies to "information protected by HIPAA captured from a patient in a health care setting" as well as "information protected by HIPAA collected, used, or stored for health care treatment, payment, or operations." The majority then concludes based on this reading that the exclusion covers only "patient information," not employee information collected, used, or stored for health

care treatment, payment, or operations. *See id.* ¶¶ 58–65. There are several problems with this interpretation.

First, the "nearest-reasonable-referent canon," or the last antecedent rule, provides that, "when the syntax in a legal instrument involves something other than a parallel series of nouns or verbs, a prepositive or postpositive modifier normally applies only to the nearest reasonable referent." *Black's Law Dictionary*, Nearest-Reasonable-Referent Canon; *see also In re E.B.*, 231 Ill. 2d 459, 467 (2008) ("The last antecedent doctrine, a long-recognized grammatical canon of statutory construction, provides that relative or qualifying words, phrases, or clauses are applied to the words or phrases immediately preceding them and are not construed as extending to or including other words, phrases, or clauses more remote, unless the intent of the legislature, as disclosed by the context and reading of the entire statute, requires such an extension or inclusion.").[1]

Here, the nearest reasonable referent is "health care treatment, pay-

[1] *Black's* distinguishes between the last antecedent canon and the nearest-reasonable-referent canon: "Strictly speaking, 'last antecedent' denotes a noun or noun phrase referred to by a pronoun or relative pronoun—since grammatically speaking, only pronouns are said to have antecedents. But in modern practice, and despite the misnomer, it is common to refer to the rule of the last antecedent when what is actually meant is the nearest-reasonable-referent canon." *Black's Law Dictionary*, Rule of the Last Antecedent.

ment, and operations." Accordingly, the modifier "under [HIPAA]" applies to only those terms.

The majority opinion disregards the nearest-reasonable-referent canon on the ground that, if it were employed, "under [HIPAA]" purportedly would apply only to the word "operations," a supposed "internal contradiction." *Mosby*, 2022 IL App (1st) 200822, ¶ 61. But this argument ignores the series-qualifier canon, which is a "presumption that when there is a straightforward, parallel construction that involves all nouns or verbs in a series, a prepositive or postpositive modifier normally applies to the entire series." *Black's Law Dictionary*, Series-Qualifier Canon; *see also id.*, Nearest-Reasonable-Referent Canon ("[W]hen the syntax in a legal instrument involves *something other than* a parallel series of nouns or verbs, a prepositive or postpositive modifier normally applies only to the nearest reasonable referent.") (emphasis added).

Here, "health care treatment, payment, or operations" is a series of nouns in a straightforward, parallel construction. Accordingly, the postpositive modifier "under [HIPAA]" presumably applies to all three nouns in the series. *See People v. Davis*, 199 Ill. 2d 130, 133 (2002) (applying the last antecedent rule to find that the phrase "any other deadly or dangerous weapon or instrument of like nature" modified entire series of

"knife with a blade of at least 3 inches in length, dagger, dirk, switch-blade knife, stiletto, or any other deadly or dangerous weapon or instrument of like nature" but did not modify earlier clauses in a statutory sentence (quoting 720 ILCS 5/33A–1(b))). And nothing in the context of the sentence or the statute overcomes this presumption. Indeed, the context supports the presumption, given that all three terms are defined by and used throughout HIPAA and thus are naturally grouped together as terms of art.

In an attempt to escape this conclusion, the majority opinion contends that the entire sentence is "a straightforward parallel construction," such that the series-qualifier canon would require "under [HIPAA]" to apply to the "two categories of information" listed in the sentence. *Mosby*, 2022 IL App (1st) 200822, ¶ 62. This contention misapprehends the series-qualifier canon, which applies to a series of *nouns or verbs*, not entire phrases or sentences. *See* Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 147–48 (2012) (listing such examples as "unreasonable searches and seizures" and "high crimes and misdemeanors"). To be sure, "[i]nformation" and "health care treatment, payment, and operations" are nouns, but only the latter are "nouns in parallel." *Id.* at 153. In fact, "health care treat-

ment, payment, and operations" are "in a prepositional phrase modifying" the phrase "information collected, used, or stored," making the phrase all the more clearly subject to the nearest-reasonable-referent canon. *Id.* And "information captured from a patient in a health care setting," is separated from "under [HIPAA]" by another use of the word "information" and *two* parallel series of nouns or verbs—"collected, used, or stored" and "health care treatment, payment, and operations." If "under [HIPAA]" had been intended to modify "information," as the majority opinion posits, then the legislature would have written, "Biometric identifiers do not include information under [HIPAA] that is captured in a health care setting or collected, used, or stored for health care treatment, payment, or operations."

