Filed 2/4/13

IN THE SUPREME COURT OF CALIFORNIA

APPLE INC.,	)	
	)	
Petitioner,	)	
	)	S199384
v.	)	
	)	Ct.App. 2/8 B238097
THE SUPERIOR COURT OF LOS ANGELES COUNTY,	)	Los Angeles County Super. Ct. No. BC463305
	)	
Respondent;	)	
	)	
DAVID KRESCENT,	)	
	)	
Real Party in Interest.	)	
_____	)	

The Song-Beverly Credit Card Act of 1971 (Credit Card Act) governs the issuance and use of credit cards. (Civ. Code, § 1747 et seq.; all further statutory references are to the Civil Code unless otherwise indicated.) One of its provisions, section 1747.08, prohibits retailers from "[r]equest[ing], or requir[ing] as a condition to accepting the credit card as payment . . . , the cardholder to write any personal identification information upon the credit card transaction form or otherwise." (§ 1747.08, subd. (a) (hereafter section 1747.08(a)).) It also prohibits retailers from requesting or requiring the cardholder "to provide personal identification information, which the [retailer] . . . writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise," and from "[u]tiliz[ing] . . . a credit card form which contains preprinted spaces specifically designed for filling in any personal identification information of the

cardholder." (*Ibid.*) In *Pineda v. Williams-Sonoma Stores, Inc.* (2011) 51 Cal.4th 524 (*Pineda*), we considered whether section 1747.08 is violated when a retailer requests and records a customer's ZIP code during a credit card transaction. Relying on the statute's language, legislative history, and purpose, we concluded that a ZIP code constitutes "personal identification information" within the meaning of the statute and that the Credit Card Act forbids a retailer from requesting or recording such information. (*Pineda*, at pp. 527–528.)

Like *Pineda*, this case involves an asserted violation of section 1747.08. David Krescent, the plaintiff in this case, alleged in his complaint that defendant Apple Inc. requested or required him to provide his address and telephone number as a condition of accepting his credit card as payment. However, unlike *Pineda*, which concerned the purchase of a physical product at a traditional "brick-and-mortar" business, this case concerns the purchase of an electronic download via the Internet. We must resolve whether section 1747.08 prohibits an online retailer from requesting or requiring personal identification information from a customer as a condition to accepting a credit card as payment for an electronically downloadable product. Upon careful consideration of the statute's text, structure, and purpose, we hold that section 1747.08 does not apply to online purchases in which the product is downloaded electronically.

Our dissenting colleagues warn that today's decision "relegate[s] to the dust heap" the " 'robust' consumer protection . . . at the heart of section 1747.08" (dis. opn. by Kennard, J., *post*, at p. 6) and represents a "major loss for consumers" (*id.* at p. 1) that "leaves online retailers free to collect and use the personal identification information of credit card users as they wish" (dis. opn. by Baxter, J., *post*, at p. 1). These ominous assertions, though eye-catching, do not withstand scrutiny. As we explain, existing state and federal laws provide consumers with a degree of protection against unwanted use or disclosure of personal identification information. The Legislature may believe these measures are inadequate and, if so, may enact additional protections. Or the Legislature

may believe that existing laws, together with market forces reflecting consumer preferences, are sufficient. It is not our role to opine on this important policy issue. We merely hold that section 1747.08 does not govern online purchases of electronically downloadable products because this type of transaction does not fit within the statutory scheme.

I.

Because this case comes to us following summary denial of a writ of mandate after the denial of a demurrer, we assume as true all facts alleged in the operative complaint. (*Sheehan v. San Francisco 49ers, Ltd.* (2009) 45 Cal.4th 992, 996.) Petitioner Apple Inc. (Apple), defendant below, operates an Internet Web site and an online iTunes store through which it sells digital media such as downloadable audio and video files. In June 2011, plaintiff below, David Krescent, sued Apple on behalf of himself and a putative class of similarly situated individuals for alleged violations of section 1747.08. Specifically, Krescent alleged that he purchased media downloads from Apple on various occasions and that, as a condition of receiving these downloads, he was required to provide his telephone number and address in order to complete his credit card purchase. He further alleged that Apple records each customer's personal information, is not contractually or legally obligated to collect a customer's telephone number or address in order to complete the credit card transaction, and does not require a customer's telephone number or address for any special purpose incidental but related to the individual credit card transaction, such as shipping or delivery. Although he alleged that "the credit card transaction would be permitted to proceed" without any personal identification information, Krescent also contended that "even if the credit card processing company or companies required a valid billing address and [credit card identification number], under no circumstance would [plaintiff's] telephone number be required to complete his transaction, that is, under no circumstance does [Apple] need [plaintiff's] phone number in order to complete a [media] download transaction."

In September 2011, Apple filed a demurrer, arguing that the Credit Card Act does not apply to online transactions and that deciding otherwise would undermine the prevention of identity theft and fraud. After a hearing, the trial court overruled the demurrer. The court noted that "the Act itself is silent on exempting online credit card transactions from its purview (and otherwise does not address online credit card transactions specifically)." While acknowledging that Apple's "assertions with respect to preventing fraud have definite appeal (a problem which the Court acknowledges is widespread in credit transactions generally, and in online credit card transactions specifically)," the trial court said it "is not prepared, at the pleading stage, to read the [Credit Card] Act as completely exempting online credit transactions from its reach." The court also found, pursuant to Code of Civil Procedure section 166.1, that appellate resolution of the issue might materially assist the resolution of the litigation.

