S286699

Case No. S_____

IN THE SUPREME COURT OF CALIFORNIA

JEAN PAUL MAGALLANES, guardian ad litem for JACOB MAGALLANES, on behalf of himself and all other similarly situated,

Plaintiff and Respondent,

v.

ILLUMINATE EDUCATION, INC., a California corporation,

Defendant and Petitioner.

After a Decision by the Court of Appeal for the
Second Appellate District, Division Six
Court of Appeal Case No. B327683
Reversing a Judgment Entered in the Superior Court of Ventura County
Superior Court Case No. 56-2022-00567324-CU-MC-VTA
Hon. Benjamin F. Coats

PETITION FOR REVIEW

KIRKLAND & ELLIS LLP

*Devin S. Anderson
(*pro hac vice* pending)
devin.anderson@kirkland.com
95 South State Street
Salt Lake City, Utah 84111
Telephone: (801) 877-8115

Cynthia Love (SBN 331988)
cynthia.love@kirkland.com
95 South State Street
Salt Lake City, Utah 84111
Telephone: (801) 877-8243

Tammy A. Tsoumas (SBN 250487)
tammy.tsoumas@kirkland.com
2049 Century Park East, Suite 3700
Los Angeles, CA 90067
Telephone: (310) 552-4334

Attorneys for Defendant and Petitioner Illuminate Education, Inc.

REDACTED - FILED CONDITIONALLY UNDER SEAL

Table of Contents

TABLE OF AUTHORITIES

Page(s)

California Cases

Non-California Cases

Statutes

Rules

Other Authorities

PETITION FOR REVIEW

In this case, the California Court of Appeal mangled two important statutes by departing from their text, their purpose, and other decisions from the Court of Appeal, with predictably disastrous results. The Confidentiality of Medical Information Act (CMIA) provides a cause of action against "providers of health care" and related entities who have disclosed an individual's medical information without authorization or failed to maintain the confidentiality of that information. The Customer Records Act (CRA) is a consumer-protection statute that requires businesses to give their customers certain information, including timely notice of data breaches. Both statutes address specific problems: the CMIA provides an important tool for keeping personal medical information confidential while in the hands of medical providers or their proxies, and the CRA ensures that business dealings operate with transparency and trust. Both statutes frequently appear in lawsuits arising out of cyberattacks.

Thanks to the Court of Appeal's remarkable decision, there is now dangerous uncertainty concerning these statutes' scope. Petitioner Illuminate Education provides educational software to schools to facilitate teaching and student learning. Illuminate does not offer or provide medical services, and it does not work for or with any medical providers at schools. Nor does it form relationships with students or their parents. Two and a half years ago, Illuminate was the victim of a cyberattack, in which a criminal actor exfiltrated some databases [redacted] which included some educational information about students in

certain school districts. There are no reported instances of identity theft or any other form of harm arising out of this incident. Plaintiffs filed a putative class action against Illuminate under both the CMIA and the CRA in Ventura County Superior Court. The trial court sustained Illuminate's demurrer, explaining that plaintiffs had failed to show that either statute applied to this circumstance.

The Court of Appeal reversed and adopted a novel interpretation of the CMIA that "extends" its reach "beyond medical providers" and far beyond what the statute can bear.[1] (Slip Op. at 1.) Under the court's new reading, a "provider of health care" includes a technology company like Illuminate with no clients in the healthcare industry and whose products are used only for educational purposes. It would also include schools, transportation companies, religious organizations, internet providers, community sports organizations, and summer camps—in short, any entity that happens to "possess or store" *any* piece of information about an individual's physical or mental condition, no matter how temporary the storage or the purpose for which it is stored. (*Id.* at 4.) If that were not bad enough, the Court of Appeal also ignored the text and held that plaintiffs need not show an "affirmative communicative act" or a loss of confidentiality to allege liability, creating a conflict with other decisions from that same Court. The implications of these rulings are astounding, and

[1] Unless otherwise noted, all quotations have been cleaned up and emphases added. A copy of the Court of Appeal's opinion is attached as Exhibit A. (Cal. Rules of Court, rule 8.504(b)(4).)

all the more so where the CMIA imposes nominal damages of $1,000 per person and does not require that a plaintiff "suffered or was threatened with actual damages." (Civ. Code, § 56.36(b)(1).)

The court then dramatically expanded the scope of the CRA, departing from the text and every other court to interpret the statute in holding that a claim could be brought without showing that the plaintiff was (i) a "customer" of the defendant as defined by the statute and (ii) injured by the alleged violation of the statute.

Individually, each of these errors was significant; together they are catastrophic. The CMIA, with its draconian nominal damages, now looms over information-technology companies, schools, and many other businesses, with potential liability stretching into the millions or even billions. And the CRA has now been stretched to cover entities that have no business dealings at all with the plaintiffs. As cyberattacks proliferate, companies that maintain personal information face uncertain liability under the CMIA and CRA due to the Court of Appeal's sharp departure from the statutory text and established California law. To ensure a correct and uniform reading of both the CMIA and the CRA in California courts, this Court should grant review.

ISSUES PRESENTED FOR REVIEW

1. Did the Court of Appeal err in expanding the reach of the CMIA to
    (i) include entities that happen to possess or maintain information about an individual's physical or mental condition for any reason, contrary to the statutory text; and
    (ii) allow claims where a plaintiff has failed to show disclosure or breach of confidentiality, contrary to the statutory text and other decisions of that same court?
2. Did the Court of Appeal err in expanding the reach of the CRA to include, contrary to text and precedent, claims brought by a plaintiff who
    (i) is not a "customer" under the statute; and
    (ii) alleges no harm from the statutory violation?

IMPORTANCE OF THE ISSUES

Review of a Court of Appeal decision is appropriate "when "necessary to secure uniformity of decision or to settle an important question of law." (Cal. Rules of Court, rule 8.500(b)(1).) This Court is likely to grant "review of a decision of the Court of Appeal on a recurring matter of statewide concern." (*Howard Jarvis Taxpayers Ass'n v. City of La Habra* (2001) 25 Cal.4th 809, 817.)

The proper scope of both the CMIA and the CRA are recurring matters of statewide concern on which decisions of the Court of Appeal have diverged. In holding that the CMIA applies

to *any* company that possesses or stores personal medical information, the Court of Appeal contradicted several other courts in this state, which have concluded that a company must be "organized *for the purpose of* maintaining medical information" (as the CMIA itself specifies). (*Oddei v. ScanSTAT Techs., LLC* (9th Cir. Dec. 8, 2022) 2022 WL 17538747, at *1.) In holding that a CMIA claim need not include allegations of affirmative disclosure or breach of confidentiality, the court below split with previous Court of Appeal decisions. (*See Sutter Health v. Superior Court* (2014) 227 Cal.App.4th 1546, 1554-55 (violating § 56.10 requires an "affirmative communicative act" and violating § 56.101 requires "an actual confidentiality breach"); *Regents of University of California v. Superior Court* (2013) 220 Cal.App.4th 549, 564, 569-70 (same).) And in permitting plaintiffs to pursue CRA claims without being "customers" as defined by the statute or suffering an injury from the alleged statutory violation, the court parted ways with yet another Court of Appeal decision, which explicitly held the opposite. (*Boorstein v. CBS Interactive, Inc.* (2013) 222 Cal.App.4th 456, 467.) These significant expansions of statutory scope and resulting conflict with other decisions of the Court of Appeal warrant immediate review.

STATEMENT OF THE CASE

A.
Factual Background

Illuminate is a California "education company" that provides programs, applications, and technology support to school districts to aid in teaching students. (AA75.) Illuminate offers many

education-related services, including screening, progress monitoring, data analysis, and remote-teaching assistance. (AA77-78.) These services are used to "store[] and assess[] data concerning students" and assist with "educational evaluation, monitoring of progress, and determining an educational plan" for each of them. (AA76.) To help educators, parents, and students track academic achievement and plan for student success, Illuminate offers an internet platform "on a contract basis" to schools and school districts. (AA76.) One of Illuminate's clients is the Ventura County Office of Education. (AA140.)

