Filed 9/16/22

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION FOUR

APRIL KAY MOORE, et al., Plaintiffs and Appellants, v. CENTRELAKE MEDICAL GROUP, INC., Defendant and Respondent.	B310859 (Los Angeles County Super. Ct. No. 19STCV19196)

APPEAL from a judgment of the Superior Court of Los Angeles County, Kenneth R. Freeman, Judge. Affirmed in part and reversed in part.

Wilshire Law Firm, Bobby Saadian, Justin F. Marquez, Thiago M. Coelho, Robert J. Dart and Jessica Behmanesh for Plaintiffs and Appellants.

Baker & Hostetler, Paul Karlsgodt, Matthew D. Pearson and Teresa C. Chow for Defendant and Respondent.

INTRODUCTION

Appellants April Kay Moore, Kimberly Joy, and Yvette McKinley are patients at medical facilities operated by respondent Centrelake Medical Group. In reliance on Centrelake's allegedly false representations that it employed reasonable safeguards for patients' personal identifying information (PII), appellants entered into contracts with Centrelake. Their contracts allegedly incorporated a privacy policy, in which Centrelake promised to maintain adequate data security practices to protect appellants' PII from unauthorized access by third parties. In early 2019, Centrelake suffered a data breach, in which appellants' PII was allegedly stolen by hackers and disseminated into the public domain. In April 2019, Centrelake issued a notice of the data breach, acknowledging that patient records and data might have been taken, and encouraging patients to protect themselves from identity theft or fraud, including by monitoring their credit and financial accounts. Appellants spent time on such monitoring, and appellant McKinley purchased credit and identity monitoring services.

In June 2019, appellants brought this action against Centrelake on behalf of themselves and a putative class of patients affected by the data breach. The complaint contained causes of action for breach of contract, negligence, and violations of the Unfair Competition Law (UCL), Business and Professions Code section 17200 et seq. Appellants alleged they suffered several injuries as a result of Centrelake's failure to maintain adequate data security, including: (1) overpayments for Centrelake's services, which did not include the adequate data security for which they had bargained; (2) time and money spent on credit monitoring and other measures to mitigate risks posed by the data breach; and (3) deprivation of some portion of the value of their PII.

Centrelake demurred, arguing that appellants had failed to adequately plead any cognizable injury, and that their negligence claim was barred by the economic loss rule. Appellants opposed the demurrer. In a footnote to their opposition brief, and at the hearing on the demurrer, appellants requested leave to amend their complaint to add allegations of future harm, viz., future costs to be incurred retaking medical tests in order to replace medical records that had been lost in the data breach. The trial court sustained the demurrer to all claims without leave to amend, concluding: (1) appellants had failed to adequately plead any injury sufficient to support either (a) standing to bring their UCL claim, or (b) the damages elements of their contract and negligence claims; and (2) appellants' negligence claim

was barred by the economic loss rule. The court entered a judgment dismissing all claims.

On appeal, appellants contend the court erred in sustaining the demurrer with respect to each of their claims, and abused its discretion in denying their request for leave to amend. We conclude appellants adequately alleged UCL standing and contract damages under their benefit-of-the-bargain theory, and appellant McKinley, who purchased monitoring services, did the same under appellants' monitoring-costs theory. However, appellants have not shown the court erred in dismissing their negligence claim under the economic loss rule; nor have they shown the court abused its discretion in denying their request for leave to amend. Accordingly, we affirm the judgment with respect to the dismissal of appellants' negligence claim without leave to amend, but reverse with respect to appellants' UCL and contract claims. For guidance on remand, we address appellants' lost-value-of-PII theory, and conclude they failed to adequately plead it as a basis for either UCL standing or contract damages.

PROCEEDINGS BELOW

A. Appellants' Complaint

In June 2019, appellants filed the complaint in this action on behalf of themselves and a putative class of all California residents whose PII was compromised as a result of Centrelake's early 2019 data breach. The facts stated in this subsection are taken from the complaint's factual

allegations, which we presume to be true for purposes of reviewing the trial court's ruling on Centrelake's demurrer.

1. The Data Breach

Centrelake is a medical provider operating eight medical facilities in southern California. Prior to January 9, 2019, appellants became patients of Centrelake. Centrelake "made repeated promises and representations" to appellants "that it would protect its patients' PII from disclosure to unauthorized third parties." Each appellant signed a contract with Centrelake that incorporated a contractually binding privacy policy, viz., Centrelake's Notice of Privacy Practices (attached to the complaint as an exhibit), in which Centrelake promised to take appropriate steps to attempt to safeguard any medical or other personal information provided to it. Centrelake also published its Notice of Privacy Practices to the public on its website. However, the Notice of Privacy Practices contained false statements concerning data security.

Centrelake failed to implement reasonable security practices to protect appellants' PII. As a result, from January 9 to February 19, 2019, Centrelake suffered a data breach, during which appellants' PII was "stolen" (in other words, "acquired" or "harvested") by hackers, and "disseminat[ed] into the public domain." The stolen PII included contact information (names, addresses, and phone numbers), Social Security numbers, driver's license information, and medical information (services performed,

diagnosis information, health insurance information, referring provider information, medical record number, and dates of service).

In April 2019, Centrelake issued a Notice of Data Breach (attached to the complaint as an exhibit). The Notice stated that "suspicious activity" began on Centrelake's network on January 9, 2019 and continued for over a month until, on February 19, Centrelake discovered that a hacker had infected Centrelake's system with a virus that prohibited its access to its files. Centrelake announced that its ongoing investigation had yet to uncover any evidence that the hacker viewed or took patient information, or any indication that such information had been misused. However, Centrelake acknowledged that the hacker might have gained access to patient records and data. Centrelake encouraged affected individuals to "remain vigilant against incidents of identity theft and fraud" by regularly reviewing their credit reports, financial account statements, and explanations of benefits for suspicious activity. Centrelake provided a toll-free phone line staffed with individuals familiar with the data breach, and invited calls from patients with questions regarding how to protect themselves from "potential harm resulting from this incident," including how to place fraud alerts on the patients' credit files.

2. Causes of Action

Appellants' first and second causes of action were for breach of contract and breach of the covenant of good faith

and fair dealing (contract claims).[1] Appellants alleged Centrelake breached its contracts with them by (1) failing to "implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure"; and (2) failing to prevent unauthorized third parties from obtaining such access.

Appellants' third and fourth causes of action were for "negligence per se" and negligence.[2] Appellants alleged: (1) Centrelake entered into a "'special relationship'" with appellants "when [Centrelake] contracted with [them] for medical services and obtained their PII from them"; (2) Centrelake owed appellants a duty of care in protecting their PII, because inadequate data security practices would foreseeably cause them harm; and (3) Centrelake breached that duty by adopting inadequate safeguards to protect their PII.

---

[1] The parties and the trial court analyzed the contract claims together. (See *Sheen v. Wells Fargo Bank, N.A.* (2022) 12 Cal.5th 905, 929 (*Sheen*) ["'The remedy for breach of [the implied] covenant [of good faith and fair dealing] is generally limited to contract damages'"].) We do the same.

[2] Appellants expressly do not challenge the trial court's conclusion that their purported cause of action for negligence per se failed to state a claim, as negligence per se is not an independent cause of action, but rather an evidentiary doctrine applied in negligence actions. We need not further address the negligence per se claim.

Appellants' fifth and final cause of action was for violations of the UCL. Appellants alleged Centrelake violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. § 1320d et seq.) and the public policy expressed therein, rendering its business practices both unlawful and unfair, by (1) failing to "implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure"; and (2) failing to prevent unauthorized third parties from obtaining such access. Appellants further alleged Centrelake's business practices were fraudulent "because they involved representations to the public which [we]re likely to deceive," including false statements concerning data security in its Notice of Privacy Practices.