Apple filed a petition for writ of mandate seeking review of the trial court's order, which the Court of Appeal summarily denied. We granted Apple's petition for review and ordered the trial court to show cause why the relief sought in the petition for writ of mandate should not be granted.

II.

We review de novo questions of statutory construction. In doing so, " 'our fundamental task is to "ascertain the intent of the lawmakers so as to effectuate the purpose of the statute." ' " (*Mays v. City of Los Angeles* (2008) 43 Cal.4th 313, 321.) As always, we start with the language of the statute, "giv[ing] the words their usual and ordinary meaning [citation], while construing them in light of the statute as a whole and the statute's purpose [citation]." (*Pineda, supra*, 51 Cal.4th at pp. 529–530.)

A.

We begin with the text of the statute. Section 1747.08(a) provides: "Except as provided in subdivision (c), no person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall do any of the following: [¶] (1)

Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to write any personal identification information upon the credit card transaction form or otherwise. [¶] (2) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the person, firm, partnership, association, or corporation accepting the credit card writes, causes to be written, or otherwise records upon the credit card transaction form or otherwise. [¶] (3) Utilize, in any credit card transaction, a credit card form which contains preprinted spaces specifically designated for filling in any personal identification information of the cardholder." Section 1747.08, subdivision (b) (hereafter section 1747.08(b)) defines " 'personal identification information' " as "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number."

The prohibitions codified in section 1747.08(a) are subject to various exceptions set forth in section 1747.08, subdivision (c) (hereafter section 1747.08(c)). Subdivision (c) provides that the requirements of subdivision (a) do not apply to "[c]ash advance transactions" or "[i]f the credit card is being used as a deposit to secure payment in the event of default . . . or other similar occurrence." (§ 1747.08(c)(1), (2).) Nor do the requirements of subdivision (a) apply if the person, firm, partnership, association, or corporation accepting the credit card "is contractually obligated to provide personal identification information in order to complete the credit card transaction"; "uses the Zip Code information solely for prevention of fraud, theft, or identity theft" in a "sales transaction at a retail motor fuel dispenser or retail motor fuel payment island automated cashier"; or "is obligated to collect and record the personal identification information by federal or state law or regulation." (§ 1747.08(c)(3)(A)–(C).) Personal identification information may also be collected if it "is required for a special purpose incidental but related to the individual credit card transaction, including, but not limited to, information

relating to shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders." (§ 1747.08(c)(4).)

Finally, section 1747.08, subdivision (d) (hereafter section 1747.08(d)) provides the following general qualification to the statute's requirements: "This section does not prohibit any person, firm, partnership, association, or corporation from requiring the cardholder, as a condition to accepting the credit card as payment in full or in part for goods or services, to provide reasonable forms of positive identification, which may include a driver's license or a California state identification card, or where one of these is not available, another form of photo identification, provided that none of the information contained thereon is written or recorded on the credit card transaction form or otherwise. If the cardholder pays for the transaction with a credit card number and does not make the credit card available upon request to verify the number, the cardholder's driver's license number or identification card number may be recorded on the credit card transaction form or otherwise."

At the outset, we observe that the text of section 1747.08 makes no reference to online transactions or the Internet. This is not surprising because former section 1747.8, section 1747.08's predecessor, was enacted in 1990 (Stats. 1990, ch. 999, § 1, p. 4191), before the privatization of the Internet (see Frischmann, *Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market* (2001) 2 Colum. Sci. & Tech. L.Rev. 1, 20) and almost a decade before online commercial transactions became widespread (see, e.g., *McDonough v. Toys "R" Us, Inc.* (E.D.Pa. 2009) 638 F.Supp.2d 461, 468).

Although section 1747.08 does not explicitly reference online transactions, both parties maintain that the Legislature's intent is apparent from the plain meaning of the statute's terms. Krescent contends that the language of section 1747.08(a) "must be read as an all-inclusive prohibition on every businesses [sic] regardless of the form of the

transaction." According to Krescent, in directing the statutory prohibition at any "person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business" (§ 1747.08(a)), the Legislature intended to include all retailers without exception. If the Legislature intended to exempt online retailers, he contends, it could have done so.

Apple, on the other hand, argues that the first sentence of section 1747.08(a) must be construed in light of other language in the statute indicating that the Legislature had in mind only in-person business transactions. For example, section 1747.08(a)(1) prohibits a retailer from requesting or requiring a "cardholder to *write* any personal identification information *upon the credit card transaction form* or otherwise." (Italics added.) Section 1747.08(a)(2) prohibits a retailer from requesting or requiring the cardholder to provide such information, which the retailer "*writes, causes to be written, or otherwise records upon the credit card transaction form* or otherwise." (Italics added.) And section 1747.08(a)(3) prohibits the retailer from utilizing "a *credit card form which contains preprinted spaces*." (Italics added.) Apple says the terms "write" and "forms" imply, by their physicality, that section 1747.08 applies only to in-person transactions. Apple further argues that the definition of "credit card" in section 1747.02 — "any card, plate, coupon book, or other single credit device existing for the purpose of being used from time to time *upon presentation* to obtain money, property, labor, or services on credit" — indicates that the Legislature contemplated only those transactions in which the card is physically presented or displayed to the retailer. (§ 1747.02, subd. (a), italics added.)