In January 2022, Illuminate discovered that certain databases associated with a handful of older products had been accessed without authorization. (AA132.) As Illuminate later reported to government regulators, a threat actor exfiltrated data from these databases [redacted] There is no evidence that the threat actor ever viewed or disseminated any data: Illuminate explained to its client the Office of Education that it "immediately took steps to secure the affected applications and launched an investigation," in which it found "no evidence that any information was subject to actual or attempted misuse." (*Ibid.*) After concluding its investigation and at the request of the Office of Education, Illuminate notified Ventura County students, including plaintiffs, whose data might have been extracted [redacted]. (AA79, 132).

B.
Proceedings in Superior Court

Plaintiffs filed a class-action complaint in Ventura County Superior Court alleging that Illuminate violated the CMIA and CRA. (AA4-32.) Following briefing and argument, the trial court sustained Illuminate's demurrer to the First Amended Complaint—the operative pleading here—and explained that plaintiffs had failed to state a cognizable claim under either the CMIA or the CRA. (AA451.) The court rejected plaintiffs' CMIA claims because plaintiffs had not shown that Illuminate was a "provider of health care" or other covered entity as defined by the statute or that "disclosure" of protected information under Civil Code section 56.10 had occurred. (*Ibid.*) And the court explained that plaintiffs' CRA claim failed for two independent reasons: (1) because the CRA created at most a duty for Illuminate to notify the school districts, which were Illuminate's customers—as opposed to plaintiffs, who were not; and (2) because plaintiffs had failed to allege an injury specific to the alleged delay in notification, which was the alleged CRA violation. (*Ibid.*)

C.
Proceedings in the Court of Appeal

Plaintiffs appealed, and the Court of Appeal reversed in a published opinion. (AA460; Slip Op. at 13.) *First*, the court reasoned that Illuminate fell within the scope of the CMIA. In addition to traditional licensed medical entities, the statute defines as a "provider of health care" "[a]ny business *organized for the purpose of maintaining medical information* in order to make the information available to an individual or a provider of health

care" or "for the diagnosis and treatment of the individual." (Civ. Code, § 56.06(a).) The court held that Illuminate fit within that definition because Illuminate "'works with school districts to provide assistance with special education and mental health services'" and allegedly "possess[ed]" or "store[d]" medical information. (Slip Op. at 4-5 (quoting AA144).) The court rejected Illuminate's argument that section 56.06 extends only to entities "organized for the purpose of maintaining medical information." (*Id.* at 6.) Because the CMIA is a "remedial statute" with "broad scope," the court emphasized that reading the text literally would "undermine[] the purpose of the CMIA." (*Id.* at 6-7.)

Second, the court held that plaintiffs could establish a violation of the CMIA without showing an "affirmative communicative act" on Illuminate's part or loss of confidentiality of their medical information. (*Id.* at 7.) Plaintiffs brought a CMIA claim for "the unauthorized release of their individual identifiable 'medical information' made unlawful by Civil Code §§ 56.10 and 56.101." (AA94.) Those provisions of the CMIA prohibited unauthorized "disclosure" of medical information and failure to "preserve[] the confidentiality" of such information, respectively. (Civ. Code, §§ 56.10(a), 56.101(a).) But the court held that plaintiffs need only allege that Illuminate was negligent in storing the data and that there was a cyberattack. (Slip Op. at 8.) It concluded that plaintiffs' allegation of "negligent storage leading to the unauthorized access of medical information," without more, established a viable CMIA claim. (*Ibid.*)

Third, the court upheld plaintiffs' CRA claim, again reasoning that the statute was "remedial and must be interpreted broadly." (Slip Op. at 11.) Although plaintiffs were not Illuminate's customers and had no contracts (or even contact) with Illuminate, the court reasoned that they were "intended beneficiar[ies] under the CRA," and that any interpretation that would "leave[] a statutory beneficiary without protection" would "undermine[] the statutory intent" of the CRA. (*Ibid.*) While Illuminate may have had contracts only with schools, the "ultimate 'customers,' consumers, and beneficiaries of its educational services were the students who trusted Illuminate to protect their information." (*Ibid.*) The court did not address Illuminate's argument that it had no obligation to report the breach to plaintiffs because it neither "owned" nor "licensed" the data in question. (Civ. Code, § 1798.82(a).) On the question of harm, the court held that plaintiffs' allegations of a five-month delay in notification, standing alone, satisfied any statutory requirement that plaintiffs show injury-in-fact. (*Id.* at 11-12.)

REASONS FOR GRANTING REVIEW

I.
The Court Should Grant Review to Ensure the Uniform and Correct Application of the CMIA in California Courts

The CMIA "is intended to protect the confidentiality of individually identifiable medical information obtained from a patient by a health care provider, while at the same time setting forth limited circumstances in which the release of such information to specified entities or individuals is permissible."

(*Loder v. City of Glendale* (1997) 14 Cal.4th 846, 859.) To that end, the statute carefully describes the type of information that is protected, the circumstances that lead to liability, and the entities that are bound by its terms. "[T]o violate the act, a provider of health care must make an unauthorized, unexcused disclosure of privileged medical information," as those terms are defined by the statute. (*Heller v. Norcal Mut. Ins. Co.* (1994) 8 Cal.4th 30, 38.)

The CMIA claim against Illuminate in this case was not viable under the statute's own terms and existing precedent. In ruling against Illuminate, the court displayed an eagerness to "extend" the law based on what it viewed as the broad remedial purpose of the statute. (Slip op. at 1, 6-7.) But that ruling exposes large swaths of the information economy to potential crippling statutory damages in class actions, contrary to the Legislature's intent as expressed in the statutory text. This Court should grant review to ensure the uniform and correct application of the CMIA.

A.
The Court Should Grant Review to Ensure the Uniform and Correct Application of the CMIA's Definition of "Provider of Health Care"

The threshold issue in any CMIA claim is whether the statute applies to the parties. The CMIA was designed to govern licensed and certified healthcare professionals, and there is no dispute that Illuminate is neither. (Civ. Code, § 56.05(p) (defining a "Provider of health care" as a "person licensed or certified" pursuant to specific legal provisions.) But the Legislature, recognizing that the medical profession was evolving, updated the statute to include certain entities that work closely with

healthcare professionals as well. The CMIA was therefore amended to define the following as "providers of health care":

> Any business *organized for the purpose of maintaining medical information* ... in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual[; and]
>
> Any business that offers software or hardware to consumers, including a mobile application or other related device *that is designed to maintain medical information* … in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual.

(Civ. Code, § 56.06(a)-(b).)

The updated definition of "provider of health care" in section 56.06 is careful. The Legislature did not intend for the CMIA to create liability for every business that happens to possess medical information. Rather, it specified that only a business "organized *for the purpose of maintaining medical information*" or one that "offers software or hardware to consumers … that is *designed to maintain medical information*" was covered by the statute. (*Ibid.*) And the purpose of the business or application must further be to

allow the individual to manage the information or for diagnosis and treatment by a healthcare provider, upon request. (*Ibid.*)

Thus, a company that designs apps to organize pharmacy prescriptions would qualify as a "provider of health care." But a company that designs generic note-taking apps would not, even if a doctor or patient could use the app to record medical information alongside other information. Section 56.06 therefore offers a sensible update for the CMIA in an era of telehealth and mobile healthcare applications, without sweeping in the entire information economy.

The Court of Appeal's decision upended that careful balancing. The court erroneously held that Illuminate fell within the ambit of section 56.06 simply because it "possess[ed] or store[d]" data that allegedly included medical information.[2] (Slip Op. at 4, 7.) That breathtaking expansion of the CMIA's scope erased the critical statutory focus on *purpose*. The court did not find that Illuminate was "organized for the purpose of maintaining medical information" as required by the text of section 56.06(a). Nor could it, because the pleaded facts showed that Illuminate was an "education company." (AA75.) Similarly, the court did not find that any of Illuminate's products were "designed to maintain

[2] The court also referred to other definitions scattered throughout the CMIA in holding that Illuminate met the definition for "provider of health care" under section 56.06. (Slip Op. at 7 (citing the definitions of "any other entity" in § 56.11 and "recipient of medical information" in § 56.13).) Those definitions are irrelevant to the CMIA claim at issue in this case, which was brought only under sections 56.10 and 56.101 (both of which apply only to "provider[s] of health care, health care service plan[s], or contractor[s]").

medical information," as section 56.06(b) specifies. Plaintiffs had acknowledged that Illuminate's products were designed to do something very different—to "store[] and assess[] data concerning students" "as an aid to educational evaluation, monitoring of progress, and determining an educational plan." (AA76.) For the same reasons, the court did not and could not find that the purpose of Illuminate's products was for the students to manage their medical information or for diagnosis and treatment by a healthcare provider. (Civ. Code, § 56.06(a)-(b).)