Appellants sought compensatory damages, restitution, and injunctive relief requiring Centrelake to implement reasonable data security practices.

3. Alleged Injuries

Appellants alleged they suffered several injuries. First, appellants alleged they overpaid for Centrelake's medical services, in that they paid for but did not receive reasonable and adequate security for their PII. In other words, appellants "paid more for [Centrelake]'s services than they [otherwise] would have paid" had they known their PII would not be protected. Relatedly, appellants "relied on [Centrelake]'s [privacy] representations in entering into

contracts with Defendants for medical services, which they would not have entered had they known their PII would be unprotected."

Second, appellants alleged they suffered "[a]scertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach." As a result of Centrelake's failure to implement adequate data security, the data breach placed appellants at risk of suffering identity theft and fraud, and they were "forced to adopt costly and time-consuming preventive and remediating efforts." All appellants were required to spend time, inter alia, monitoring their credit reports and accounts for unauthorized activity. In addition, appellant McKinley purchased credit and personal identity monitoring services, as a "reasonable and necessary" prophylactic measure. Although appellants Moore and Joy had not made such purchases, they would be forced to do so in the future.

Finally, appellants alleged they suffered "[a]scertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market." In general terms, appellants alleged that hackers and other criminals value stolen PII, and that some legitimate businesses pay users for PII. Appellants did not allege they ever had received payment for their PII, or expected to do so in the future.

B. Centrelake's Demurrer

In August 2020, Centrelake demurred to the complaint. It challenged each of appellants' causes of action on the ground that appellants failed to allege any cognizable injury.[3] With respect to appellants' allegations that they overpaid for Centrelake's services in reliance on its representations concerning data security, Centrelake argued this benefit-of-the-bargain theory was too "'flimsy'" to establish cognizable injury, as appellants paid for and received medical services, which they did not allege were deficient. Further, Centrelake challenged appellants' reliance on costs incurred in monitoring their credit, arguing their monitoring-costs theory was deficient because (1) mere time spent monitoring credit was not cognizable; (2) appellants Moore and Joy had not purchased monitoring

---

[3] Neither in the trial court nor in its appellate brief did Centrelake contend that appellants failed to adequately plead the existence of enforceable contracts incorporating its Notice of Privacy Practices. At oral argument, Centrelake argued for the first time that appellants failed to adequately plead consideration for such contracts, because Centrelake was required to issue its Notice of Privacy Practices under HIPAA and one of its implementing regulations (45 C.F.R. § 164.520). Centrelake has forfeited this untimely argument. (See *In re I.C.* (2018) 4 Cal.5th 869, 888, fn. 5 [respondent forfeited argument raised for first time at oral argument "by failing to raise it in a timely manner"]; *J & A Mash & Barrel, LLC v. Superior Court of Fresno County* (2022) 74 Cal.App.5th 1, 32, fn. 9 [""[C]ontentions raised for the first time at oral argument are disfavored and may be rejected solely on the ground of their untimeliness""].)

services, instead merely alleging they expected to do so in the future; and (3) although appellant McKinley had purchased monitoring services, her purchase was prompted by mere risks of identity theft and fraud, not by any actual occurrence of such crimes. Finally, Centrelake argued appellants' theory that the data breach diminished the value of their PII was insufficient to establish cognizable harm, because appellants did not allege they ever intended to sell their PII or were foreclosed from using it in a value-for-value transaction.

Centrelake challenged appellants' negligence cause of action on the additional ground that it was barred by the economic loss rule, which generally bars recovery in negligence for purely economic losses, meaning financial harm unaccompanied by personal injury or property damage. (See *Sheen*, *supra*, 12 Cal.5th at 922.) Anticipating appellants' contention that the rule did not apply because the parties entered into a special relationship, Centrelake argued this special-relationship exception was inapplicable because, inter alia, appellants alleged their relationship with Centrelake was contractual.

In September 2020, appellants opposed the demurrer. Appellants argued they had adequately pled cognizable injuries under benefit-of-the-bargain, monitoring-costs, and lost-value-of-PII theories. Appellants further argued the economic loss rule did not bar their negligence claim because (1) the parties entered into a special relationship; (2) appellants' time spent monitoring their credit and

identities was a *non*-economic loss; and (3) independent of the parties' contracts, Centrelake had a duty under HIPAA to protect appellants' PII.[4] In a footnote, appellants referenced purported allegations (not included in their complaint) that they "lost access to medical records due to the encryption of their data," and added: "To the extent that the Court finds that this theory is not adequately alleged in the Complaint, Plaintiffs respectfully request leave to amend."

In reply, Centrelake generally repeated the arguments in its initial brief. In addition, Centrelake argued appellants alleged no facts to "support the proposition" that their PII was taken by the hackers. Centrelake asserted: "[This case] is not even a data-breach case. It is a ransomware-attack case where criminals unlawfully encrypted Centrelake's data and refused to de-encrypt it absent a fee."

---

[4] Appellants also argued Centrelake had an independent duty under Civil Code section 1798.81.5 and the Federal Trade Commission Act (15 U.S.C. § 41 et seq.). On appeal, appellants do not mention either statute, instead relying solely on HIPAA. We note that where HIPAA applies, Civil Code section 1798.81.5 does not. (See Civ. Code, § 1798.81.5, subd. (e)(3) ["The provisions of this section do not apply to . . . [a] covered entity governed by the medical privacy and security rules issued . . . pursuant to [HIPAA]"].)

C. Hearing and Ruling

In October 2020, the trial court held a hearing on Centrelake's demurrer. Centrelake argued appellants' lost-value-of-PII and benefit-of-the-bargain theories were insufficient to plead cognizable injury. In support of these arguments, Centrelake asserted the complaint did not allege the hackers obtained patients' PII, as opposed to merely encrypting it. In response, appellants observed their complaint did, in fact, allege the hackers obtained their PII, and argued the court was required to accept this allegation as true in ruling on Centrelake's demurrer. Appellants' counsel also elaborated on their request for leave to amend: "[A]fter the complaint was filed, we found out that the plaintiffs no longer had access to their records. So that means that in the future they will have to have those same tests done again and they will have to pay for it. That future harm is the cost of the additional records for [*sic*] which they lost. [¶] So we ask simply for leave to amend as to the future risk of harm . . . ." The court took the matter under submission.

In November 2020, the court issued an order sustaining Centrelake's demurrer to all appellants' claims without leave to amend.[5] The court concluded appellants failed to adequately plead a loss of money or property, as

---

[5] The court did not address appellants' request for leave to amend their complaint to add allegations concerning a future need to retake medical tests.

required to establish standing to bring their UCL claim, or cognizable damages, as required to state their contract and negligence claims. Appearing to accept Centrelake's characterization of the complaint as alleging mere encryption of PII in a ransomware attack, the court stated the complaint contained "no allegation that the security breach has, in fact, resulted in a dissemination of the PII." Relying on this characterization, the court deemed appellants' benefit-of-the-bargain theory insufficient: "Plaintiffs allege only that there was a security breach stemming from the Ransomware Attack. Without more, such as an allegation . . . that there was actual misappropriation of the PII, the benefit of the bargain theory fails. [¶] Plaintiffs have not made that allegation and cannot, based on the allegations on the face of the complaint." The court further rejected appellants' monitoring-costs theory, reasoning that "'general allegations of lost time are too speculative to constitute cognizable injury,'" and that even appellant McKinley's completed purchase of monitoring services did not constitute present injury, because it was made in response to a mere future risk of harm. Finally, the court rejected appellants' lost-value-of-PII theory, reasoning that (1) such a theory had been rejected in federal cases, including *In re Jetblue Airways Corp. Privacy Litigation* (E.D.N.Y. 2005) 379 F.Supp.2d 299 (*Jetblue*); and (2) to the extent other federal cases approved such a theory, they were distinguishable, because appellants

did not allege Centrelake voluntarily disclosed their PII or that their PII had been misused.