We think the text of section 1747.08(a) alone is not decisive on the question before us. The statutory language suggests that the Legislature, at the time it enacted former section 1747.8, did not contemplate commercial transactions conducted on the Internet. But it does not seem awkward or improper to describe the act of typing characters into a digital display as "writing" on a computerized "form." In construing statutes that predate their possible applicability to new technology, courts have not relied

on wooden construction of their terms. Fidelity to legislative intent does not "make it impossible to apply a legal text to technologies that did not exist when the text was created. . . . Drafters of every era know that technological advances will proceed apace and that the rules they create will one day apply to all sorts of circumstances they could not possibly envision." (Scalia & Garner, Reading Law: The Interpretation of Legal Texts (2012) pp. 85–86.)

For example, in *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, the Court of Appeal considered whether an online news magazine constitutes a "periodical publication" for purposes of California's journalism shield law, which was enacted well before the advent of "digital magazines." (*Id.* at p. 1461.) The court considered the argument that "the shield law only applies to 'periodical publications' *in print*, because that was a common feature of newspapers and magazines at the time the law was enacted." (*Id.* at p. 1462.) But the court did not regard that meaning as dispositive, instead finding the statutory term ambiguous enough to encompass the Web site at issue. (*Id.* at pp. 1463–1466.) The court ultimately found the shield law applicable to the Web site through a careful examination of the Legislature's purpose in enacting the statute, not on the basis of the plain meaning of " 'periodical publication.' " (*Id.* at pp. 1462–1463; see *id.* at p. 1465 ["Given the numerous ambiguities presented by 'periodical publication' in this context, its applicability must ultimately depend on the purpose of the statute"].)

In *Ni v. Slocum* (2011) 196 Cal.App.4th 1636, 1649 (*Slocum*), the Court of Appeal considered "whether the use of electronic signature qualifies as 'personally affix[ing]' the signature" on an initiative petition as that phrase is used in the Elections Code. (See Elec. Code, § 100 ["Each signer shall at the time of signing the petition or paper personally affix his or her signature, printed name, and place of residence . . . ."].) The county argued that a signer must "*physically* 'attach[]' the signature to the petition by inscribing it with a writing utensil," whereas the petitioner claimed that the statutory requirement can be satisfied by "tracing one's signature and address on the face of a smartphone in

response to online instructions accompanying a copy of the petition." (*Slocum*, *supra*, 196 Cal.App.4th at pp. 1649–1650.) Although the statute was enacted in 1933, long before electronic signatures existed, the Court of Appeal found "no reason to reject either of these definitions solely on the basis of the plain language of the statute." (*Id.* at p. 1650; see *id.* at p. 1652 ["Statutory interpretation must be prepared to accommodate technological innovation, if the technology is otherwise consistent with the statutory scheme"].)

Rather, the court in *Slocum* ultimately concluded that an electronic signature system was "not entirely consistent with the present statutory scheme for the endorsement of initiative petitions because . . . electronic signature software deletes the circulator from the signature collection process" by allowing "voters to gain access to petitions from the Internet and execute them without the assistance or intervention of a circulator." (*Slocum*, *supra*, 196 Cal.App.4th at pp. 1652–1653.) The court explained that the "Elections Code requires each petition submitted to county election officials to be accompanied by the declaration of the circulator, attesting to the genuineness of the signatures on the petition," and that "the Legislature viewed the participation of the circulator as a protection against fraud in the collection of signatures." (*Id*. at p. 1652.) Thus, the court concluded that "the electronic signature system is partially incompatible with the current statutory scheme" because it "eliminates from the signature collection system one of its primary protections against fraud." (*Id.* at p. 1653.)

In this case, as in *O'Grady* and *Slocum*, the plain meaning of the statute's text is not decisive. An examination of the statutory scheme as a whole is necessary to determine whether it is applicable to a transaction made possible by technology that the Legislature did not envision.

B.

We recently considered the history and purpose of the Credit Card Act in *Pineda*, *supra*, 51 Cal.4th 524. There we said "[t]he statute's overriding purpose was to 'protect

the personal privacy of consumers who pay for transactions with credit cards.' " (*Id.* at p. 534, quoting Assem. Com. on Finance and Ins., Analysis of Assem. Bill No. 2920 (1989–1990 Reg. Sess.) as amended Mar. 19, 1990, p. 2.) Specifically, the Legislature "sought to address the misuse of personal identification information for, inter alia, marketing purposes, and found that there would be no legitimate need to obtain such information from credit card customers if it was not necessary to the completion of the credit card transaction." (*Absher v. AutoZone, Inc.* (2008) 164 Cal.App.4th 332, 345, quoted in *Pineda*, at p. 535.) "To protect consumers, the Legislature sought to prohibit businesses from 'requiring information that merchants, banks or credit card companies do not require or need.' " (*Pineda*, at p. 534, quoting Assem. Com. on Finance and Ins., Analysis of Assem. Bill No. 2920 (1989–1990 Reg. Sess.) as amended Mar. 19, 1990, p. 2.)