The Court of Appeal instead abandoned these critical textual safeguards and held that the CMIA applies to any business that "maintain[s] medical information … *whether or not the business was organized for that purpose*." (Slip Op. at 6.) The basis for this holding was an article that purported to summarize recent changes to the CMIA in the California Lawyers Association journal. (*See id.* (quoting Joseph R. Tiffany II et al., *The Doctor Is In, But Your Medical Information is Out: Trends in California Privacy Cases Relating to Release of Medical Information*, 24 Cal. State Bar J. 206, 225 (2015)).) Musings of practitioners in a bar association article are no substitute for the statute's text, which plainly focuses on the purpose of the business or product. Moreover, the relevant portion of the article simply points out that section 56.06(b) was added to cover companies that design medical software, even if the companies themselves have no explicitly medical purpose as in section 56.06(a). Section 56.06(b) simply shifts the purpose analysis from the company to the application. It does not dispense with the requirement entirely.

It is not surprising that the Court of Appeal cited no legal authority for its holding: there is none. To the contrary, courts have consistently held that simply collecting or maintaining medical information, with no accompanying medical purpose, does *not* create obligations under CMIA. The Ninth Circuit rejected a recent CMIA claim where the complaint "include[d] no allegation that" the defendant "was organized for the purpose of maintaining medical information." (*Oddei*, *supra,* 2022 WL 17538747, at *1.) And as a recent district court decision explained, "§ 56.06(a) requires more than an allegation that" a defendant "maintained or even presently maintains medical information"; the defendant "must have been 'organized *for the purpose of* maintaining medical information.'" (*In re Accellion, Inc. Data Breach Litig.* (N.D. Cal. Jan. 29, 2024) 2024 WL 333893, at *13 (quoting Civil Code § 56.06(a)); *see also Fernandez v. Leidos, Inc.* (E.D. Cal. 2015) 127 F.Supp.3d 1078, 1089-90 ((company providing "electronic information management and data security services for safeguarding" personal identification and health information was not an "entity governed by the CMIA"); *Aguilar v. Hartford Accident & Indemnity Co.* (C.D. Cal. Mar. 13, 2019) 2019 WL 2912861, at *2 (similar).)

Nor is it surprising that no other court has taken such an expansive view of the CMIA. The consequences of broadening section 56.06 to include *any* entity that possesses or stores "medical information"—no matter how fleetingly or indirectly—are staggering. That is especially so considering that "medical information" encompasses "any individually identifiable

information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental health application information, reproductive or sexual health application information, mental or physical condition, or treatment." (Civ. Code, § 56.05(j).)

Begin with the obvious: the internet. Under the Court of Appeal's ruling, hundreds of technology companies are now potentially "providers of health care." Every website, app, or social-media post containing any reference to identifiable information about a person's "mental or physical condition" would suddenly subject its host company to CMIA liability. A comment on social media about persistent headaches; a thread on a video describing weight loss (or gain); a "mommy blog" post about postpartum health—all of these would qualify, as would the many online forums and support communities that provide support for specific health issues from bulimia to multiple sclerosis. Entities would suddenly have responsibility not to allow any such content hosted or published through their platforms. And because the CMIA contains a $1,000-per-person nominal damages provision, that responsibility would quickly translate into massive liability. (Civ Code, § 56.36(b)(1).) The Court of Appeal's decision transforms the internet, where individuals frequently comment on their own (and each other's) "medical information," into a minefield.

And it does not stop there. Any organization that "store[s]" or "possess[es]" information about the "mental or physical

condition" of individuals would find itself subject to CMIA if the reasoning of the Court of Appeal is permitted to stand. (Slip op. at 4; Civ. Code, § 56.05(j).) For instance, summer camps and community sports teams that ask whether participants have injuries or physical needs could find themselves liable under the statute. So would childcare companies that keep notes about children's medical needs. Even caterers, restaurants, and reservation services that request information about food allergies could be covered by the Court of Appeal's definition. All these entities, like Illuminate, store or possess medical data, though not for medical purposes.

The Court of Appeal did not shy away from its desire to "extend" the statute "beyond medical providers," contrary to the text of the statute. (Slip Op. at 1.) Indeed, the court blithely extended CMIA liability to schools without that issue being argued by either party. (*Id.* at 5.) The court reached beyond the pleaded facts to observe that schools "are authorized to hire 'physicians as full-time supervisors of health' and to provide ambulance care. They are required to 'assess' a child's disabilities; to provide medical care at sports events; and to cooperate with local health officials in preventing communicable diseases." (*Ibid.*) And even if they hired no medical personnel and kept no medical records, schools would *still* be liable under the Court of Appeal's rationale simply by retaining photographs of students that revealed the use of eyeglasses, mobility aids, or any other tells about a child's "mental or physical condition." Nothing in the text of the CMIA or any of its legislative history suggests that the Legislature intended

to impose the statute's obligations—and potentially crippling liability—on schools.

The Court of Appeal's overbroad definition of "provider of health care" would make nearly every business in California that touches personal health information, from schools to social media, subject to the CMIA and its potential for massive damages suits. And those companies, faced with such liability, would pass the costs of compliance and litigation on to consumers. Fortunately, the text of the CMIA itself provides the cure. By limiting statutory obligations (and attendant liability) to businesses either "organized for the purpose of maintaining medical information" or offering technology products "designed to maintain medical information," the Legislature wisely broadened the CMIA to include companies that partner with traditional healthcare entities to provide healthcare services (such as healthcare app developers)—and only those companies. The statute's purposive requirement is the key to its scope, and the Court of Appeal erred in abandoning it.

"The rule that a remedial statute is construed broadly does not permit a court to ignore the statute's plain language." (*Even Zohar Constr. & Remodeling, Inc. v. Bellaire Townhouses, LLC* (2015) 61 Cal. 4th 830, 842.) The decision below destabilizes the law; no other court has adopted the Court of Appeal's position. It will also invite exploratory lawsuits against a wide range of companies doing business in California. This Court should thus grant review to realign California law with the text of the CMIA.

B.
The Court Should Grant Review to Ensure the Uniform and Correct Interpretation of the CMIA's Requirements for Alleging a Statutory Violation

The Court of Appeal exacerbated its expansion of the scope of the CMIA by redefining what constitutes a CMIA violation. Ignoring the text of the statute, the court held that a plaintiff may bring a CMIA claim under sections 56.10 and 56.101 without alleging either an "affirmative communicative act" or a breach of confidentiality. (Slip Op. at 7.) This holding contradicts prior Court of Appeal rulings in *Sutter Health v. Superior Court* and *Regents of University of California v. Superior Court* and independently warrants review.

Begin with CMIA section 56.10, which states that a "provider of health care, health care service plan, or contractor *shall not disclose* medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization." (Civ. Code, § 56.10(a).) "Disclosure is not defined in the statute," so California courts have looked to "the context and ordinary meaning" of the CMIA to fill in the gap. (*Sutter Health*, *supra,* 227 Cal.App.4th at p.1555.) They have determined that "disclosure occurs when the health care provider affirmatively shares medical information with another person or entity." (*Id.* at pp.1555-56; *see also Regents*, *supra,* 220 Cal.App.4th at p.564.)) A defendant is not liable under section 56.10 when it "did not intend to disclose the medical information"—for instance, where the information was "stolen by, not given to, [an] unauthorized person," as in the case of a data breach. (*Sutter Health*, *supra,* 227 Cal.App.4th at p.1556.)

