Filed 7/25/24

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.