While it is clear that the Legislature enacted the Credit Card Act to protect consumer privacy, it is also clear that the Legislature did not intend to achieve privacy protection without regard to exposing consumers and retailers to undue risk of fraud. The legislative history shows that the Legislature enacted the statute's prohibitions only after carefully considering and rejecting the possibility that the collection of personal identification information by brick-and-mortar retailers could serve a legitimate purpose such as fraud prevention. In particular, the Senate Judiciary Committee considered the standard procedure followed by brick-and-mortar retailers in the 1990s to verify the identity of credit card users — which included "verify[ing] the identification of the cardholder by comparing the signature on the credit card transaction form with the signature on the back of the card" and "contact[ing] the credit card issuer's authorization center [to] obtain approval" for sales above a specified "floor limit" — and concluded that the collection of personal identification information was not a necessary step in that procedure. (Sen. Judiciary Com., Analysis of Assem. Bill No. 2920 (1989–1990 Reg. Sess.) as amended June 27, 1990, p. 3.) This finding supported the Legislature's

judgment that brick-and-mortar retailers in the 1990s had no genuine need to collect personal identification information and would instead use such information primarily for unsolicited marketing. (See *id.* at pp. 3–4 [noting that the "problem" the bill was designed to address was retailers' practice of leading consumers "to mistakenly believe that [personal identification information] is a necessary condition to complete the credit card transaction, when, in fact, it is not" and "acquir[ing] this additional personal information for their own business purposes — for example, to build mailing or telephone lists which they can subsequently use for their own in-house marketing efforts, or sell to direct-mail or tele-marketing specialists, or to others"]; *id.* at pp. 5–7 [explaining that retailers had no genuine need for personal identification information to address problems such as billing errors, lost credit cards, and product problems].) We cannot assume that the Legislature, had it confronted a type of transaction in which the standard mechanisms for verifying a cardholder's identity were not available, would have made the same policy choice as it did with respect to transactions in which it found no tension between privacy protection and fraud prevention.

Further, the Legislature in 1991 "added a provision (former § 1747.8, subd. (d)) . . . substantially similar to the subdivision (d) now in section 1747.08, permitting businesses to require cardholders to provide identification so long as none of the information contained thereon was recorded." (*Pineda, supra*, 51 Cal.4th at p. 535, citing Stats. 1991, ch. 1089, § 2, p. 5042.) The adoption of this provision was described as "a clarifying, nonsubstantive change." (State and Consumer Services Agency, Enrolled Bill Rep. on Assem. Bill No. 1477 (1991–1992 Reg. Sess.) Sept. 9, 1991, p. 3.) As previously noted, section 1747.08(d) makes clear that nothing in the statute prevents retailers from requiring customers to provide positive identification — "which may include a driver's license or a California state identification card, or where one of these is not available, another form of photo identification" — as a condition of accepting a credit card as payment. In addition, although section 1747.08(d) generally prohibits a retailer

from recording information contained on a customer's photo identification card, a retailer may record the customer's driver's license number or similar information when the customer does not make the credit card available for verification, presumably so that the customer may be identified and located in the event of a problem with the use of the credit card. Section 1747.08(d) shows that while the Legislature indeed sought to protect consumer privacy, it did not intend to do so at the cost of creating an undue risk of credit card fraud. Rather, section 1747.08(d) demonstrates the Legislature's intent to permit retailers to use and even record personal identification information when necessary to combat fraud and identity theft — objectives that not only protect retailers but also promote consumer privacy.

The safeguards against fraud that are provided in section 1747.08(d) are not available to the online retailer selling an electronically downloadable product. Unlike a brick-and-mortar retailer, an online retailer cannot visually inspect the credit card, the signature on the back of the card, or the customer's photo identification. Thus, section 1747.08(d) — the key antifraud mechanism in the statutory scheme — has no practical application to online transactions involving electronically downloadable products. We cannot conclude that if the Legislature in 1990 had been prescient enough to anticipate online transactions involving electronically downloadable products, it would have intended section 1747.08(a)'s prohibitions to apply to such transactions despite the unavailability of section 1747.08(d)'s safeguards.

Krescent's complaint reinforces our conclusion insofar as it failed to allege that Apple does not require any personal identification information to verify the identity of the credit card user. His complaint merely alleged that "the credit card transaction would be permitted to proceed without any further information" and that Apple "is not contractually obligated to provide a consumer's telephone number and/or address in order to complete the credit card transaction," thereby rendering inapplicable the exception set forth in section 1747.08(c)(3)(A). Even if credit card transactions may proceed without

any personal identification information under the contractual terms that bind retailers and credit card companies, the fact remains that the Legislature saw fit to include section 1747.08(d)'s safeguards against fraud in the statutory scheme. The inclusion of section 1747.08(d), separate and apart from the exception in section 1747.08(c)(3)(A), reflects the Legislature's judgment that consumers and retailers have an interest in combating fraud that is independent of whatever security measures are (or are not) required by contracts between retailers and credit card issuers. Consistent with this legislative judgment, both parties acknowledged at oral argument that retailers often bear the risk of loss from fraudulent credit card charges.