Section 56.101, the other basis for plaintiffs' CMIA claim, requires that "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that *preserves the confidentiality of the information* contained therein." (Civ. Code, § 56.101(a).) California courts have held that "more than an allegation of loss of possession" is necessary to show a failure to preserve confidentiality. (*Regents, supra*, 220 Cal.App.4th at p.570.) Instead, "[w]hat is required is pleading, and ultimately proving, that the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence." (*Ibid.*; *see also Sutter Health*, *supra,* 227 Cal.App.4th at p.1557 ("No breach of confidentiality takes place until an unauthorized person views the medical information."); *Vigil v. Muir Med. Grp. IPA, Inc.* (2022) 84 Cal.App.5th 197, 213 ("Based on the statute's plain language, we agree with *Sutter Health* that a breach of confidentiality under the CMIA requires a showing that an unauthorized party viewed the confidential information.").)

The Court of Appeal departed from this settled law when it held that plaintiffs need only plead negligence to establish a full-fledged CMIA violation. It explained that plaintiffs alleged "that there was an agreement to safeguard this information, Illuminate breached it, and it was also negligent," and that those "allegations demonstrate the type of harm the Legislature sought to prevent in

enacting the CMIA." (Slip Op. at 8-9.)[3] Missing from the court's analysis—and plaintiffs' complaint—is any allegation of disclosure (required for a claim under section 56.10) or breach of confidentiality (required for a claim under section 56.101).

The Court of Appeal's departure from the holdings of *Regents* and *Sutter Health*, not to mention the text of the CMIA, was unjustified. *First*, the court failed to address *Sutter Health*'s holding that a claim of unauthorized "disclosure" under section 56.10 requires an "affirmative communicative act." (*Sutter Health*, *supra,* 227 Cal.App.4th at pp.1555-56; *cf.* Slip Op. at 7-9.) As *Regents* explained, "disclose" is "an active verb, denoting in the context of CMIA and the protections afforded confidential medical information *an affirmative act of communication*." (*Regents*, *supra,* 220 Cal.App.4th at p.564.) And in the years since *Regents*, California courts have repeatedly held that the "disclose" language of section 56.10 is not satisfied without such an "affirmative communicative act." (*See, e.g.*, *Sutter Health*, *supra,* 227 Cal.App.4th at p.1555; *Farhood v. StrataCare, LLC* (Cal. Ct. App. Apr. 23, 2019) 2019 WL 1771651, at *4.) Other courts applying California law have followed suit. (*See, e.g.*, *B.K. v. Eisenhower Med. Ctr.* (C.D. Cal. Feb. 29, 2024) ___ F.Supp.3d ___, 2024 WL 878100, at *4; *Lurry v. PharMerica Corp.* (W.D. Ky. June 12, 2024) 2024 WL 2965642, at *12.) Plaintiffs did not and could not plead that Illuminate committed an affirmative act of disclosure. Quite

---

[3] The Court of Appeal also noted plaintiffs' allegation that Illuminate "failed to promptly notify the victims of the data breach for five months," but that allegation is relevant only to the CRA claim, not the CMIA claim. (Slip op. at 8-9.)

the opposite: Illuminate was the victim of a cybercrime. Plaintiffs' data was indisputably "stolen by, not given to, [an] unauthorized person," and so not "disclosed." (*Sutter Health*, *supra,* 227 Cal.App.4th at p.1556.)

Second, the Court of Appeal failed to recognize that a plaintiff must allege a breach of confidentiality to bring a claim under section 56.101. That was the holding of *Regents*, a case in which the plaintiff alleged that an encrypted hard drive containing her confidential medical information was stolen from a physician's home (the physical equivalent of the [redacted] here). (*Regents, supra,* 220 Cal.App.4th at p.570.) Because "no one (except perhaps the thief) kn[ew] what happened to the encrypted external hard drive," the plaintiff did not (and could not) allege that her records were ever viewed by anyone, and her section 56.101 claim was dismissed. *(Ibid.*) Courts have consistently required plaintiffs bringing similar CMIA claims to show actual loss of confidentiality. *See, e.g.*, *Eisenhower Med. Center*, *supra,* 2024 WL 878100, at *4 (dismissing claim where plaintiffs alleged that their data had been "intercepted, viewed[,] analyzed, and used," but provided no factual basis); *Cousin v. Sharp Healthcare* (S.D. Cal. 2023) 681 F. Supp. 3d 1117, 1128-29 (dismissing claim because plaintiffs did "not allege that their medical information was viewed" or provide facts sufficient for such an inference).

Regents is on all fours with this case. Plaintiffs do not plead facts showing, or even suggesting, that the confidentiality of their information was compromised. Although the Court of Appeal hastened to conclude that the alleged delay, standing alone,

"g[a]ve rise to the inference that [plaintiffs'] medical information ha[d] been viewed by an unauthorized third party," no pleaded facts support that inference. (Slip Op. at 9 (quoting *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.* (S.D.Cal 2020) 613 F.Supp.3d 1284, 1299.) In *Solara*, the case relied upon by the court, the plaintiffs alleged not only a delay, but also "medical-related spam emails and phone calls following the data breach"—specific facts that could "plausibly give rise to the inference" that their data had been taken, viewed, and exploited. (613 F.Supp.3d at p.1299.) Here, in contrast, there is no indication of actual misuse of plaintiffs' data—whether affecting these plaintiffs or any others—and it has been more than two and half years since [redacted][4] As in *Regents*, "no one (except perhaps the thief) knows what happened" to plaintiffs' information [redacted], which means that plaintiffs have alleged only a loss of possession. And "[w]hile loss of possession may result in breach of confidentiality, loss of possession does not necessarily result in a breach of confidentiality." (*Sutter Health*, *supra,* 227 Cal.App.4th at p.1557.) The Court of Appeal's holding to the contrary was error.

The opinion below creates a split in California law, and it is decidedly on the wrong side. Unlike *Sutter Health* and *Regents*,

---

[4] While plaintiffs did argue on appeal (though did not allege in the Amended Complaint) that they received an uptick in "spam," they have never explained how any increase in spam indicates that the confidentiality of their *medical* information was compromised—or has anything to do with the incident.

the opinion here jettisoned the disclosure and breach-of-confidentiality requirements found in the plain text of the CMIA. And it circumvented the Legislature's reasoned decision to impose liability only for affirmative acts of disclosure under section 56.10 and for loss of confidentiality under section 56.101—not mere loss of possession. The Court of Appeal's decision unsettles the law defining CMIA violations, and this Court should grant review to restore a uniform and correct interpretation of the statute.

II.
The Court Should Grant Review to Ensure the Uniform and Correct Application of the CRA

The Court of Appeal further disrupted California law with its novel interpretation of the CRA. The Customer Records Act, as its name suggests, imposes obligations on California businesses to maintain and protect customer information. (Civ. Code, §§ 1798.80-1798.83.) For instance, consistent with the "the intent of the Legislature to ensure that personal information about California residents is protected," the CRA requires that businesses properly dispose of customer records and timely notify customers whose data they maintain if that data is breached. (*Id.* §§ 1798.81.5, 1798.81, 1798.82.)

The CRA provides a cause of action to "[a]ny customer injured by a violation" of the statute. (*Id.* § 1798.84.) As California courts have uniformly recognized until now, that provision requires that a plaintiff (1) be a "customer" who has provided personal information to the defendant for the purpose of obtaining a product or service and (2) suffer an injury due to the alleged statutory violation. The Court of Appeal abandoned both

requirements and impermissibly broadened the reach of the CRA, creating a conflict with another decision of Court of Appeal in *Boorstein v. CBS Interactive* (as well as every other court to interpret the statute). This Court should grant review to ensure the uniform and correct application of the CRA.

A.
The Decision of the Court of Appeal Conflicts with Precedent Limiting CRA Claims to "Customers"

The Court of Appeal first expanded the scope of the CRA by allowing claims by plaintiffs who are not "customers" as defined by the statute. In so doing, it departed from established precedent, disregarded statutory text, and created potentially limitless liability for defendants who have no business relationship with potential claimants. This unjustified expansion of the CRA is at odds with every previous interpretation of the statute.

The Legislature made clear that the CRA—the *Customer* Records Act—does not provide a damages remedy for just any plaintiff. It supplies a cause of action only to "[a]ny *customer* injured by a violation of this title." (Civ. Code, § 1798.84(b).) The Legislature further clarified that a customer is "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business." (*Id.* § 1798.84(c).) The intent behind the "customer" requirement could not be clearer: the Legislature sought to create a cause of action under the CRA only for customers who provide their information as part of business transactions.