Second, the majority opinion uses an unnatural definition of "under" given the context in which the word is used. "The word 'under' has many dictionary definitions and must draw its meaning from its context." *Ardestani v. I.N.S.*, 502 U.S. 129, 135 (1991). Where, as here, "under" appears in a statute, its most natural meaning is the legalistic "subject to," "governed by," or "in accordance with" synonyms of "pursuant to." *Id.*; *Black's Law Dictionary*, Pursuant To (11th ed. 2019) ("1. In compliance with; in accordance with; under <she filed the motion pursuant to the court's order>. 2. As authorized by; under <pursuant to Rule 56, the

plaintiff moves for summary judgment>."); *accord* Bryan A. Garner, *A Dictionary of Modern Usage*, Under (2d ed. 1995) ("[U]nder is preferable to *pursuant to* when the noun that follows refers to a rule, statute, contractual provision, or the like.").

By contrast, as Defendants note in their Petition, *see* Pet'n at 14, the majority opinion selected a definition of "under"—"protected by" or "covered by"—that is generally associated in dictionaries with *physical* concealment. *See* Merriam-Webster Online Dictionary, https://perma.cc/YQ84-4D2J, ("below or beneath so as to be overhung, surmounted, covered, protected, or concealed by," for instance, "under sunny skies" or "a soft heart under a stern exterior"); *see also* Collins Dictionary, https://perma.cc/7CBD-57BR, under ("If a person or thing is under something, they are at a lower level than that thing, and may be covered or hidden by it," for instance, "swimming in the pool or lying under an umbrella").

Third, the straightforward reading avoids any surplusage, consistent with the canon that, "if possible, every word and every provision in a legal instrument is to be given effect." *Black's Law Dictionary*, Surplusage Canon; *see Kozak v. Ret. Bd. of Firemen's Annuity & Ben. Fund of Chicago*, 95 Ill. 2d 211, 216 (1983) (refusing to adopt a construction of a statutory phrase that "would strip [a] word … of any contribution to the

meaning of the statute, thus violating the rule of statutory construction which requires a statute to be applied in a way that no word, clause or sentence is rendered superfluous or meaningless").

As Justice Mikva explained, "[u]nder [the Appellate Court's] reading, there is simply no reason to use the word 'information' twice in the disjunctive, suggesting that the exclusion is referencing two different kinds of information," one defined by its "source" and the other defined by the purpose for which it is used. *Mosby*, 2022 IL App (1st) 200822, ¶¶ 75, 84 (Mikva, P.J., dissenting). If the second use of "information" had not been intended to denote a separate category of information, then the legislature easily could have omitted it, writing instead, "Biometric identifiers do not include information that is captured from a patient in a health care setting or collected, used, or stored for health care treatment, payment, or operations under [HIPAA]."

Indeed, if the statute had been intended to exclude only information protected by HIPAA, or only patient information, then the legislature could simply have written, "Biometric identifiers do not include information protected by [HIPAA] that is captured in a health care setting or collected, used, or stored for health care treatment, payment, or operations," or, more clearly, "Biometric identifiers do not include patient information that is captured in a health care setting or collected, used, or

stored for health care treatment, payment, or operations." The only thing the legislature would not have done to achieve the majority's posited purpose is to enact the language that it did.

The rules of statutory construction are not tools that can be invoked when convenient and ignored when inconvenient. They are "principles that guide this [C]ourt's construction of statutes" and should be "utilized in *every* statutory construction case." *JPMorgan Chase Bank, N.A. v. Earth Foods Inc.*, 238 Ill. 2d 455, 462 (2010) (emphasis added). This Court has consistently refused to impose extratextual limitations on the text of the Privacy Act in order to achieve specific outcomes or to vindicate policy preferences. This Court should adhere to that commitment here as well.