The court additionally concluded appellants' negligence claim was barred by the economic loss rule, because appellants sought recovery for financial losses unaccompanied by personal injury or property damage. The court rejected appellants' reliance on the special-relationship exception to the rule, reasoning that appellants did not allege any "third party relationship" with Centrelake, but instead alleged they and Centrelake were "in direct contractual privity." In concluding the rule barred appellants' recovery of their asserted damages for lost time, the court declined to follow *Bass v. Facebook, Inc.* (N.D. Cal. 2019) 394 F.Supp.3d 1024 (*Bass*), on which appellants relied, instead following two cases it deemed better reasoned. (See *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.* (S.D. Cal., Nov. 3, 2016, No. 3:16-CV-00014-GPC-BLM) 2016 U.S. Dist. LEXIS 152838, *36-*37 (*Dugas*) [economic loss rule barred recovery of lost-time damages]; *Castillo v. Seagate Technology, LLC* (N.D. Cal., Sept. 14, 2016, No. 16-CV-01958-RS) 2016 U.S. Dist. LEXIS 187428, at *5, *17-*20 [same].)

In January 2021, the court entered a judgment dismissing all appellants' claims. Appellants timely appealed.

DISCUSSION

"On appeal from a judgment of dismissal after a demurrer is sustained without leave to amend, appellate courts assume the truth of all facts properly pleaded by the plaintiff-appellant and may also consider matters subject to judicial notice, [but] 'not contentions, deductions, or conclusions of fact or law.' [Citations.] [¶] Likewise, the reviewing court . . . considers all evidentiary facts found in recitals of exhibits attached to the complaint [citation]." (Eisenberg et al., Cal. Practice Guide: Civil Appeals & Writs (The Rutter Group 2021) ¶ 8:136.) "Appellate courts will examine the complaint's factual allegations to 'determine de novo whether the complaint states facts sufficient to state a cause of action under any possible legal theory.'" (*Ibid.*) "If facts appearing in exhibits to a complaint conflict with the allegations of the complaint, . . . the appellate court will accept as true the factual contents of the exhibits rather than the factual allegations of the complaint. [Citations.] [¶] However, where the exhibits are ambiguous and can be construed as suggested by plaintiff, the court must accept plaintiff's construction." (*Id.* at ¶ 8:136.1a.)

Applying these standards, we reject Centrelake's continued attempts on appeal to mischaracterize appellants' complaint as failing to allege that appellants' PII was obtained by any third party. In fact, the complaint alleged that "unauthorized individuals gained access to and harvested" appellants' PII, that "patient information was stolen," and that the stolen PII was "disseminat[ed] into the

public domain." These allegations were consistent with Centrelake's Notice of Data Breach, attached as an exhibit. Although the Notice of Data Breach stated Centrelake's *ongoing* investigation had yet to uncover *evidence* that patients' PII had been taken, the Notice also acknowledged that a hacker had gained access to Centrelake's servers containing patients' PII over a month earlier, and that the hacker might have accessed patient records and data. Indeed, that is precisely why Centrelake encouraged patients to remain vigilant against identity theft and fraud, and established a hotline to assist them in doing so. Accordingly, in reviewing the ruling on Centrelake's demurrer below, we accept as true appellants' allegations that their PII was stolen and publicly disseminated. (See Eisenberg et al., Cal. Practice Guide: Civil Appeals & Writs, *supra*, ¶¶ 8:136, 8:136.1a.)

A. Appellants Adequately Pled a UCL Claim

Appellants contend the trial court erred in sustaining Centrelake's demurrer to their UCL claim on the basis of the court's conclusion they failed to allege a loss of money or property, as required to plead UCL standing. We agree.

1. Principles

A private plaintiff has standing to bring a UCL claim if the plaintiff "has suffered injury in fact and has lost money or property as a result of the unfair competition." (Bus. & Prof. Code, § 17204.) In other words, the plaintiff must

have suffered a "loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., *economic injury* . . . ." (*Kwikset Corp. v. Superior Court* (2011) 51 Cal.4th 310, 322 (*Kwikset*).) The UCL incorporates the meaning of injury in fact as a requirement for Article III standing to sue in federal court, under which it suffices to allege "'"some specific, 'identifiable trifle' of injury."'" (*Id.* at 322, 324; see also *id.* at 325 ["If a party has alleged or proven a personal, individualized loss of money or property in any nontrivial amount, he or she has also alleged or proven injury in fact"].) "There are innumerable ways in which economic injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." (*Id.* at 323.)

2. Benefit of the Bargain

We conclude appellants adequately pled UCL standing under their benefit-of-the-bargain theory. "[A] 'benefit of the bargain' approach to establishing UCL standing is rooted in the California Supreme Court's recognition that a plaintiff may demonstrate economic injury from unfair competition by establishing he or she 'surrender[ed] in a transaction more, or acquire[d] in a transaction less, than he or she

otherwise would have.'" (*Cappello v. Walmart Inc.* (N.D. Cal. 2019) 394 F.Supp.3d 1015, 1019-1020, quoting *Kwikset*, *supra*, 51 Cal.4th at 323; see also *Kwikset*, at 332 [plaintiffs adequately pled UCL standing, where plaintiffs alleged "[t]hey bargained for locksets that were made in the United States" but "got ones that were not," and thus did not receive the benefit of their bargain].) Here, appellants alleged they relied on Centrelake's false representations and promises concerning data security in entering contracts with Centrelake and accepting its pricing terms, paying more than they would have had they known the truth that Centrelake had not implemented and would not maintain adequate data security practices. We conclude these allegations adequately pled UCL standing under *Kwikset*. (See *Kwikset*, at 330 [plaintiffs alleged they selected locksets for purchase in part because locksets were mislabeled as made in USA: "because of the misrepresentation the consumer (allegedly) was made to part with more money than he or she otherwise would have been willing to expend . . . . That increment, the extra money paid, is economic injury and affords the consumer standing to sue"].) Indeed, many federal courts, applying *Kwikset* in the context of data-breach litigation, have held plaintiffs adequately pled UCL standing under similar benefit-of-the-bargain theories. (See, e.g., *In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation* (S.D. Cal., May 7, 2020, No. 3:19-CV-2284-H-KSC) 2020 U.S. Dist. LEXIS 80736, at *4, *27 (*Solara*) ["Plaintiffs have all pled that 'they acquired less in

their transactions with [medical supplier] than they would have if [supplier] had sufficiently protected their Personal Information.' [Citation.] These allegations are enough to establish standing for purposes of the UCL"]; *In re Marriott International, Inc., Customer Data Security Breach Litigation* (D. Md. 2020) 440 F.Supp.3d 447, 492 ["Plaintiffs allege that 'had consumers known the truth about Defendants' data security practices -- that they did not adequately protect and store their data -- they would not have stayed at a Marriott Property, purchased products or services at a Marriott Property, and/or would have paid less.' [Citation.] This is sufficient to establish standing for the UCL claim"].)[6]

---

[6] We find these cases more persuasive than the federal cases on which Centrelake relies, which did not cite *Kwikset*. (See *Fernandez v. Leidos, Inc.* (E.D. Cal. 2015) 127 F.Supp.3d 1078, 1089 [plaintiff failed to adequately plead UCL standing, where plaintiff alleged defendant contracted with plaintiff's employer to provide data security, but defendant left data tapes containing plaintiff's PII unattended in car, allowing PII to be stolen]; *Estrada v. Johnson & Johnson* (E.D. Cal., Mar. 26, 2015, No. 2:14-CV-01051-TLN-EFB) 2015 U.S. Dist. LEXIS 39581, *12-*13 [same, where plaintiff alleged defendant failed to warn her that defendant's talc-based baby powder would increase her risk of ovarian cancer]; *Dozier v. Walmart Inc.* (C.D. Cal., Mar. 5, 2021, No. CV20-05286-AB(PVCX)) 2021 U.S. Dist. LEXIS 76852, at *4-*5, *12-*16 [same, where plaintiff alleged retailer from which he bought new tires failed to comply with federal regulation requiring it to facilitate registration of tires with manufacturer].)