Every court to interpret the CRA so far has recognized as much. In the leading case of *Boorstein v. CBS Interactive, Inc.*, the

Court of Appeal explained the obvious: "Because the right to institute a civil action arises only under subdivision (b), a plaintiff must meet the terms of that section—*i.e.*, he or she must be a 'customer' who has been 'injured by a violation of this title'—to pursue an action for a violation."[5] (*Boorstein, supra,* 222 Cal.App.4th at p.467.)

Other courts have carefully followed this instruction, holding that a "[p]laintiff must show that he is a 'customer'" of the defendant to state a valid cause of action under the CRA. (*Gamez v. VF Corp.* (C.D. Cal. Nov. 21, 2018) 2018 WL 6333560, at *2; *see also Doe v. MKS Instruments, Inc.* (C.D. Cal. Nov. 3, 2023) 2023 WL 9421115, at *4 (CRA not satisfied when plaintiff is an employee rather than a customer).) And individuals are not "customers" for CRA purposes when they are merely "customers or employees" of another entity that has a business relationship with the defendant—being one step removed is not close enough, because section 1798.84 requires that there must be "allegations that Plaintiffs had paid money to or obtained [a] service from Defendant." (*In re Accellion, Inc. Data Breach Litig.*, *supra,* 2024 WL 333893, at *14.)

Federal courts in other states applying California law have reached similar conclusions. (*See In re Waste Mgmt. Data Breach Litig.* (S.D.N.Y. Feb. 24, 2022) 2022 WL 561734, at *7 (dismissing

---

[5] *Boorstein* and other cases occasionally refer to claims under California's "Shine the Light Law" (Civ. Code, § 1798.83) rather than under the broader Customer Records Act (Civ. Code, § 1798.80 *et seq.*). But the holdings in *Boorstein* and related cases interpret the language of section 1798.84—the same provision at issue here.

CRA claim in part because the complaint did "not allege that the plaintiffs provided their PII to [Defendant] in exchange for a product or service"); *Toretto v. Donnelley Fin. Sols., Inc.* (S.D.N.Y. 2022) 583 F.Supp.3d 570, 603 (same); *Miller v. NextGen Healthcare, Inc.* (N.D. Ga. July 25, 2024) 2024 WL 3543433, at *8 (same).) In short, courts both inside and outside California have been united in holding that "the CRA's plain language clearly applies only to individuals who provide PII to a business in exchange for a product or service." (*Kirsten v. California Pizza Kitchen, Inc.* (C.D. Cal. July 29, 2022) 2022 WL 16894503, at *6.)

The Court of Appeal deviated from this unbroken line of precedent. Without acknowledging the text of the CRA or any of the case law interpreting it, the court erroneously held that plaintiffs could bring a CRA claim simply because they were "intended beneficiar[ies] under the CRA." (Slip Op. at 11.) It then went on to conclude that "the ultimate 'customers,' consumers, and beneficiaries of [Illuminate's] educational services were the students who trusted Illuminate to protect their information"—despite there being no business relationship at all between those students and Illuminate. (*Ibid.*)

That novel reading of the CRA was never argued by plaintiffs, who in fact failed to challenge on appeal the trial court's finding that Illuminate had no duty under the CRA to notify them of the breach. And no wonder: the Court of Appeal's interpretation of section 1798.84 as providing a cause of action to "beneficiaries" rather than "customers" has no legal basis. The Court of Appeal reasoned that the CRA is "remedial and must be interpreted

broadly" to achieve its purpose of protecting information. (Slip Op. at 11.) But a court "may not add to or alter [statutory] words in order to accomplish a purpose that does not appear on the face of the statute or from its legislative history," and the manifest purpose of the CRA is to protect the rights of *customers*. (*People v. Salcido* (2008) 166 Cal.App.4th 1303, 1311.) Nothing in the text or history of the statute creates rights for "beneficiaries" as distinct from the statutory definition of "customer."

The Court of Appeal's reference to "ultimate customers" is similarly ungrounded. The Legislature carefully delineated the reach of the CRA by specifying that only a "customer"—that is, "an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business"—has a cause of action under the statute. (Civ. Code, §§ 1798.80(c), 1798.84(b).) There is no such thing as an "ultimate customer" that fails to meet the CRA's definition of whom it protects. Either a plaintiff has provided personal information to a defendant for the purpose of obtaining a product or service, or not. If not, the CRA does not apply.

The court below did not find, and plaintiffs do not allege, that they meet the definition of "customer" in section 1798.80(c) of the CRA. After all, Illuminate's customers are *schools*, not students. Only by rewriting the statute to include "intended beneficiaries" and "ultimate customers" (both of which the court did not define) could the Court of Appeal find that the CRA applied to Illuminate, contradicting years of consistent holdings that the CRA provides a cause of action only to California *customers*.

The Court of Appeal's decision has perverse consequences. Under the court's new interpretation of the CRA, defendants would face lawsuits brought by individuals with whom they have never conducted business, leading to litigation between virtually unrelated parties. A student could sue a technology company whose products he has never used nor heard of; a patient could sue a biotech company that does business with a hospital she visited a single time; a smartphone owner could sue a data-management company that has a contract with the manufacturer of her phone—all because *someone else* provided their information to those entities, as the school district did here. That is not the scheme the Legislature enacted.

Because the undefined concept of an "ultimate customer" has no connection to the "customers" the CRA itself defines, the Court of Appeal's approach would leave businesses unable to discern their obligations under the statute. Here, for instance, Illuminate notified the school districts that had provided it data in exchange for the use of its products and services. Some of those districts, like Ventura County, asked Illuminate to also notify potentially affected students; others asked it *not* to do so. In that situation, is Illuminate required by California law to notify individuals other than "customers" as defined by the CRA? The Court of Appeal answered "yes"—but gave no hint as to where the obligation to "ultimate customers" runs out. If businesses cannot rely on the limits the legislature enacted in the CRA itself, they cannot know what their legal obligations are until a court decides after the fact.

The CRA "intends to protect California residents in their role [as] customers." (*Corona v. Sony Pictures Ent., Inc.* (C.D. Cal. June 15, 2015) 2015 WL 3916744, at *7.) The statute's title, text, and judicial interpretations have all worked together to support that intention—until now. This Court should grant review to remedy the Court of Appeal's unwarranted expansion of the CRA beyond the "customers" it was meant to protect.

B.
The Decision of the Court of Appeal Conflicts with Precedent Requiring that a Plaintiff Identify an Injury Specific to the Alleged CRA Violation

The Court of Appeal created yet another judicial conflict when it held that plaintiffs need only show a *violation* of the CRA, without showing that they experienced *injury* resulting from the alleged violation. Once again, the court could only do so by ignoring the text of the CRA. And once again, only this Court's review can resolve the conflict among the decisions of the Court of Appeal and clarify the proper interpretation of the CRA moving forward.

Prior to the decision below, California courts uniformly held that "a plaintiff must have suffered a statutory injury to have standing to pursue a cause of action under the [CRA] law." (*Boorstein*, *supra,* 222 Cal.App.4th at p.466.) The injury requirement flows directly from the statutory text: "section 1798.84, subdivision (b) creates a private right of action in any customer 'injured by a violation of this title,'" but in no one else. (*Id.* at pp.466-67 (quoting Civ. Code, § 1798.84(b)).) In other words, the CRA "does not allow a cause of action based solely upon

a failure to comply with the statute. Rather, § 1798.84(b) expressly requires an injury resulting from a violation. Thus, a violation of the statute, without more, is insufficient." (*Id.* at p.467.) The inescapable conclusion is that a plaintiff who cannot identify an injury specific to the CRA violation "lacks statutory standing for his [CRA] claim, regardless of whether his allegations are sufficient to state a violation." (*Ibid.*) The statute is clear: no injury, no standing to bring a claim.