II. AFFIRMING THE LOWER COURT'S DECISION WOULD IMPOSE SIGNIFICANT ADDITIONAL COSTS ON ILLINOIS HEALTH CARE PROVIDERS AND CONSUMERS

Health care is expensive. National health care "spending was $4.3 trillion or $12,914 per capita in 2021." Dr. Apoorva Rama, *National Health Expenditures, 2021: Decline in Pandemic-Related Government Spending Results in 8-Percentage Point Decrease in Total Spending Growth*, Am. Med. Ass'n, at 1–2 (2023), *available at* https://perma.cc/F7ND-RJRU. This amounts to "18.3 percent of GDP in 2021, less than the unprecedented 19.7 percent of GDP in 2020[,] but

still not as low as 17.6 percent in 2019 and 2018." *Id.*

A substantial portion of the cost of health care is attributable to regulatory compliance. "[T]he costs that hospitals have incurred for implementing HIPAA's privacy provisions," for example, "are estimated to exceed $22 billion." Jack Brill, *Giving HIPAA Enforcement Room to Grow: Why There Should Not (Yet) Be a Private Cause of Action*, 83 NOTRE DAME L. REV. 2105, 2132–33 (2008); *see also* Mindy J. Steinberg and Elain R. Rubin, *The HIPAA Privacy Rule: Lacks Patient Benefit, Impedes Research Growth*, Ass'n for Academic Health Cntrs. (2009), *available at* https://perma.cc/W8WX-UV45 (finding that HIPAA "has imposed barriers to research at academic health centers"). "According to one study, the costs associated with implementing HIPAA ranged from a minimum of $10,000 for a small physician group practice[] to as much as $14 million for a larger covered entity." *Id.* at 2132–33. To comply with HIPAA's highly technical guidelines, providers must train their staff, employ privacy officers, develop policies, and install special equipment. *Id.* And these costs inevitably are passed on to health care consumers. *Id.* at 2135.

The costs of HIPAA compliance, while significant, are at least limited because Congress chose not to provide a private right of action for HIPAA violations. *See Payne v. Taslimi*, 998 F.3d 648, 660 (4th Cir. 2021). Indeed,

alleged harms for "privacy violations" are often intangible, while the legal costs to defend against them can be immense. *See* U.S. Chamber of Commerce, Institute for Legal Reform, *Ill-Suited: Private Rights of Action and Privacy Claims*, 1–14 (July 2019), *available at* https://perma.cc/5JEJ-V7ZV (detailing how private rights of action, which often allege "intangible[] or nonexistent" harms, "clutter courts," "chill[] innovation," and increase costs). Private rights of action are also prone to abuse. Motivated by the promise of large cash awards, plaintiffs' attorneys need only file boilerplate complaints to coerce "staggeringly high settlements." *See id*. at 15–17; *see also Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co*., 559 U.S. 393, 445 n.3 (2010) (Ginsburg, J., dissenting) ("When representative plaintiffs seek statutory damages, [the] pressure to settle may be heightened because a class action poses the risk of massive liability unmoored to actual injury.").

Medical malpractice suits provide a useful analogue in this regard. Prominent researchers at Duke University and the Massachusetts Institute of Technology, including an architect of the Patient Protection and Affordable Care Act (Obamacare), recently found "evidence that liability immunity [from private malpractice lawsuits] reduces inpatient spending by 5% with *no* measurable negative effect on patient outcomes." Michael Franks & Jonathan Gruber, *Defensive Medicine: Evidence from*

Military Immunity, 11 AM. ECON. J. OF ECON. POLICY 3, 197 (2019), *available at* https://perma.cc/58RQ-SHZ2; *see also id*. at I.B (discussing "[a] number of [medical] studies" from early 2000s finding that medical liability leads to increased health care costs); *see also* James D. Reschovsky & Cynthia B. Saiontz-Martinez, *Malpractice Claim Fears and the Costs of Treating Medicare Patients: A New Approach to Estimating the Costs of Defensive Medicine*, 53 Health Serv. Res. 3, 1498–1516 (2018), *available at* https://perma.cc/ZJF9-3EHW (noting that "malpractice fear" leads to higher "patient spending" and "likely contributes substantial additional costs" to health care).