In addition, Krescent suggested in his complaint and expressly conceded at oral argument that Apple may need at least a valid billing address, if not a telephone number, to verify the credit card. However, according to Krescent's own allegations, there would be no way for Apple to collect this information under the statute. As noted, Krescent alleged that Apple is neither contractually nor legally obligated to collect such information; hence, the exceptions in section 1747.08(c)(3)(A) and (C) do not apply. Krescent also alleged that Apple does not require a customer's address for a special purpose incidental but related to the credit card transaction, such as shipping, because the product is electronically downloadable; hence, the exception in section 1747.08(c)(4) does not apply. Likewise, the exceptions concerning motor fuel retailers, cash advance transactions, and transactions in which a credit card is used as a form of security have no applicability to this case. (§ 1747.08(c)(1), (2), (3)(B).)

At oral argument, Krescent suggested that Apple might be able to collect a customer's billing address as a "reasonable form[] of positive identification" under section 1747.08(d). But section 1747.08(b) includes "the cardholder's address" as a type of personal identification information retailers are forbidden to collect. Moreover, Krescent's view cannot be squared with the full text of section 1747.08(d), which says retailers may require the cardholder "to provide reasonable forms of positive

identification, which may include a driver's license or California state identification card, or where one of these is not available, another form of photo identification, provided that none of the information provided thereon is written or recorded on the credit card transaction form or otherwise." A billing address is not a "form of photo identification." (See *Costco Wholesale Corp. v. Superior Court* (2009) 47 Cal.4th 725, 743 ["Under the principle of statutory construction known as '*ejusdem generis*,' the general term ordinarily is understood as being ' "restricted to those things that are similar to those which are enumerated specifically" ' "].) And Krescent's own complaint alleged that Apple "records each consumer's personal information, including, but not limited to a telephone number and address, in line with each credit card transaction, and keeps records of such personal information." In short, section 1747.08(d) does not permit Apple to collect a billing address in the course of an online transaction.

In his brief (but not in his complaint), Krescent argued that requiring a customer to provide his or her name, credit card number, card expiration date, and credit card identification number suffices to prevent fraud. But it is clear that the Legislature has disagreed. A customer's name, credit card number, expiration date, and security code are all apparent to a "brick-and-mortar" retailer on the credit card itself when the card is presented during an in-person transaction. Yet the Legislature expressly authorized retailers to request additional information — namely, a driver's license, state identification card, or another form of photo identification — in order to combat fraud. (§ 1747.08(d).) The Legislature has thus decided that the information on the credit card is not necessarily sufficient by itself to protect consumers and retailers against fraud.

Our dissenting colleagues offer various arguments against the conclusion that the statute, if applied to the online transaction in this case, would prohibit Apple from collecting information necessary to combat fraud. Justice Kennard cites section 1747.08(c)(3)(A), which allows retailers to collect personal identification information that they are "contractually obligated to provide . . . in order to complete the credit card

transaction," as one "layer of protection against fraud." (Dis. opn. by Kennard, J., *post*, at p. 7.) But Krescent's complaint stated that Apple is not contractually obligated to collect any such information, and we must accept this allegation as true on demurrer. (See *ante*, at p. 13.) Justice Kennard also notes that the second sentence of section 1747.08(d) allows retailers "to record the number appearing on the buyer's driver's license or similar identification." (Dis. opn. by Kennard, J., *post*, at p. 7.) But the second sentence of section 1747.08(d) allows a retailer to record such information when a buyer "pays for the transaction with a credit card number and does not make the credit card available upon request," presumably so that the buyer may be tracked down if the use of the credit card number turns out to be improper. This provision contemplates that the retailer can verify that the driver's license or identification card belongs to the buyer; indeed, section 1747.08(d) makes clear that a driver's license or identification card has significance in this context as a "form of photo identification." In an online transaction, even if the retailer were to collect a driver's license number, the retailer has no way to verify that the number corresponds to the person using the credit card number.

In his dissent, Justice Baxter asserts that we indulge an unwarranted "factual assumption — that the personal identification information defendant allegedly demanded and collected here, i.e., cardholder addresses and telephone numbers, are 'necessary to combat fraud and identity theft' in online credit card transactions." (Dis. opn. by Baxter, J., *post*, at pp. 7–8.) In fact, we do nothing of the sort. We express no view as to what type of information — whether an address, telephone number, or something else — is essential to verify a cardholder's identity. We hold only that the statutory scheme and legislative history make clear the Legislature's concern that there be *some mechanism* by which retailers can verify that a person using a credit card is authorized to do so. No such mechanism would exist in the context of online purchases of electronically downloadable products if the statute were read to apply to such transactions. Because the statutory scheme provides no means for online retailers selling electronically

downloadable products to protect against credit card fraud, we conclude that the Legislature could not have intended section 1747.08 to apply to this type of transaction.