Federal courts applying California law have unanimously accepted this commonsense interpretation of the CRA, noting that "California courts have construed [the CRA's] statutory language to require a plaintiff to show that his or her injury was caused *by a violation of the statute*." (*Gilbert v. Bank of Am.* (N.D. Cal. Sept. 23, 2014) 2014 WL 12644028, at *3; *see also, e.g.*, *Boorstein v. Men's Journal LLC* (C.D. Cal., June 14, 2012) 2012 WL 2152815, at *2 (same); *King v. Conde Nast Publications* (C.D. Cal. Aug. 3, 2012) 2012 WL 3186578, at *3 (citing *Boorstein v. CBS Interactive* and dismissing CRA claim where alleged injury "was not caused by the defendant's alleged [CRA] violation"); *Howell v. Grindr*, *LLC* (S.D. Cal. Dec. 15, 2015) 2015 WL 9008801, at *4 (following California courts to hold that "[a] violation of the statute itself is not enough" because the CRA "requires a showing that the economic injury suffered by [plaintiff] was due to a violation of the statute"); *Antman v. Uber Techs., Inc.* (N.D. Cal. May 10, 2018) 2018 WL 2151231, at *11 (citing Civ. Code, § 1798.84(b)) (holding that "[a]ctual injury is required for [a defendant's] alleged failure to protect [plaintiff] PII" under the CRA); *Miller v. Hearst*

Communications, Inc. (C.D. Cal. Aug. 3, 2012), 2012 WL 3205241, at *5 (dismissing CRA claim because plaintiff had "not pled sufficient facts to show that she was 'injured' by Defendant's alleged violation of § 1798.83(b)(1)"); *Razuki v. Caliber Home Loans, Inc.* (S.D. Cal. Nov. 15, 2018) 2018 WL 6018361, at *2 ("As other courts in this Circuit have recognized, a Plaintiff alleging a violation of 1798.82 must show *that the delay in notification led to incremental harm*, which Plaintiff plainly has not shown here.").)

In a case like this one that arises from an alleged delay in notification, a plaintiff must identify an incremental injury specific to the defendant's alleged delay in notifying the plaintiff—one that goes above and beyond any purported injury arising from the incident itself. "Where Plaintiffs have failed to allege injury arising from a Defendant's 'delayed notification,' courts have dismissed § 1798.82 claims." (*Solara*, *supra,* 613 F.Supp.3d at p.1300; *see also, e.g.*, *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.* (S.D. Cal. Nov. 3, 2016) 2016 WL 6523428 (dismissing CRA claim and explaining that when a "[p]laintiff has failed to allege any injury proximately caused by any violation of" the CRA, she has also "failed to state a cause of action under" that statute).)

Once again, the Court of Appeal charted a path leading away from statutory text and judicial consensus. Here, the alleged CRA violation did not arise from the data breach itself—only from the *delay* in notification. Plaintiffs alleged that Illuminate violated the CRA by waiting too long to notify them of the data breach. (Civ. Code, § 1798.82(b); AA95-97). But the pleaded facts, without

exception, alleged harms (such as "financial and personal losses") from the data breach itself—*not* from the delay that constituted the actual CRA violation. (Slip Op. at 12.) Not a single alleged injury was caused (or even affected) by Illuminate's alleged delay. Yet the Court of Appeal nonetheless held that plaintiffs had stated a viable claim under the CRA simply because plaintiffs "alleged that Illuminate made an unreasonable delay of five months before making the disclosure about the data breach," and the "CRA require[d] a prompt disclosure of the data breach." (Slip Op. at 11.) That holding, in direct contradiction to *Boorstein*, inserted into the CRA "a cause of action based solely upon a failure to comply with the statute." (*Boorstein*, *supra,* 222 Cal.App.4th at p.467.)

The Court of Appeal's justification for discarding the text of the CRA is unavailing. The court reasoned that Illuminate's delay prevented plaintiffs from "taking prompt steps to protect their personal information" (for instance, from identity theft), and so created a "credible threat of immediate harm." (Slip Op.at 11-12.) But once again, the court conflated harm from the *data breach* with harm from the *delay*. None of the harms alleged by plaintiffs stemmed from Illuminate's alleged delay—only from the cyberattack itself. And critically, plaintiffs have alleged no facts suggesting that they suffered identity theft, much less identity theft that could have been prevented but for Illuminate's CRA violation. The Court of Appeal allowed the CRA claim to move forward even though Illuminate's alleged delay inflicted no injury on plaintiffs.

The Court of Appeal's break with *Boorstein*—and with the holding of every other court to consider the question—undermines a key requirement that the Legislature added to the enforcement provision of the CRA. The statutory text explicitly states that the CRA provides relief only to plaintiffs *injured by a violation* of the statute. It is not intended to provide damages where there is nothing to make whole. The harm alleged by plaintiffs in this case stems only from the loss of personal data, not from any delay on Illuminate's part in reporting that loss. By nevertheless allowing a CRA claim to proceed, the Court of Appeal has effectively written section 1798.84(b) out of the CRA.

"[T]o have standing under the [CRA], a plaintiff must suffer an injury caused by a violation of the statute." (*Boorstein*, *supra,* 222 Cal.App.4th at p.467.) The Court of Appeal wrongly dispensed with this statutory standing requirement and unsettled California law. This Court should grant review to correct that error and restore a uniform interpretation of the CRA.

CONCLUSION

The Court should grant review.

DATED: September 3, 2024

Respectfully submitted,

KIRKLAND & ELLIS LLP

/s/ Tammy A. Tsoumas

Tammy A. Tsoumas (SBN 250487)
tammy.tsoumas@kirkland.com
KIRKLAND & ELLIS LLP
2049 Century Park East, Suite 3700
Los Angeles, CA 90067
Telephone: (310) 552-4334

Devin S. Anderson (*pro hac vice* pending)
devin.anderson@kirkland.com
Cynthia D. Love
cynthia.love@kirkland.com
KIRKLAND & ELLIS LLP
95 S. State Street
Salt Lake City, UT 84111
Telephone: (801) 877-8115

Attorneys for Defendant and Petitioner Illuminate Education, Inc.

CERTIFICATE OF WORD COUNT

I, Tammy A. Tsoumas, hereby certify that in accordance with the Rules of Court, Rule 8.504(d)(1), I employed the word count feature of Microsoft Word to verify that the number of words contained in this brief, excluding materials excepted under Rule 8.504(d)(3), but including footnotes, is 8,331 words.

Dated: September 3, 2024

/s/ Tammy A. Tsoumas
Tammy A. Tsoumas
KIRKLAND & ELLIS LLP

Attorneys for Defendant and Petitioner Illuminate Education, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on September 3, 2024, I electronically filed the foregoing document titled PETITION FOR REVIEW through the Court's electronic filing system.

Furthermore, a copy of the PETITION FOR REVIEW was mailed to the interested parties below:

Mark D. Potter
James M. Treglio
Potter Handy, LLP
100 Pine Street, Suite 1250
San Francisco, CA 94111

Attorneys for Plaintiff and Appellant Jean Paul Magallanes, guardian ad litem for Jacob Magallanes

COURT OF APPEAL
Sixth Appellate District
333 W. Santa Clara Street,
Suite 1060
San Jose, CA 95113

Hon. Benjamin F. Coats,
Ventura County Superior Court
Department 43
P.O. Box 6489
Ventura, California 93006-6489

By: */s/ Tammy A. Tsoumas*
Tammy A. Tsoumas
KIRKLAND & ELLIS LLP

Attorneys for Defendant and Petitioner Illuminate Education, Inc.

EXHIBIT A

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION SIX

J.M., a Minor, etc.,

Plaintiff and Appellant,

v.

ILLUMINATE EDUCATION, INC.,

Defendant and Respondent.

2d Civ. No. B327683
(Super. Ct. No. 56-2022-00567324-CU-MC-VTA)
(Ventura County)

The Confidentiality of Medical Information Act (CMIA) protects confidential medical information. Here we decide its reach extends beyond medical providers.

J.M., a minor, by his guardian ad litem Jean Paul Magallanes, appeals a judgment of dismissal following the sustaining of a demurrer without leave to amend on his class action lawsuit against defendant Illuminate Education, Inc. (Illuminate). He claims Illuminate violated the CMIA (Civ. Code,[1] § 56 et seq.) and the Customer Records Act (CRA) (§ 1798.80 et seq.).

[1] All statutory references are to the Civil Code unless otherwise stated.