Viewed in this light, the Illinois legislature's decision to avoid imposing additional litigation and compliance costs on health care providers by excluding *all* information "collected, used, or stored for health care treatment, payment, or operations" makes perfect sense. Health care providers regularly make use of biometric identifiers to protect patient data and to monitor access to controlled substances. *See* Electronic Prescriptions for Controlled Substances, 75 Fed. Reg. 61, 16250 (Mar. 31, 2010), *available at* https://perma.cc/ULZ4-YYCT (explaining that, as of 2008, health care systems had been routinely using biometrics for years "as a tool to provide security for electronic patient data." (citing Healthcare Information and Management Systems Society Survey (Oct.

28, 2008))).

The legislature presumably was aware of the widespread use of biometrics for health care treatment, payment, and operations, as well as of the fact that the federal government had been encouraging their use to comply with HIPAA and other federal laws. In 2006, for example, the U.S. Department of Health and Human Services, which administers and enforces HIPAA, recommended that covered entities "use [] biometrics, such as fingerprint readers," to protect access to sensitive health data in the course of health care treatment, payment, and operations. Dep't of Health and Human Servs., *HIPAA Security Guidance*, 5 (Dec. 28, 2006), *available at* https://perma.cc/UH28-Y8T9. Similarly, in 2008 the federal government recommended that health care providers use biometric identifiers to monitor access to controlled substances. *See, e.g.*, Risk Assessment of Electronic Prescriptions of Controlled Substances, 73 Fed. Reg. 125, 36735–36 (June 27, 2008), *available at* https://perma.cc/H4BB-Y444 (describing authentication protocols for distributing controlled substances, including "biometrics"). Two years later, the U.S. Drug Enforcement Agency codified this recommendation. *See* 21 C.F.R. § 1311.115 (2010). And the American Society of Health-System Pharmacists also recommends that, before accessing and dispensing controlled substances, pharmacists use biometric readers "whenever possible." *See* American

Society of Health-System Pharmacists, *ASHP Guidelines on Preventing Diversion of Controlled Substances*, 79 AM. J. OF HEALTH-SYSTEM PHARMS. 24, 2288–89 (Dec. 15, 2022); *see also* Institute for Safe Medication Practices, *Guidelines for the Safe Use of Automated Dispensing Cabinets* § 2.2 (Feb. 7, 2019), *available at* https://perma.cc/9KMY-EKSU (same).

Given the proliferation of—and acute need for—the use of biometric identifiers by health care providers, the Appellate Court's decision to limit the Privacy Act's health care exclusion to patient information, in disregard of the plain text of the statute, threatens to impose crippling costs and "annihilative liability," *Cothron*, 2023 IL 128004, ¶ 40 (Overstreet, J., dissenting), on Illinois health care providers. And those costs will ultimately be borne by Illinois consumers.

Unlike all other U.S. states that have enacted biometric privacy laws (as well as the European Union), Illinois' Privacy Act provides for a private right of action by "any person aggrieved by a violation of" the Privacy Act. 740 ILCS 14/20. Other state biometric privacy laws vest enforcement exclusively with the attorney general. *See, e.g.*, Ark. Code § 4-110-108 ("Any violation of this chapter is punishable by action of the Attorney General."); Cal. Civ. Code § 1798.199.90 ("Attorney General enforcement"); Tex. Bus. & Com. Code § 503.001(d) ("The attorney general

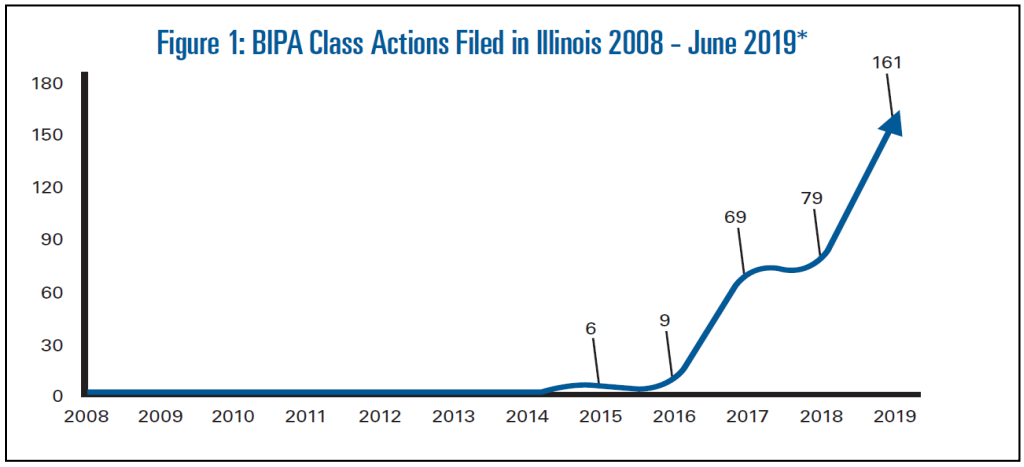
may bring an action to recover the civil penalty."); Va. Code Ann. § 59.1-584(A) ("The Attorney General shall have exclusive authority to enforce the provisions of this chapter."); Wash. Rev. Code § 19.375.030(2) ("This chapter may be enforced solely by the attorney general") (Washington); *see also* Neil L. Bradley, *U.S. Chamber Letter on National Privacy Legislation* (May 31, 2022), *available at* https://perma.cc/XD4Z-W43G (explaining that "[m]ore than 130 countries have enacted general privacy protections, and five state legislatures have passed comprehensive data protections bills," yet a "private right of action is not included in any of these state laws, nor is it part of the" European data regulation).