We have no occasion here to decide whether section 1747.08 applies to online transactions that do not involve electronically downloadable products or to any other transactions that do not involve in-person, face-to-face interaction between the customer and retailer. Our dissenting colleagues contend that section 1747.08 must apply to online transactions because the Legislature intended it to apply to "other card-not-present transactions" such as mail order and telephone order (MOTO) transactions. (Dis. opn. by Baxter, J., *post*, at pp. 9–10; see dis. opn. by Kennard, J., *post*, at pp. 4–6.) We express no view on whether the statute governs mail order or telephone order transactions, as that issue is not presented and has not been briefed in this case. In any event, even if the statute does apply to MOTO transactions, we do not think such transactions, which often involve "shipping [or] delivery . . . of the purchased merchandise" (§ 1747.08(c)(4)), are readily likened to online purchases of electronically downloadable products with respect to possible means of preventing or detecting fraud.

III.

Krescent contends that the text and legislative history of a 2011 amendment to the Credit Card Act show that section 1747.08 applies to online transactions. As explained below, we disagree.

In 2011, the Legislature amended the Credit Card Act to add section 1747.08(c)(3)(B), which provides that the prohibitions of section 1747.08(a) do not apply if "[t]he person, firm, partnership, association, or corporation accepting the credit card in a sales transaction at a retail motor fuel dispenser or retail motor fuel payment island automated cashier uses the Zip Code information solely for prevention of fraud, theft, or identity theft." This amendment applies to "pay-at-the-pump" transactions in which no employee or other seller of the agent is present. (See § 1747.02, subd. (n) [defining " 'retail motor fuel dispenser' " as "a device that dispenses fuel . . . , that processes the

sale of fuel through a remote electronic payment system, and that is in a location where an employee or other agent of the seller is not present"]; § 1747.02, subd. (o) [defining " 'retail motor fuel payment island automated cashier' " in similar terms].) Krescent argues that because the 2011 amendment creates a narrow exception for a certain type of remote transaction, it would have been unnecessary surplusage if the statute was never intended to apply to remote transactions in the first place. In his view, the 2011 amendment confirms that all retailers, including retailers conducting business remotely, are governed by the statute.

The logic of Krescent's argument holds only if one assumes that a remote transaction conducted at a gas station stands on equal footing with an online transaction, and that by addressing the former in 2011, the Legislature necessarily signaled the statute's applicability to the latter. But there are good reasons to doubt this assumption. As Apple points out in its brief, "the customer engaging in a pay-at-the-pump transaction has physical possession of the card, which must be swiped," and "is capable of being seen, either because an employee is at the gas station, or because there is video surveillance of the pump." Thus, pay-at-the-pump transactions arguably present less risk of fraud than online transactions because a customer engaged in an online transaction need not possess a physical card and can complete the transaction in the privacy of his or her own home. It seems counterintuitive to posit that the Legislature created a fraud prevention exemption only for pay-at-the-pump retailers while leaving online retailers unprotected, when online retailers — a multibillion-dollar industry by the year 2011 — have at least as much if not more need for an exemption to protect themselves and consumers from fraud.

The more logical inference is that the Legislature did not address pay-at-the-pump transactions in 2011 against the backdrop of the statute's applicability to all remote transactions, including online transactions, but rather that the Legislature addressed pay-at-the-pump transactions against the backdrop of the statute's applicability to in-person transactions at ordinary brick-and-mortar retailers, the paradigmatic type of transaction addressed by the statute's text. Compared to ordinary brick-and-mortar retailers, gas stations with payment island automated cashiers may indeed have heightened fraud concerns, and it would make sense for the Legislature to grant them more leeway to record personal identifying information. Indeed, the 2011 amendment supports the view that the Legislature's policy behind the statute has been, and continues to be, to protect consumer privacy without putting retailers in the position of having to accept credit card payments when they are unable to confirm that the person using the card is authorized to do so.

We acknowledge that the legislative history of the 2011 amendment contains some indications that appear to support Krescent's position. The gas station exemption became law with the passage of Assembly Bill No. 1219 (2011–2012 Reg. Sess.). One version of the bill proposed to "amend the Song-Beverly Credit Card Act in a manner that would restrict its application to instances in which a card is 'physically presented' to a retailer, apparently with the intent of allowing retailers to collect personal information for fraud prevention purposes where the card is not physically presented, as in an on-line or other electronic transaction." (Assem. Com. on Judiciary, Analysis of Assem. Bill No. 1219 (2011–2012 Reg. Sess.) as amended May 4, 2011, p. 1, italics omitted.) In reviewing this version, the Assembly Committee on Judiciary concluded it "sweeps too broadly in effectively removing on-line and telephonic transactions from the scope of the existing law's protection." (*Ibid.*, italics omitted.) Because "this was not the bill's intent" according to its sponsor, the committee said it "strongly recommends that this language come out of the bill." (*Id.* at p. 5, underlining omitted.) Consistent with that

recommendation, Assembly Bill No. 1219 (2011–2012 Reg. Sess.) was enacted without the restrictive language. (§ 1747.08, as amended by Stats. 2011, ch. 690; see also Sen. Judiciary Com., Analysis of Assem. Bill No. 1219 (2010-2011 Reg. Sess.) as amended June 22, 2011, p. 2.) As passed, the bill provided a specific exemption for automated cashiers at gas stations.