We disagree with the trial court's conclusion that appellants' benefit-of-the-bargain theory failed because appellants did not allege "actual misappropriation of the PII." As explained above, at this stage of the litigation, we are required to accept as true appellants' allegations that their PII was stolen and disseminated into the public domain. In any event, appellants' economic injury allegedly occurred at the time Centrelake unlawfully caused them to pay more than they otherwise would have. (See *Kwikset*, *supra*, 51 Cal.4th at 334 ["in the eyes of the law, a buyer forced to pay more than he or she would have is harmed at the moment of purchase"].) This alleged injury was not contingent upon any subsequent misappropriation of appellants' PII.

We also disagree with Centrelake's contention that appellants' benefit-of-the-bargain theory fails because data security was at most "incidental" to appellants' bargain for medical services. To the contrary, appellants alleged that data security was sufficiently material to them that had they known the truth of the matter, they would not have entered into contracts for medical services with Centrelake, or would not have accepted Centrelake's pricing terms. Such materiality is to be expected in light of the sensitive and confidential nature of the information appellants entrusted to Centrelake, including medical diagnoses and services performed, as well as Social Security numbers, driver's license numbers, and health insurance information. Few prospective patients would entrust such information -- and

pay full market prices -- to a medical provider known to be careless with it. Indeed, the Legislature has acted to protect patients' expectations that their information will be kept confidential and secure. (See Civ. Code, § 56.101, subds. (a)-(b) [requiring health care providers to maintain medical information in manner that preserves its confidentiality, and electronic medical records systems to protect and preserve integrity of electronic medical information]; cf. *Kwikset*, *supra*, 51 Cal.4th at 333 [by prohibiting fraudulent made-in-America representations, Legislature made clear that products' American origin "is precisely the sort of consideration reasonable people can and do attach importance to in their purchasing decisions"].) Moreover, "as 'materiality is generally a question of fact' [citation], it is not a basis on which to decide this case on demurrer."[7] (*Kwikset*, at 333.)

---

[7] Centrelake argues that under *Kwikset*, even a material misrepresentation cannot support a UCL claim unless the misrepresentation was "*relate[d] to the product*" purchased by the plaintiff. Under this reading of *Kwikset*, Centrelake suggests, its alleged misrepresentations concerning data security did not support appellants' UCL standing because its misrepresentations did not "describe[] its medical services." Centrelake identifies no support for this reading of *Kwikset* in the opinion itself, and we discern none. At oral argument, Centrelake argued for the first time that *Kwikset* is distinguishable because Centrelake's Notice of Privacy Practices was required under HIPAA. As noted above, Centrelake forfeited its untimely arguments concerning this

(Fn. is continued on the next page.)

Centrelake's reliance on *Irwin v. Jimmy John's Franchise, LLC* (C.D. Ill. 2016) 175 F.Supp.3d 1064 is misplaced. There, the plaintiff used debit and credit cards to purchase food at Jimmy John's restaurant, which suffered a data breach potentially exposing the plaintiff's financial information to unauthorized third parties, prompting the plaintiff to sue Jimmy John's in federal court on behalf of herself and a putative class of affected consumers. (*Id.* at 1068.) In the portion of the opinion on which Centrelake relies, the court dismissed the plaintiff's unjust enrichment claim under Arizona and Illinois law, reasoning: "[Plaintiff] paid for food products. She did not pay for a side order of data security and protection; it was merely incident to her food purchase . . . ." (*Id.* at 1071-1072.) But in a separate, more relevant portion of the opinion, the court held the plaintiff had adequately pled a claim under an Arizona consumer-protection statute similar to the UCL, by alleging the restaurant induced her and other consumers to make purchases in reliance on the restaurant's deceptive indications that their financial information would be secure. (See *id.* at 1072-1073.) Thus, to the extent this case is relevant to appellants' UCL claim, it supports their benefit-of-the-bargain theory. We conclude appellants adequately pled that theory as a basis for UCL standing.

HIPAA requirement. (See, e.g., *In re I.C.*, *supra*, 4 Cal.5th at 888.)

3. Monitoring Costs

We further conclude appellant McKinley adequately pled UCL standing under appellants' monitoring-costs theory. Under *Kwikset*, economic injury may be shown where, as a result of the defendant's unlawful conduct, the plaintiff is "required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." (*Kwikset*, *supra*, 51 Cal.4th at 323.) Here, McKinley alleged just that: because of Centrelake's unlawful failure to implement adequate data security, which resulted in the theft of McKinley's PII and an attendant risk of identity theft and fraud, she was forced to purchase credit and identity monitoring services as a reasonable and necessary prophylactic measure. We conclude these allegations adequately pled economic injury under *Kwikset*. (See, e.g., *Huynh v. Quora, Inc.* (N.D. Cal. 2020) 508 F.Supp.3d 633, 659-661 [plaintiff raised triable issue of fact regarding UCL standing by presenting evidence that defendant's challenged conduct compelled her to spend money on credit monitoring services: "payments toward enhanced credit monitoring that arise from a data breach and that are not reimbursed . . . 'constitute economic injury, sufficient to confer UCL standing'" (collecting cases applying *Kwikset*)]; accord, *Witriol v. LexisNexis Grp.* (N.D. Cal. Feb. 10, 2006) No. C05-02392 MJJ, 2006 U.S. Dist. LEXIS 26670, at *18-*19 [plaintiff adequately pled UCL standing by alleging he incurred costs monitoring and repairing credit after defendants released his PII to third parties without

authorization]; cf. *Ghazarian v. Magellan Health, Inc.* (2020) 53 Cal.App.5th 171, 193 [reversing summary judgment for defendant on UCL claim: "Due to the wrongful denial of their insurance claim, plaintiffs retained and paid an attorney to assist them with the IMR process. This is sufficient to establish standing under the UCL. . . . The transaction would have been unnecessary without defendants' conduct"].)[8]

Centrelake argues McKinley's purchase of monitoring services was unreasonable and unnecessary, relying on factors articulated by our Supreme Court in a toxic tort case, for assessing the reasonableness and necessity of medical monitoring. (See *Potter v. Firestone Tire & Rubber Co.* (1993) 6 Cal.4th 965, 1009.) Centrelake does not attempt to reconcile this argument with its own Notice of Data Breach, which encouraged patients to remain vigilant against identity theft and fraud, including by monitoring their credit and financial accounts. (See *Huynh v. Quora, Inc.*, *supra*, 508 F.Supp.3d at 652-653 [jury could reasonably find plaintiff's purchase of credit monitoring services in wake of data breach was reasonable and necessary, where

---

[8] Again, Centrelake relies on federal cases that did not cite *Kwikset*. (See *Ruiz v. Gap, Inc.* (N.D. Cal. 2009) 622 F.Supp.2d 908, 914; *Gardner v. Health Net, Inc.* (C.D. Cal., Aug. 12, 2010, No. CV 10-2140 PA (CWX)) 2010 U.S. Dist. LEXIS 157448, at *11; *Storm v. Paytime, Inc.* (M.D. Pa. 2015) 90 F.Supp.3d 359, 367; *In re SuperValu, Inc.* (D. Minn. Jan. 7, 2016, No. 14-MD-2586 ADM/TNL) 2016 U.S.Dist.LEXIS 2592, at *19--*20.)