We conclude, among other things, that: 1) Illuminate falls within the scope of the CMIA and CRA; 2) J.M. stated sufficient facts to state causes of action under the CMIA and CRA; and 3) the trial court abused its discretion by sustaining the demurrer without leave to amend. We reverse and remand. J.M. may file an amended complaint in which he alleges additional facts.

FACTS

J.M., an 11-year-old student, filed a class action lawsuit by his guardian ad litem Jean Paul Magallanes, against Illuminate, an education consulting business. He alleged Illuminate obtained possession of his personal and medical information from his school and its office of education so that it could assist the school and evaluate his educational progress at the school. Illuminate promised to maintain that information confidentially, but it negligently maintained its database. Because of a data breach, a cyber hacker gained access to that personal information.

Illuminate did not promptly notify J.M. and other victims about the breach. It provided specific notice about the breach involving his personal information five months after the breach. After the data breach, J.M. started receiving "solicitations by mail from third parties" that were sent to "an address [J.M.] only provided to [Illuminate] through the Office of Education."

J.M. alleged Illuminate's negligence in maintaining its database and its delayed disclosure of the breach constituted violations of the CMIA and CRA (§§ 56 et seq., 1798.80 et seq.), and he sought damages and injunctive relief.

Illuminate demurred claiming it did not fall within the CMIA or CRA and J.M. failed to state a cause of action.

The trial court sustained the demurrer. J.M. filed a proposed second amended complaint stating more facts about Illuminate and the harm caused by the delayed notification of the data breach. He filed a motion for reconsideration.

The trial court reviewed J.M.'s amended pleadings and concluded that he had not stated a cause of action and he could not amend to state a cause of action. It sustained the demurrer without leave to amend and entered judgment for Illuminate.

DISCUSSION

"A demurrer tests the sufficiency of the plaintiff's complaint, i.e., whether it states facts sufficient to constitute a cause of action upon which relief may be granted." (*Seidler v. Municipal Court* (1993) 12 Cal.App.4th 1229, 1233.) "A demurrer should not be sustained without leave to amend if the complaint states a cause of action under any theory or if there is a reasonable possibility the defect can be cured by amendment." (*Ibid*.) The allegations of a pleading must be "liberally construed, with a view to substantial justice between the parties." (Code Civ. Proc., § 452; *American Telephone & Telegraph Co. v. California Bank* (1943) 59 Cal.App.2d 46, 53.)

Does Illuminate Fall Within the Scope of the CMIA?

J.M. alleged facts showing that Illuminate is an entity that falls within the scope of the CMIA. The CMIA "prohibits health care providers and *related entities* from disclosing medical information regarding a patient without authorization except in certain specified instances." (*Regents of the University of California v. Superior Court* (2013) 220 Cal.App.4th 549, 553 (*Regents of University*), italics added.) A plaintiff may bring an action for damages against an entity that "negligently released

confidential medical information concerning him or her in violation of CMIA." (*Ibid*.)

The CMIA broadly applies to the entities that possess or store confidential medical information, including providers of health care, health care service plans, and contractors. (§ 56.10, subd. (a).) It also applies to "[a]ny business organized *for the purpose of maintaining medical information* in order to make the information available to an individual or a provider of health care" or "for the diagnosis and treatment of the individual." (§ 56.06, subd. (a).) Such a business "shall be deemed to be a provider of health care subject to the requirements" of the CMIA. (*Ibid*.) This includes businesses that supply "software or hardware" to "maintain medical information." (*Id.*, subd. (b).) The inclusion of the broad scope of entities that maintain this information is to (1) protect this information, and (2) require those who have it to act "in a manner that preserves the confidentiality of that information." (*Regents of University*, *supra*, 220 Cal.App.4th at p. 553.)

J.M. alleged that Illuminate is an "education company" that provides "support" for school districts by maintaining student medical records on its "computer network." Illuminate monitors the progress of students K-12 and their "social-emotional behavior." Its services are provided to meet " 'the unique needs of students who require additional supports in order to succeed.' " To perform its functions, Illuminate uses student medical information and "the diagnosis and treatment plans of children" to "diagnose students' needs" and monitor their progress. Illuminate obtained J.M.'s medical records with the understanding that it would maintain them confidentially in its services to evaluate his educational performance. J.M. alleged

that because of its storage and use of confidential medical records to perform its services, Illuminate falls within the scope of the CMIA.

In a proposed second amended complaint, J.M. alleged Illuminate "primarily works with school districts to provide assistance with special education and *mental health services*" and it maintains "mental health records of children." (Italics added.) Illuminate's system is "licensed to 5,000 schools nationally and has a total enrollment of approximately 17 million students."

School districts maintain student medical records for a variety of reasons. They are authorized to hire "physicians as full-time supervisors of health" and to provide ambulance care. (Ed. Code, §§ 49472, 49474.) They are required to "assess" a child's disabilities (*D.O. ex rel. Walker v. Escondido Union School Dist*. (9th Cir. 2023) 59 F.4th 394, 405); to provide medical care at sports events (*Brown v. El Dorado Union High School Dist*. (2022) 76 Cal.App.5th 1003, 1032); and to cooperate with local health officials in preventing communicable diseases. (*Let Them Choose v. San Diego Unified School Dist*. (2022) 85 Cal.App.5th 693, 708.) When school districts share this medical information with entities such as Illuminate that has a large database, the CMIA's confidentiality provisions are necessarily triggered.

Illuminate contends the CMIA does not apply to it because it is not involved in health care. J.M. alleges that Illuminate provides assistance to school districts by evaluating students with "social-emotional behavior" issues by using their medical records. Illuminate assists schools' mental health services and maintains children's mental health records. The statute includes entities that maintain medical records for the "diagnosis and treatment" of the individual. (§ 56.06, subd (a).) J.M. alleges

Illuminate is diagnosing the educational progress of children with learning disabilities and mental health issues based on their medical records.

Illuminate argues it is not covered by the CMIA's definition of a "provider of health care," a "health care service plan," or a "contractor." (§ 56.10, subd. (a).) A "contractor" is defined as a medical group, an independent practice association, pharmaceutical benefits manager, or a medical service organization. (§ 56.05, subd. (d).)

The Legislature did not confine the CMIA's scope to these medical groups. In 2013 it amended the statute to expand the definition of a "provider of health care" to include "any business" that maintains medical information used "for the diagnosis" of an individual (§ 56.06, subds. (a) & (b)), or that provides "software or hardware" for that purpose (*id.*, subd. (b)). This "amendment was intended to ensure that the CMIA would apply to all [personal health record] vendors that maintain medical information . . . whether or not the business was organized for that purpose." (Tiffany II et al., *The Doctor Is In, But Your Medical Information Is Out Trends In California Privacy Cases Relating to Release of Medical Information* (2015) 24, No. 1 Cal. State Bar J. 206, 225; see also Legis. Counsel's Dig., Assem. Bill No. 658 (2013-2014 Reg. Sess.) 7 Stats. 2013, pp. 2611-2612.) The CMIA also applies to "[a] recipient of medical information" (§ 56.13) and to a "provider of health care, health care service plan, pharmaceutical company, contractor, *or any other entity*" that seeks an authorization for "disclosure of protected health information." (§ 56.11, subd. (c), italics added.)

The CMIA is a remedial statute. "Remedial and protective statutes will be liberally interpreted to advance their clear

purposes." (*Fitch v. Pacific Fidelity Life Ins. Co.* (1975) 54 Cal.App.3d 140, 148.) Consistent with this broad scope of coverage, Illuminate falls within the definitions of "any other entity" in section 56.11, subdivision (c); a "recipient of medical information" under section 56.13; and "any business" under section 56.06, subdivisions (a) and (b). J.M. alleged Illuminate possessed the medical information with the understanding that it would safeguard its confidentiality, thus making it a "recipient of medical information."

"Statutes should be given a construction consistent with the legislative purpose . . . ." (*Silberman v. Swoap* (1975) 50 Cal.App.3d 568, 571.) The CMIA's purpose is to protect the confidentiality of medical records. (*Regents of University*, *supra*, 220 Cal.App.4th at p. 553.) Illuminate's position eliminates that protection for school children. Such a result undermines the purpose of the CMIA.

Did J.M. Allege a CMIA Cause of Action?