For several reasons, however, we do not find this legislative history persuasive on the meaning of section 1747.08 as enacted in 1990. First, "[t]he declaration of a later Legislature is of little weight in determining the relevant intent of the Legislature that enacted the law." (*Peralta Community College Dist. v. Fair Employment & Housing Com.* (1990) 52 Cal.3d 50, 52). This is especially true where, as here, "a gulf of decades separates the two [legislative] bodies." (*Western Security Bank v. Superior Court* (1997) 15 Cal.4th 232, 244.) We thus give little weight to the views of the Legislature of 2011 as to what the Legislature of 1990 intended.

Second, "[u]npassed bills, as evidences of legislative intent, have little value." (*Dyna-Med, Inc. v. Fair Employment & Housing Com.* (1987) 43 Cal.3d 1379, 1396). Although plaintiff contends that the never-enacted provisions were premised on the Legislature's understanding that section 1747.08 applies to online transactions, the Legislature's decision not to enact those provisions plausibly supports the opposite inference: the Legislature may have concluded that it was unnecessary to remove online transactions from the statute's coverage because such transactions were never covered by the statute in the first place.

Third, the legislative history on whether the statute applies to online transactions is conflicting. For example, when the 2011 amendment was first proposed, a federal district court had already ruled in *Saulic v. Symantec Corp.* (C.D.Cal. 2009) 596 F.Supp.2d 1323 that section 1747.08 does not apply to online transactions, and "the Legislature is deemed to be aware of existing laws and judicial decisions in effect at the time legislation is enacted and to have enacted and amended statutes ' "in the light of such decisions as have

a direct bearing upon them." ' " (*People v. Overstreet* (1986) 42 Cal.3d 891, 897.) In addition, an Assembly analysis of proposed Senate amendments noted that "this bill simply creates an express exemption in current law from the prohibition on collecting zip code information in a retail credit card transaction at a motor fuel dispenser so long as the zip code information is used to prevent fraud, theft or identity theft," an exemption that "the courts may determine in current litigation . . . *always existed*." (Assem. Floor analysis, Assem. Bill No. 1219 (2011–2012 Reg. Sess.) Sept. 8, 2011, p. 3, italics added.) Similarly, the sponsor of the unenacted proposal to remove online and telephonic transactions from the statute's coverage indicated that the proposal was "intended to clarify existing law." (Assem. Com. on Judiciary, Analysis of Assem. Bill No. 1219 (2011–2012 Reg. Sess.) as amended May 4, 2011, p. 2.)

Fourth, in contrast to the conflicting evidence and legally dubious inferences from the 2011 legislative history as to whether the 1990 statute applies to online transactions, what *is* clear from the legislative history is that the 2011 amendment was enacted to address a very specific problem. Our 2011 holding in *Pineda*, *supra*, 51 Cal.4th 524, that a ZIP code constitutes "personal identification information" within the meaning of section 1747.08(b) applied retroactively to uses of the ZIP code prior to our ruling. The California Retailers Association, the sponsor of Assembly Bill No. 1219, "claim[ed] that about 150 lawsuits [had] been filed against retailers in the wake of the Supreme Court decision, including against gas stations that collect zip codes for fraud prevention purposes." (Assem. Com. on Judiciary, Analysis of Assem. Bill No. 1219 (2011–2012 Reg. Sess.) as amended May 4, 2011, p. 1, italics omitted.) The Western States Petroleum Association argued to the Legislature that "[w]ithout specific language expressly exempting fraud prevention, . . . its member companies 'may face years of costly litigation.' " (*Id.* at p. 8; see also Assem. Com. on Banking and Finance, Analysis

of Assem. Bill No. 1219 (2010–2011 Reg. Sess.) as amended Apr. 25, 2011, p. 2 ["The need for this bill arises from . . . *Pineda v. Williams-Sonoma Stores, Inc*. . . ."].) In response, the Legislature created an "express exemption from the prohibition against the collection and retention of zip code information when the zip code is used solely for prevention of fraud, theft, or identity theft in a sales transaction at a retail motor fuel dispenser or retail motor fuel payment island automated cashier." (Assem. Floor analysis, Assem. Bill No. 1219 (2011–2012 Reg. Sess.) Sept. 8, 2011, p. 1.)

Thus, the problem the Legislature sought to address in 2011 was a narrow one: how to deal with lawsuits filed against traditional brick-and-mortar retailers, particularly gas stations, that had been collecting ZIP codes for years under the mistaken belief that they were not prohibited from doing so under section 1747.08. Given the Legislature's specific focus, it is not surprising that the Assembly Committee on Judiciary recommended that the bill be written narrowly, without the use of broad language unnecessary to address the particular problem faced by gas stations that use automated cashiers. In sum, we cannot draw any firm conclusion concerning the applicability of section 1747.08 to online transactions from the legislative history of the 2011 gas station exemption for the simple reason that the Legislature in 2011 was not presented with that issue.

IV.

Finally, the California Online Privacy Protection Act of 2003 (COPPA) shows that the Legislature knows how to make clear that it is regulating online privacy and that it does so by carefully balancing concerns unique to online commerce. COPPA provides that "[a]n operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site . . . ." (Bus. & Prof. Code, § 22575, subd. (a).) The privacy policy must: "(1) Identify the categories of personally identifiable

information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information. [¶] (2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process. [¶] (3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service. [¶] (4) Identify its effective date." (Bus. & Prof. Code, § 22575, subd. (b).)