Moreover, the Privacy Act allows a private plaintiff to recover fixed statutory damages of either $1,000 for each negligent violation of the statute or $5,000 for each intentional or reckless violation, without the need to prove any actual loss stemming from a violation of the statute's requirements. *See* 740 ILCS 14/20. Nor is there any cap on attorney's fees and costs, or a safe harbor to protect against liability for trivial violations. *See* 740 ILCS 14/20(3); *cf.* N.Y.C. Admin. Code § 22-1203 (providing that, "[i]f, within 30 days, [a] commercial establishment cures" a violation of the city's biometric privacy law, "no action may be initiated.").

This Court's recent decisions interpreting the Privacy Act have also

significantly expanded potential liability under the statute. After remaining largely dormant for years after the statute's enactment, lawsuits under the Privacy Act spiked in January 2019 after *Rosenbach*, 2019 IL 123186, held that plaintiffs need not show any actual injury in order to sue.

This holding spurred a massive wave of class actions against entities of all size. In fact, more than 160 cases were filed in the first half of 2019 alone:



Institute for Legal Reform 4. "2019 [then] closed out with close to 300 [Privacy Act] lawsuits filed in Illinois—almost four times the number of cases filed the year before." *Id.*

Subsequently, in *Tims v. Black Horse Carriers, Inc.*, this Court held that Privacy Act actions are governed by a five-year statute of limitations instead of the shorter one-year statute of limitations. 2023 IL 127801, ¶ 5. Then, in *Cothron*, this Court held that claims accrue "each time a

private entity scans or transmits an individual's biometric identifier or information." 2023 IL 128004, ¶ 1. A majority of this Court was unmoved by the possibility of disastrous damages for organizations, including billions of dollars for one business alone. *Id.* ¶ 40. Three justices dissented in *Cothron.* They noted that the majority opinion "will lead to consequences that the legislature could not have intended," including "annihilative liability for businesses." *Id.* ¶¶ 48, 61 (Overstreet, J., dissenting); *see also Cothron v. White Castle System, Inc.*, 20 F.4th 1156 (7th Cir. 2021) (warning of the "staggering damages awards" from an accrual rule that recognizes each scan as a separate violation—"consequences [] the General Assembly could not possibly have intended").

These decisions collectively, together with the unlimited attorneys' fees provided under the Privacy Act, *see* 740 ILCS 14/20(3), have caused an explosion of lawsuits against entities of all size. Recent reports have catalogued nearly 2,000 state-court class actions alleging Privacy Act violations in just the past few years alone,[2] while federal-court Privacy Act class actions have increased more than tenfold.[3] And, even if no violations occur going forward, it will be half a decade before the gold rush

[2] Erin Mulvaney, *Biometric-Privacy Rulings in Illinois Expand Potential Liability for Companies*, WSJ (Feb. 27, 2023), available at https://perma.cc/JZB8-FEUR; Daniel Wiessner, *White Castle could face multibillion-dollar judgment in Illinois privacy lawsuit*, Reuters (Feb. 17, 2023), available at https://perma.cc/2KBV-2LMQ .

[3] Institute for Legal Reform 5.

peters out, given the five-year statute of limitation period applicable to Privacy Act claims. *See Tims*, 2023 IL 127801, ¶ 5.