The CMIA statute requires "pleading and proof that confidential information has been released in violation of CMIA to bring a private cause of action." (*Regents of University*, *supra*, 220 Cal.App.4th at p. 564.) But such a cause of action does not require proof of "an affirmative communicative act" by the entity that has stored the medical information. (*Regents of University*, at p. 564.) Instead, such an entity may be liable for "negligently" releasing or disclosing that information. (*Id.* at p. 553.) The Legislature mandates that those maintaining confidential medical records must "implement appropriate administrative, technical and physical safeguards to protect the privacy of a patient's medical information and to safeguard it from 'any unauthorized access or unlawful access, use, or disclosure.' " (*Id.*

at p. 568.) It thus "created" a "private cause of action for negligent maintenance or disposal of confidential medical information." (*Ibid*.)

J.M. alleged the medical information was obtained by Illuminate with the understanding that Illuminate would safeguard it. Illuminate promised to "deploy meaningful safeguards to protect" this information. Illuminate thereafter "failed to adequately safeguard Plaintiff's and Class members' . . . Medical information." It did not monitor external e-mails and identify "e-mail [borne] threats and defend against them." It failed to install systems to "detect a breach" of its data. It used an online data system that was easy for hackers to penetrate. It failed to encrypt the information.

In June 2022, Illuminate notified J.M. and others that a data breach subjected their private information to "unauthorized access," and the information taken may have contained "medical information." Illuminate delayed providing notice of this breach for five months because this breach occurred in December 2021 and January 2022. As a result, J.M. alleged he is subject to an immediate "risk of harm." He alleged the personal information "was not encrypted" and it is "in the hands of cyber criminals." The data breach "has already begun to [cause] . . . financial and personal losses to [the victims]." Illuminate's delayed notification of the data breach permitted cyber thieves to trade their private information on the black market.

These allegations are sufficient to state a cause of action under the CMIA. (*Regents of University*, *supra*, 220 Cal.App.4th at p. 568.) The Legislature intended to create a cause of action for "negligent storage" leading to the "unauthorized 'access' " of medical information. (*Ibid*.) Here there is an allegation that

there was an agreement to safeguard this information, Illuminate breached it, and it was also negligent. It also failed to promptly notify the victims of the data breach for five months.

The allegations demonstrate the type of harm the Legislature sought to prevent in enacting the CMIA–negligence causing a data breach that exposed confidential information to cyber hackers. (*Regents of University*, *supra*, 220 Cal.App.4th at pp. 553, 568.) They support "a credible threat of real and immediate harm" as a result of the data breach. (*Krottner v. Starbucks Corp.* (9th Cir. 2010) 628 F.3d 1139, 1143.) "[T]he risk that Plaintiffs' personal data will be misused by the hackers who breached [the data system] is immediate and very real." (*In re Adobe Systems , Inc. Privacy Litigation* (N.D.Cal. 2014) 66 F.Supp.3d 1197, 1214.) The allegations of future harm in the complaint are sufficient to show "injury-in-fact" and support a cause of action for the data breach. (*Id*. at p. 1216.)

The allegations concerning Illuminate's late notice of the personal information data breach "give rise to the inference that [plaintiff's] medical information has been viewed by an unauthorized third party." (*In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation* (S.D.Cal. 2020) 613 F.Supp.3d 1284, 1299 (*Solara Medical Supplies*).) Allegations that a plaintiff has received increased spam after the data breach also supports such an "inference." (*Ibid*.)

Denying Leave to Amend

In his proposed second amended complaint, J.M. alleged additional facts showing Illuminate's use of medical records to diagnose children's disabilities that impact their educational progress. He alleged his personal information was stolen and "actually viewed" by others because of Illuminate's negligence;

and after the breach, he has been receiving "numerous phone calls from solicitors regarding phantom Amazon accounts and other odd phone calls." He has received numerous mail solicitations "from third parties" that were sent to "an address [J.M.] only provided to [Illuminate] through the Office of Education." Illuminate told J.M. and others to monitor their credit reports in response to the data breach.

We " 'accept as true not only those facts alleged in the complaint but also facts that may be implied or inferred from those expressly alleged.' " (*Munoz v. Patel* (2022) 81 Cal.App.5th 761, 771.) Because the facts he alleged supported a cause of action for damages (*Regents of University, supra*, 220 Cal.App.4th at pp. 553, 564, 568; *Huynh v. Quora, Inc.* (N.D.Cal. 2020) 508 F.Supp.3d 633, 650 [time spent on credit monitoring may constitute "cognizable harm" for damages]), the trial court erred by denying J.M. leave to file his proposed second amended complaint. (*Munoz*, at p. 771.)

Did J.M. State a Cause of Action Under the CRA?

The CRA provides protection for customers who do business with entities that maintain their personal information. The CRA " 'regulates businesses with regard to treatment and notification procedures relating to their customers' personal information.' " (*Solara Medical Supplies*, *supra*, 613 F.Supp.3d at p. 1300.) The CRA authorizes a private cause of action against businesses that violate the disclosure provisions of the statute. (*Ibid.*)

Section 1798.82, subdivision (a) provides, in relevant part, that a business that "owns or licenses computerized data that includes personal information, *shall disclose a breach of the security of the system* following discovery or notification of the breach in the security of the data to a resident of California (1)

whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (§ 1798.82, subd. (a), italics added.) "The disclosure shall be made in the most *expedient time possible and without unreasonable delay* . . . ." (*Ibid.*, italics added.)

"It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information." (§ 1798.81.5, subd. (a)(1).)

Because J.M. alleged his confidential personal information was provided to Illuminate to evaluate his educational progress, and because that information was subject to the data breach, he was an intended beneficiary under the CRA. (§ 1798.81.5, subd. (a)(1); *Solara Medical Supplies*, *supra*, 613 F.Supp.3d at p. 1300.) This statute is remedial and must be interpreted broadly. A narrow interpretation that leaves a statutory beneficiary without protection undermines the statutory intent. (*Silberman v. Swoap, supra*, 50 Cal.App.3d at p. 571.) Illuminate had a contract with the school district. But the ultimate "customers," consumers, and beneficiaries of its educational services were the students who trusted Illuminate to protect their information.

J.M. alleged Illuminate made an unreasonable delay of five months before making the disclosure about the data breach. CRA requires a prompt disclosure of the data breach. A five-month disclosure delay supports a cause of action under the CRA because such a delay prevents victims from taking prompt steps to protect their personal information. (*Solara Medical Supplies*, *supra*, 613 F.Supp.3d at p. 1300.) This resulted in a "credible

threat" of "immediate harm" to the plaintiff. (*Krottner v. Starbucks Corp.*, *supra*, 628 F.3d at p. 1143.) The facts pled about the delayed disclosure support "injury-in-fact." (*In re Adobe Systems, Inc. Privacy Litigation*, *supra*, 66 F.Supp.3d at pp. 1214, 1216.) A delay of even three months in notifying victims has been held to be sufficient to state a cause of action for damages under the CRA. (*In re Ambry Genetics Data Breach Litigation* (C.D.Cal. 2021) 567 F.Supp.3d 1130, 1150.)

Moreover, J.M. pled facts showing current harm to himself and others. He pled the data breach "has already begun to [cause] . . . financial and personal losses," and the delayed notification has allowed cyber thieves to trade their personal information on the black market. In his proposed second amended complaint, he alleged his personal information was stolen and "actually viewed" by others. He pled he has been receiving "numerous phone calls from solicitors regarding phantom Amazon accounts and other odd phone calls." Because we are at the demurrer stage, we must " 'accept as true' " those allegations. (*Munoz v. Patel*, *supra*, 81 Cal.App.5th at p. 771.)

Illuminate's remaining contentions do not change the result we have reached.

DISPOSITION

The judgment of dismissal and the order sustaining the demurrer are reversed. The case is remanded to the trial court for further proceedings. Costs on appeal are awarded in favor of appellant.

CERTIFIED FOR PUBLICATION.

GILBERT, P. J.

We concur:

BALTODANO, J.

CODY, J.

Benjamin F. Coats, Judge

Superior Court County of Ventura

Potter Handy, Mark D. Potter, and James M. Treglio for Plaintiff and Appellant.

Kirkland & Ellis, Devin S. Anderson, Cynthia Love and David R. Williams for Defendant and Respondent.