defendant's notice of data breach could reasonably be interpreted to indicate "the severity of the Data Breach, and therefore the threat of identity theft or fraud, was still unknown"].) Moreover, appellants alleged McKinley's purchase was reasonable and necessary. Nothing in the record permits us to decree these allegations untrue, as a matter of law, at this early stage of the litigation. (See *Schmitt v. SN Servicing Corp.* (N.D.Cal. Aug. 9, 2021, No. 21-cv-03355-WHO) 2021 U.S.Dist. LEXIS 149252, at *25 ["To the extent that [defendant] factually disputes whether plaintiffs' credit monitoring costs were 'required' or 'necessary,' that cannot be resolved at this [motion to dismiss] stage"]; cf. *Potter v. Firestone Tire & Rubber Co.*, *supra*, at 1009 [medical-monitoring factors are to be applied by trier of fact on basis of competent medical testimony]; *Ruiz v. Gap, Inc.*, *supra*, 622 F.Supp.2d at 914 [granting defendants summary judgment on plaintiff's negligence claim, where plaintiff sought to recover costs of credit monitoring, but had not "presented *evidence* sufficient to overcome the kind of *evidentiary* burdens that apply in medical monitoring cases" (italics added)].)

We need not decide whether appellants Moore and Joy, who did not allege they had purchased monitoring services, adequately pled UCL standing under their monitoring-costs theory. As explained above, they adequately pled UCL standing under their benefit-of-the-bargain theory.

B. Appellants Adequately Pled Contract Claims

Appellants contend the trial court erred in sustaining Centrelake's demurrer to their contract claims based on the court's conclusion that they failed to adequately plead any cognizable contract damages. We agree.

1. Principles

"Contract damages compensate a plaintiff for its lost expectation interest. This is described as the benefit of the bargain that full performance would have brought.'" (*New West Charter Middle School v. Los Angeles Unified School Dist.* (2010) 187 Cal.App.4th 831, 844 (*New West*); accord, 24 Williston on Contracts (4th ed. 2022) § 64:3.) "Contractual damages are of two types -- general damages (sometimes called direct damages) and special damages (sometimes called consequential damages)." (*Lewis Jorge Construction Management, Inc. v. Pomona Unified School Dist.* (2004) 34 Cal.4th 960, 968 (*Lewis Jorge*).) "General damages are often characterized as those that flow directly and necessarily from a breach of contract, or that are a natural result of a breach." (*Ibid.*) General damages "'are based on the value of the performance itself, not on the value of some consequence that performance may produce.'" (*Id.* at 971; see also 24 Williston on Contracts, *supra*, § 64:3 ["When the promisor fails to perform as promised, the promisee becomes entitled to damages designed to compensate him or her for . . . the loss . . . [of] the value to the promisee of the promise that was broken"].)

"Special damages . . . represent loss that 'occurred by reason of injuries following from' the breach." (*Lewis Jorge*, *supra*, 34 Cal.4th at 969; see also 24 Williston on Contracts, *supra*, § 64:16 ["Consequential damages are those damages that do not flow directly and immediately from the breach, but only from some of the consequences or results of the breach"].) "Special damages for breach of contract are limited to losses that were either actually foreseen [citation] or were 'reasonably foreseeable' when the contract was formed." (*Lewis Jorge*, at 970.) Foreseeability is an issue of fact. (*Ash v. North American Title Co.* (2014) 223 Cal.App.4th 1258, 1268; cf. *Lewis Jorge*, at 977 [relying on trial evidence in holding contractor's lost profits were neither foreseen nor foreseeable].)

2. Benefit of the Bargain

We conclude appellants adequately pled general damages under their benefit-of-the-bargain theory. Centrelake allegedly made and breached a contractually binding promise to take appropriate steps to secure appellants' PII. General damages for this alleged breach include the value to appellants of the promised data security (i.e., performance itself). (See *Lewis Jorge*, 34 Cal.4th at 968; *New West, supra*, 187 Cal.App.4th at 844 [proper measure of damages for school district's breach of promise to allow charter school to co-locate with another school was value of promised co-location, minus costs charter school would have incurred in co-locating]; cf. *In re Adobe Systems,*

Inc. Privacy Litigation (N.D. Cal. 2014) 66 F.Supp.3d 1197, 1224 [plaintiffs adequately pled UCL standing, where plaintiffs alleged they spent more on Adobe products than they would have had they known Adobe was not providing reasonable data security as it represented it was: "It is . . . plausible that a company's reasonable security practices reduce the risk of theft of customer's personal data and thus that a company's security practices have economic value"].) Indeed, federal cases applying California law have allowed plaintiffs to seek contract damages for the lost value of promised data security or privacy. (See *In re Anthem, Inc. Data Breach Litigation* (N.D. Cal., May 27, 2016, No. 15-MD-02617-LHK), 2016 U.S. Dist. LEXIS 70594, *123-*128 [plaintiffs adequately pled contract damages, where plaintiffs alleged defendants deprived them of "'the difference in value between what Plaintiffs should have received from Defendants when they enrolled in and/or purchased insurance from Defendants that Defendants represented, contractually and otherwise, would be protected by reasonable data security, and Defendants' partial, defective, and deficient performance by failing to provide reasonable and adequate data security'" (citing *New West*, at 844)]; *Svenson v. Google Inc.* (N.D. Cal., Apr. 1, 2015, No. 13-CV-04080-BLF) 2015 U.S. Dist. LEXIS 43902, *12-*15 [same, where plaintiff alleged Google's payment-processing service was "worth quantifiably less" as a result of Google's breach of its promise not to share plaintiff's personal information with app vendor]; cf. *In re Marriott*

International, Inc., Customer Data Security Breach Litigation, *supra*, 440 F.Supp.3d at 465-466, 494-495 [same, addressing data-breach contract claims under Maryland, New York, and Oregon law].)

In challenging appellants' benefit-of-the-bargain theory as applied to their contract claims, Centrelake makes the same argument we have rejected with respect to the UCL claim, viz., that data security was at most "incidental" to the parties' bargains. As explained above, we are unpersuaded. Centrelake does not address appellants' allegation that Centrelake's promises to maintain adequate data security were incorporated into their contracts. Nor does Centrelake cite any authority -- state or federal -- addressing contract damages under California law.

We reject Centrelake's further argument that appellants' benefit-of-the-bargain theory is fatally "implausible" because appellants did not allege "how, or even whether, the cost of data protection varied among Centrelake clientele." Although appellants may be required to address such variations among the members of their putative class at later stages of the litigation, their failure to address them in the complaint is not fatal to their claims at the pleading stage. Again, Centrelake cites no California authority. The federal cases it cites are distinguishable. (See *In re Target Corp. Data Sec. Breach Litigation* (D. Minn. 2014) 66 F.Supp.3d 1154, 1178 (*In re Target*) [unjust enrichment claim against retailer was fatally implausible, where plaintiffs alleged they paid for data security when

purchasing goods with payment cards, but retailer charged same prices to customers who paid with cash and thus had no need for data security]; *Gordon v. Chipotle Mexican Grill, Inc.* (D. Colo., Aug. 1, 2018, No. 17-CV-1415-CMA-MLC) 2018 U.S. Dist. LEXIS 129928, *9-*10 [following *In re Target*; plaintiffs' allegations that restaurant's purchase prices incorporated charges for data security were too implausible to support Article III standing, because cash customers paid same prices], report and recommendation adopted in part, rejected in part (D. Colo. 2018) 344 F.Supp.3d 1231.) Indeed, *In re Target* distinguished a case decided on allegations similar to appellants'. (See *Resnick v. AvMed, Inc.* (11th Cir. 2012) 693 F.3d 1317, 1328 (*Resnick*) [plaintiffs adequately pled unjust enrichment claim against health care plan, from which laptops containing plaintiffs' PII had been stolen, by alleging their health insurance premiums incorporated payments for data security that health care plan did not provide]; *In re Target*, *supra*, 66 F.Supp.3d at 1178 [deeming *Resnick* "not on point" because in *Resnick*, all members of health care plan -- unlike retailer's cash customers -- shared their PII in their relevant transactions, and therefore paid for adequate data security].) We conclude appellants' allegations sufficed to plead general contract damages under their benefit-of-the-bargain theory.