Plaintiffs' lawyers are the primary beneficiaries of these lawsuits. For example, in the *Facebook* settlement involving facial recognition technology and the Privacy Act, a judge approved a $650 million settlement, of which $97.5 million went to attorneys' fees. Institute for Legal Reform 6. As yet another instance, in April 2021, another judge approved a $25 million Privacy Act class action, with counsel receiving more than $8.5 million. *Id*. The list goes on. *See id*. at 6–7. It is not just large corporations facing Privacy Act lawsuits either. Local businesses are also fending off claims for alleged violations. *See id*.

In light of the foregoing, imposing the Appellate Court's extra-textual limitation on the Privacy Act's health care exclusion would impose extreme additional costs on Illinois health care providers, to the ultimate detriment of Illinois health care consumers. Moreover, many health care institutions will be dissuaded from deploying useful biometric technologies, such as medication-distribution tools to safeguard controlled substances.

Such a result is contrary to the intent of the legislature, which specifically excluded critical industries and, here, particular segments and operations within a critical industry from the Privacy Act's reach. *See*

also, e.g., 740 ILCS 14/25(a) (legal); *id.* 14/25(c) (financial); *id.* 14/25(d) (security); *id.* 14/25(e) (government).

To be clear, the Privacy Act does not provide a blanket exemption for the entire health care industry, but it does offer a critical "exclusion to allow the healthcare industry to use biometric information for treatment, payment[,] and operations" for patient care consistent with "HIPAA." *Mosby*, 2022 IL App (1st) 200822, ¶ 87 (Mikva, P.J., dissenting). "It is hard to imagine a better example of this than finger-scan information collected by [Defendants] to ensure that medication is properly dispensed." *Id.*

It is just as hard to imagine why the legislature would have wanted to interfere with HIPAA compliance and the safeguarding of controlled medication and to expose Illinois' health care industry, already prone to high inflation, to an explosion of lawsuits against providers of all size who will, in turn, pass on those costs to their patients. Such consequences are not what the legislature intended.

CONCLUSION

For the foregoing reasons, and those presented by Defendants-Appellants, the decision of the Appellate Court should be reversed.

Dated: April 26, 2023

Respectfully submitted,

/s/ *Daniel D. Birk*

Daniel D. Birk
John K. Adams
EIMER STAHL LLP
224 South Michigan Avenue
Suite 1100
Chicago, Illinois 60604
(312) 660-7600
dbirk@eimerstahl.com
jkadams@eimerstahl.com

Rule 341(c) Certificate of Compliance

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 4,965 words.

/s/ *Daniel D. Birk*
Daniel D. Birk

Certificate of Filing and Service

The undersigned certifies under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, that on April 26, 2023, the foregoing was filed with the Clerk of the Supreme Court of Illinois using the court's electronic filing system and served on all parties to this appeal that are listed with that system.

Persons Served:

Ryan F. Stephan
James B. Zouras
Andrew C. Ficzko
Catherine T. Mitchell
Paige L. Smith
STEPHAN ZOURAS, LLP
100 North Riverside Plaza
Suite 2150
Chicago, IL 60601
Tel: (312) 233-1440
Email: rstephan@stephanzouras.com
jzouras@stephanzouras.com
aficzko@stephanzouras.com
cmitchell@stephanzouras.com
psmith@stephanzouras.com

Attorneys for Plaintiffs-Appellees

Gary M. Miller (6229867)
Matthew C. Wolfe (6307345)
Elisabeth A. Hutchinson (6338043)
SHOOK, HARDY & BACON L.L.P.
111 South Wacker Drive
Suite 4700
Chicago, IL 60606
(312) 704-7700
Email: gmiller@shb.com
mwolfe@shb.com
ehutchinson@shb.com

Attorneys for Defendant-Applicant Becton, Dickinson and Company

Joel Griswold
Bonnie Keane DelGobbo
BAKER & HOSTETLER LLP
1 North Wacker Drive
Suite 4500
Chicago, IL 60606
Tel: (312) 416-6200

Email: jcgriswold@bakerlaw.com
bdelgobbo@bakerlaw.com

Counsel for Northwestern Lake Forest Hospital and Northwestern Memorial HealthCare

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct, except as to matters therein stated to be on information and belief and as to such matters the undersigned certifies as aforesaid that he verily believes the same to be true.

/s/ *Daniel D. Birk*
Daniel D. Birk