3. *Monitoring Costs*

We further conclude appellant McKinley adequately pled special contract damages under appellants' monitoring-

costs theory. McKinley's financial loss in purchasing credit and identity monitoring services did not flow directly from Centrelake's alleged breach of contract (failure to provide promised data security), but did flow from an alleged consequence thereof (the data breach). (See *Lewis Jorge*, *supra*, 34 Cal.4th at 969.) Further, McKinley's purchase may well have been foreseeable. Indeed, Centrelake's Notice of Data Breach encouraged patients to monitor their credit and financial accounts to protect against harm resulting from the breach; Centrelake might have foreseen that McKinley would pay for assistance in doing so. In any event, foreseeability is an issue of fact. (*Ash v. North American Title Co.*, *supra*, 223 Cal.App.4th at 1268.) Centrelake does not argue otherwise, instead contending McKinley's purchase was unreasonable and unnecessary. For the reasons explained in our UCL analysis above, we reject that contention at this early stage of the litigation. Similarly, for reasons explained above, we need not decide whether appellants Moore and Joy adequately pled contract damages under their monitoring-costs theory.

C. Appellants Fail to Show the Court Erred in Dismissing Their Negligence Claim Without Leave to Amend

Appellants contend the trial court erred in sustaining Centrelake's demurrer to appellants' negligence claim under the economic loss rule, because: (1) the parties entered a special relationship, as established by an analysis of six

factors first articulated in *Biakanja v. Irving* (1958) 49 Cal.2d 647, 650 (*Biakanja*); (2) independent of the parties' contracts, Centrelake had a duty to protect appellants' PII; and (3) appellants' asserted damages for lost time are *non*-economic losses. Appellants further contend the court abused its discretion in denying their request for leave to amend their complaint. We address each contention in turn.

1. Economic Loss Rule

"The [economic loss] rule itself is deceptively easy to state: In general, there is no recovery in tort for negligently inflicted 'purely economic losses,' meaning financial harm unaccompanied by physical or property damage." (*Sheen*, *supra*, 12 Cal.5th at 922; see also *id.* at 915 [defining economic losses as "pecuniary losses unaccompanied by property damage or personal injury"]; *Southern California Gas Leak Cases* (2019) 7 Cal.5th 391, 398 [economic loss is "shorthand for 'pecuniary or commercial loss that does not arise from actionable physical, emotional or reputational injury to persons or physical injury to property'"].) The economic loss rule applies, inter alia, where the parties are in contractual privity and the plaintiff's claim arises from the contract (in other words, the claim is not independent of the contract). (*Sheen*, at 923 ["Not all tort claims for monetary losses between contractual parties are barred by the economic loss rule. But such claims are barred when they arise from -- or are not independent of -- the parties' underlying contracts"].) In such circumstances, there is no

need to analyze the *Biakanja* special-relationship factors. (*Sheen*, at 915, 942.)

We conclude appellants have failed to show error in the trial court's application of the economic loss rule. As the court observed, appellants alleged they and Centrelake were "in direct contractual privity." Further, appellants have failed to show their claim is independent of their contracts with Centrelake. Appellants provided their PII to Centrelake pursuant to the contracts establishing their provider-patient relationships, and appellants' asserted injuries arose from Centrelake's failure to provide data security allegedly promised in their contracts. Appellants identify only one potential source of an independent duty, viz., a federal regulation implementing HIPAA. But the sole California authority on which they rely did not address an independent duty of care under any statute (much less HIPAA), instead addressing the evidentiary doctrine of negligence per se, which concerns *standards* of care. (See *Satterlee v. Orange Glenn School Dist. Of San Diego County* (1947) 29 Cal.2d 581, 567-590 [under negligence per se doctrine, standard of care may be prescribed by statute, but "liability is also dependent upon proof that a duty was owed to persons in the class of the plaintiff"]; 6 Witkin, Summary of Cal. Law (11th ed. 2022) Torts, § 1004 ["It is the tort of negligence, and not the violation of the statute itself, that entitles a plaintiff [asserting negligence per se] to recover damages. Either the courts or the Legislature must have created a duty of care. The presumption of negligence

created by [California's statute codifying the negligence per se doctrine] concerns the *standard* of care, rather than the *duty* of care"].)[9] In their reply brief, appellants make no mention of HIPAA, instead relying on a federal case concluding the economic loss rule did not bar a claim of negligent misrepresentation. (See *Whittington v. KidsEmbrace, LLC* (C.D. Cal., July 19, 2021, No. CV 21-1830-JFW(JPRX)) 2021 U.S. Dist. LEXIS 138713, at *16-*18.) That case is inapposite, as negligent

---

[9] Similarly, appellants' out-of-state authorities do not support their reliance on HIPAA, except perhaps as a basis for applying the evidentiary doctrine of negligence per se. (See *Tuck v. City of Gardiner Police Department* (D. Me., Feb. 13, 2019, No. 1:18-CV-00212-JDL) 2019 U.S. Dist. LEXIS 23180, at *9 [noting defendant medical provider did not dispute plaintiff's contention that defendant had duty to ensure privacy of patients' medical information], citing *Bonney v. Stephens Memorial Hosp.* (Me. 2011) 17 A.3d 123, 128 [stating, in dicta, HIPAA standards "may be admissible to establish the *standard* of care associated with a state tort claim" (italics added)]; *Acosta v. Byrum* (N.C. Ct. App. 2006) 180 N.C.App. 562, 571-572 (*Acosta*) [trial court erred in purporting to dismiss HIPAA cause of action, where complaint included no such cause of action, and plaintiff merely cited HIPAA as "evidence of the appropriate standard of care"]; Ilene N. Moore et al., *Confidentiality and Privacy in Health Care from the Patient's Perspective: Does HIPAA Help?* (2007) 17 Health Matrix 215, 230-231 [citing *Acosta* for proposition that HIPAA regulations have been used as "evidence of standards in state tort actions"].)

misrepresentation is a tort "'separate and distinct'" from negligence.[10] (*Sheen*, *supra*, 12 Cal.5th at 943.)

We reject appellants' contention that their asserted lost-time damages are *non*-economic losses and therefore exempt from the economic loss rule. Appellants' complaint alleged they suffered "[a]scertainable losses in the form of . . . the value of their time," implicitly referring to their time's financial value. Appellants do not claim these financial losses were accompanied by any personal injury or property damage. Accordingly, appellants fail to show the trial court erred in concluding these losses were economic. (See *Sheen*, *supra*, 12 Cal.5th at 915, 922; *Castillo v. Seagate Technology, LLC*, *supra*, 2016 U.S. Dist. LEXIS 187428, *5, *17-*20 [concluding plaintiffs' expenditures of "considerable time and effort" were economic losses]; *Dugas*, *supra*, 2016 U.S. Dist. LEXIS 152838, at *36-*37 [concluding plaintiff's "time spent and loss of productivity" were economic losses].)[11]

---

[10] Because the parties are in contractual privity and appellants have failed to show their claim is independent of the parties' contracts, we need not address the parties' arguments concerning the existence of a special relationship under the *Biakanja* factors. (See *Sheen*, at 915, 942.) We note that appellants' complaint alleged the parties entered into a special relationship "when they contracted" for medical services.

[11] Appellants misrepresent *Dugas*, asserting it "clearly holds that loss of time is compensable," but citing its discussion of
(Fn. is continued on the next page.)

We are not persuaded by the cases on which appellants rely. The sole California case they cite is inapposite. (See *Rupp v. Summerfield* (1958) 161 Cal.App.2d 657, 667 [trial court did not erroneously permit double recovery in malicious prosecution action, where court instructed jury it could award plaintiff damages for both lost earnings and lost time during plaintiff's underlying incarceration].) As the trial court did, we decline to follow *Bass*, *supra*, 394 F.Supp.3d 1024, the leading federal case on which appellants rely. (See, e.g., *Solara*, *supra*, 2020 U.S. Dist. LEXIS 80736, at *11 [following *Bass* on this issue].) In *Bass*, the court concluded the economic loss rule did not bar a negligence claim arising from a data breach, because the plaintiff alleged a non-economic loss, viz., time spent sorting through phishing emails. (*Bass*, at 1039.) But *Bass* neither articulated any reasoning for concluding the plaintiff's lost-time damages were non-economic, nor cited any authority for this conclusion. In fact, this conclusion was undermined by the very authority *Bass* cited in determining that the plaintiff's lost time was an injury in fact. (See *Bass*, at 1035 ["loss of time establishes injury in fact," because "'the value of one's own time needed to set things straight is a loss from an opportunity-cost perspective'" (quoting *Dieffenbach v. Barnes & Noble, Inc.* (7th Cir. 2018) 887 F.3d 826, 828 (*Dieffenbach*))]; *Dieffenbach*, at 828-829 [where hackers stole

---

Article III standing. (See *Dugas*, *supra*, 2016 U.S. Dist. LEXIS 152838, at *18-*20.)

plaintiff's payment card information from retailer, plaintiff's resulting loss of time sorting matters with police and bank was loss, "at least in *economic* terms," under California authority indicating "significant time and paperwork costs incurred to rectify violations . . . can qualify as *economic* losses" (italics added)]; cf. *Perdue v. Hy-Vee, Inc.* (C.D. Ill. 2020) 455 F.Supp.3d 749, 761 [following *Dieffenbach*; plaintiffs' losses of time in wake of data breach were economic losses, which plaintiffs were barred from recovering under Illinois economic loss rule].) We conclude appellants have failed to show the trial court erred in applying the economic loss rule to sustain Centrelake's demurrer to appellants' negligence claim.

2. Proposed Amendment

"Review of the trial court's failure to grant leave to amend is conducted under the abuse of discretion standard." (Eisenberg et al., Cal. Practice Guide: Civil Appeals & Writs, *supra*, ¶ 8:136.2.) "The plaintiff-appellant has the burden of demonstrating abuse of discretion by showing how the complaint can be amended to state a cause of action." (*Id.* at ¶ 8:136.3; accord, Weil & Brown, Cal. Practice Guide: Civil Procedure Before Trial (The Rutter Group 2022) Ch. 7(I)-A ¶ 7:130 ["It is not up to the judge to figure out how the complaint can be amended to state a cause of action. Rather, the burden is on plaintiff to show *in what manner* plaintiff can amend the complaint, and *how* that amendment will change the legal effect of the pleading"].) Although "such

showing may be made in the first instance to the appellate court," the plaintiff-appellant "must still offer details on how the amendment would cure the defects." (Weil & Brown, Cal. Practice Guide: Civil Procedure Before Trial, *supra*, ¶ 7:130.)

We conclude appellants have failed to show the trial court abused its discretion in sustaining Centrelake's demurrer to their negligence claim without leave to amend. Appellants fault the court for failing to allow them to add allegations of a future need to retake medical tests, asserting that "[e]ven if Plaintiffs' other damages theories were deficient, an amendment to the Complaint fully alleging this new theory would clearly cure the defect." They do not specify any defect, much less explain how the proposed amendment would cure it. Nor do they attempt to explain how the proposed amendment might enable their negligence claim to overcome the economic loss rule. Accordingly, they have forfeited any such argument. (See *People v. Guzman* (2019) 8 Cal.5th 673, 683, fn. 7 [appellant forfeited due process claim by failing to "develop the argument"]; *In re Phoenix H.* (2009) 47 Cal.4th 835, 845 [""Contentions supported neither by argument nor by citation of authority are deemed to be without foundation and to have been abandoned""].) We conclude appellants have failed to show an abuse of discretion in the court's dismissal of their negligence claim without leave to amend. (See Eisenberg et al., Cal. Practice Guide: Civil Appeals & Writs, *supra*,

¶ 8:136.3; Weil & Brown, Cal. Practice Guide: Civil Procedure Before Trial, *supra*, ¶ 7:130.)

D. Guidance on Remand

As explained above, although appellants have failed to show error in the trial court's dismissal of their negligence claim without leave to amend, we have concluded the court erred in sustaining Centrelake's demurrer to appellants' UCL and contract claims. Accordingly, we will affirm the judgment with respect to the negligence claim, reverse with respect to the UCL and contract claims, and remand for further proceedings on the latter claims. To provide guidance to the court and the parties on remand, we address appellants' allegations that the data breach deprived them of some portion of the value of their PII. We conclude appellants failed to adequately plead their lost-value-of-PII theory as a basis for either UCL standing or an award of contract damages.

First, we conclude appellants' lost-value-of-PII theory, as pled, is insufficient to support UCL standing. We need not accept as true appellants' allegation that they suffered "[a]scertainable losses in the form of deprivation of the value of their PII," as this constitutes a conclusion or deduction, unsupported by any properly pled facts. (See Eisenberg et al., Cal. Practice Guide: Civil Appeals & Writs, *supra*, ¶ 8:136.) Appellants properly pled only that their PII was stolen and disseminated, and that a market for it existed. They did not allege they ever attempted or intended to

participate in this market, or otherwise to derive economic value from their PII. Nor did they allege that any prospective purchaser of their PII might learn that their PII had been stolen in this data breach and, as a result, refuse to enter into a transaction with them, or insist on less favorable terms. In the absence of any such allegation, appellants failed to adequately plead that they lost money or property in the form of the value of their PII. (See, e.g., *In re Google Inc. Cookie Placement Consumer Privacy Litigation* (3d Cir. 2015) 806 F.3d 125, 149, 152 [affirming dismissal of UCL claim against Google, where plaintiffs alleged Google allowed defendant advertisers to circumvent plaintiffs' cookie blockers and track plaintiffs' internet-history information in contravention of Google's own public statements: "when it comes to showing 'loss,' the plaintiffs' argument lacks traction. They allege no facts suggesting that they ever participated or intended to participate in the market they identify, or that the defendants prevented them from capturing the full value of their internet usage information for themselves"]; *Bass*, *supra*, 394 F.Supp.3d at 1040 ["That the information has external value, but no economic value to plaintiff, cannot serve to establish that plaintiff has personally lost money or property"]; cf. *Folgelstrom v. Lamps Plus, Inc.* (2011) 195 Cal.App.4th 986, 989, 994 [plaintiff failed to adequately plead UCL standing, where plaintiff alleged retailer obtained plaintiff's zip code under false pretenses and, using zip code, paid third party for license to use plaintiff's address: "The fact that the

address had value to [the retailer], such that the retailer paid [the third party] a license fee for its use, does not mean that its value to plaintiff was diminished in any way"]; *Archer v. United Rentals, Inc.* (2011) 195 Cal.App.4th 807, 816 [same, where plaintiffs claimed retailers unlawfully collected and recorded their PII as condition to accepting credit card payments].)

We further conclude appellants' lost-value-of-PII theory, as pled, is insufficient to support an award of contract damages. We find persuasive *Jetblue*, *supra*, 379 F.Supp.2d 299, on which the trial court relied. There, the plaintiffs alleged they made reservations to fly with JetBlue airline, in reliance on JetBlue's contractual promises not to share their PII with third parties, but JetBlue breached the contracts by sharing their PII with a federal government subcontractor. (*Id.* at 324-325.) At a hearing on JetBlue's motion to dismiss, the plaintiffs requested leave to amend their complaint's contract claim to allege they were deprived of the economic value of their PII. (*Id.* at 326.) Denying this request, the court dismissed the contract claim. (*Id.* at 326-327.) The court explained that the proposed damages theory "ignore[d] the nature of the contract asserted," under which appellants had no expectation interest in the economic value of their PII: "Plaintiffs may well have expected that in return for providing their personal information to JetBlue and paying the purchase price, they would obtain a ticket for air travel and the promise that their personal information would be safeguarded consistent with the terms of the

privacy policy. They had no reason to expect that they would be compensated for the 'value' of their personal information. In addition, there is absolutely no support for the proposition that the personal information of an individual JetBlue passenger had any value for which that passenger could have expected to be compensated. It strains credulity to believe that, had JetBlue not provided [plaintiffs'] data en masse to [the subcontractor], [the subcontractor] would have gone to each individual JetBlue passenger and compensated him or her for access to his or her personal information."[12] (*Id.* at 327.) Although *Jetblue* applied New York contract law, its focus on the expectations of the parties is consistent with California law. (See *New West*, *supra*, 187 Cal.App.4th at 844.) *Jetblue* is also consistent with other federal cases, including *Pruchnicki v. Envision Healthcare Corporation* (9th Cir. 2021) 845 Fed.Appx. 613 (*Pruchnicki*). There, the Ninth Circuit affirmed dismissal of a breach of contract claim where, despite studies showing PII "may have value in general," the plaintiff failed to adequately allege that as a result of a data breach, her PII "actually lost value." (*Id.* at 614-615, citing *In re Google, Inc. Privacy Policy Litigation* (N.D. Cal., July 15, 2015, No. 5:12-CV-001382-PSG) 2015 U.S. Dist. LEXIS 92736, at *18, fn. 63; see also

---

[12] In purporting to distinguish *Jetblue*, appellants ignore its holding on the contract claim, instead citing its separate holding concerning a claim of trespass to chattels. (See *Jetblue*, *supra*, 379 F.Supp.2d at 328.)

LaCourt v. Specific Media, Inc. (C.D. Cal., Apr. 28, 2011, No. SACV 10-1256 GW (JCGX)) 2011 U.S. Dist. LEXIS 50543, at *3-*4, *11-*12 [plaintiffs failed to adequately plead Article III standing, where plaintiffs alleged defendant's unauthorized collection and use of plaintiffs' internet-history information deprived them of its economic value, but did not allege they personally "ascribed an economic value" to such information or were "foreclosed from entering into a 'value-for-value exchange' as a result of [defendant's] alleged conduct"].)

We find these cases, including the Ninth Circuit's recent decision in *Pruchnicki*, more persuasive than an older Ninth Circuit case on which appellants rely. (See *In re Facebook Privacy Litigation* (9th Cir. 2014) 572 Fed.Appx. 494, 494 (*Facebook Privacy*) [district court erred in dismissing breach of contract claims for failure to adequately plead damages: "Plaintiffs allege that the information disclosed by Facebook [to third-party advertisers] can be used to obtain personal information about plaintiffs, and that they were harmed . . . by losing the sales value of that information. In the absence of any applicable contravening state law, these allegations are sufficient to show the element of damages for their breach of contract and fraud claims"].) In relying on the purported absence of contravening state law, *Facebook Privacy* put the cart before the horse -- damages are not recoverable unless authorized by law. The scant California authority cited by *Facebook Privacy* did not address the value of PII, much less any

deprivation thereof. (See *Gautier v. General Tel. Co.* (1965) 234 Cal.App.2d 302, 305-306 [trial court properly sustained demurrer to plaintiffs' claim that defendant telephone company breached contract by refusing to transfer calls]; *Lazar v. Superior Court* (1996) 12 Cal.4th 631, 637, 648-649 [trial court erred in sustaining demurrer to plaintiff's claim that defendant fraudulently induced him to leave former job for new job in another state].) We find *Facebook Privacy* unpersuasive.[13]

---

[13] Accordingly, we are unpersuaded by appellants' reliance on federal district court cases that followed *Facebook Privacy* on this issue. (See, e.g., *Calhoun v. Google LLC* (N.D. Cal. 2021) 526 F.Supp.3d 605, 636 (*Calhoun*) [following *Facebook Privacy* and three district court cases that had followed it, including two earlier cases decided by same judge, in holding plaintiffs adequately pled UCL standing by alleging Google collected information from them without authorization, diminishing information's property value].) In their appellate reply brief, appellants misrepresent *Calhoun*, asserting "the court held broadly that loss of privacy in personal information is a legally recognized injury . . . ." In fact, *Calhoun* addressed a loss of *privacy* -- as opposed to a loss of property value -- only in holding the plaintiffs had adequately pled an intrusion-upon-seclusion claim (one variety of the tort of invasion of privacy). (See *id.* at 629-631.) In any event, appellants forfeited any contention that "'privacy harm' . . . itself adequately demonstrates damages," by failing to raise such a contention before the trial court or in their opening appellate brief. (See *People v. Morales* (2020) 10 Cal.5th 76, 98 [finding argument "doubly forfeited" by appellant's failure to object in trial court or raise issue in opening appellate brief].)

Many other cases on which appellants rely are inapposite. (See *Fraley v. Facebook, Inc.* (N.D. Cal. 2011) 830 F.Supp.2d 785, 791-792, 798-799, 811 [distinguishing *Jetblue*, where plaintiffs alleged Facebook misappropriated their names and likenesses by using them in commercial endorsements, but did *not* allege "that their personal information ha[d] inherent economic value and that the mere disclosure of such data constitute[d] a loss of money or property"]; *CTC Real Estate Services v. Lepe* (2006) 140 Cal.App.4th 856, 858-861 [trial court erred in denying identity-theft victim's unopposed claim for recovery of remaining proceeds of the theft, on unjust enrichment theory]; *KNB Enterprises v. Matthews* (2000) 78 Cal.App.4th 362, 364-365 [federal copyright law did not preempt statutory claims based on defendant's misappropriation of photography models' right of publicity]; *In re Facebook, Inc. Internet Tracking Litigation* (9th Cir. 2020) 956 F.3d 589, 610-611 (*Facebook Tracking*) [affirming dismissal of contract claim, where plaintiffs failed to adequately plead existence of contract].) In the portion of *Facebook Tracking* on which appellants rely, the court held the plaintiffs had Article III standing to bring certain claims not at issue here, based on Facebook's unauthorized collection and use of the plaintiffs' internet-history information, which the court recognized had value to Facebook. (*Facebook Tracking*, 956 F.3d at 599-601.) But the court did not suggest the plaintiffs suffered any corresponding loss of value -- on the contrary, it relied on unjust enrichment law, under which each plaintiff had a

stake in Facebook's profits "regardless of whether . . . the individual's data [wa]s made less valuable." (*Id.* at 600.) Here, in contrast, appellants rely on a theory that Centrelake made their PII less valuable to them. We conclude they did not adequately plead this theory as a basis for either UCL standing or contract damages.

DISPOSITION

The judgment is affirmed with respect to the dismissal of appellants' negligence claim without leave to amend. The judgment is otherwise reversed. The matter is remanded for further proceedings consistent with this opinion. Appellants are awarded their costs on appeal.

CERTIFIED FOR PUBLICATION

MANELLA, P. J.

We concur:

WILLHITE, J.

CURREY, J.