Although it is theoretically possible to construe COPPA as imposing requirements on online transactions that go above and beyond the requirements of section 1747.08, we find no evidence of such a legislative intent. Instead, there is evidence to the contrary. The Senate Rules Committee's third reading analysis of COPPA indicated that this legislation was necessary because "[e]xisting law does not directly regulate the privacy practices of online business entities." (Sen. Rules Com., 3d reading analysis of Assem. Bill No. 68 (2003-2004 Reg. Sess.) as amended Sept. 3, 2003, p. 2.) The bill's author explained that because "many consumers refuse to do business online because they have little protection against abuse," online retailers should be required at least to disclose in their online privacy policies what personal information may be collected and how it is used. (Assem. Com. on Business and Professions, Analysis of Assem. Bill No. 68 (2003–2004 Reg. Sess.) as amended Apr. 28, 2003, p. 2; see also Assem. Com. on Judiciary, Analysis of Assem. Bill No. 68 (2003–2004 Reg. Sess.) as amended Apr. 2, 2003, p. 3 ["Any policy will do. The bill simply requires that an operator have a policy and then follow it"].) According to the bill's author, this disclosure regime would "provide[] meaningful privacy protection[] that will help foster the continued growth of

the Internet economy." (Assem. Com. on Business and Professions, Analysis of Assem. Bill No. 68 (2003–2004 Reg. Sess.) as amended Apr. 28, 2003, p. 2.)

The enactment of COPPA suggests that when the Legislature intends to address online transactions, it does so unambiguously. In addition, the fact that COPPA enacts merely a disclosure regime suggests that the Legislature in 2003 sought to proceed cautiously in regulating online commerce or, at least for the time being, to strike a different policy balance than the Credit Card Act did in 1990 for the collection of personally identifiable information.

COPPA also refutes our dissenting colleagues' assertion that today's decision will leave online retailers "free to require personal identification information as a condition of credit card acceptance and to use such information for whatever purposes they wish." (Dis. opn. by Baxter, J., *post,* at p. 12; see dis. opn. by Kennard, J., *post,* at pp. 1, 6.) As noted, COPPA requires online retailers to "conspicuously post" their privacy policies, to disclose "the categories of personally identifiable information" they collect, and to identify "the categories of third-party persons or entities with whom [they] may share that personally identifiable information." (Bus. & Prof. Code, § 22575, subds. (a), (b).) If a consumer is not satisfied with the policy of a particular retailer, he or she may decline to purchase a product from that retailer. The Legislature could have reasonably believed that its disclosure regime creates significant incentives, in light of consumer preferences, for online retailers to limit their collection and use of personally identifiable information.

Federal law also provides some degree of protection against the use of personal identification information for unwanted commercial solicitation. The Telephone Consumer Protection Act of 1991 (TCPA; Pub.L. No. 102–243 (Dec. 20, 1991) 105 Stat. 2394) was enacted "to protect the privacy interests of residential telephone subscribers by placing restrictions on unsolicited, automated telephone calls to the home and to facilitate interstate commerce by restricting certain uses of facsimile . . . machines and automatic dialers." (Sen.Rep. No. 102-178, 1st Sess., p. 1, reprinted in 1991 U.S. Code Cong. &

Admin. News, p. 1968; see 47 U.S.C. § 227.) "[T]he TCPA instructs the [Federal Communications Commission] to issue regulations 'concerning the need to protect residential telephone subscribers' privacy rights to avoid receiving telephone solicitations to which they object." (*Charvat v. NMP, LLC* (6th Cir. 2011) 656 F.3d 440, quoting 47 U.S.C. § 227(c)(1).) "In 2003, two federal agencies — the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) — promulgated rules that together created the national do-not-call registry. [Citations.] The national do-not-call registry is a list containing the personal telephone numbers of telephone subscribers who have voluntarily indicated that they do not wish to receive unsolicited calls from commercial telemarketers. Commercial telemarketers are generally prohibited from calling phone numbers that have been placed on the do-not-call registry, and they must pay an annual fee to access the numbers on the registry so that they can delete those numbers from their telephone solicitation lists." (*Mainstream Mktg. Servs. v. FTC* (10th Cir. 2004) 358 F.3d 1228, 1233–1234, fns. omitted.) Thus, federal legislation limits the commercial use of customer telephone numbers.

There can be no doubt that retail commerce has changed dramatically since section 1747.08 was enacted and even since COPPA and the federal TCPA were enacted. In 1990, the idea of computerized transactions involving the sale and purchase of virtual products was beyond any legislator's imagination. Such technology was not even a twinkle in Steve Jobs's eye; at the time, Jobs had just begun to experiment with the concept of "interpersonal computing." (*New Models of NeXT Computer Lauded; Users, Analysts Praise Changes in Hardware, Software*, Rocky Mountain News (Sept. 23, 1990) p. B8; see Isaacson, Steve Jobs (2011) pp. 211–237, 293–294 [discussing Jobs's attempted innovations in personal computing during the late 1980s and early 1990s].) Today, retail "e-commerce" sales in the United States approach $200 billion a year (see U.S. Census Bur., E-Stats (May 12, 2012) pp. 3–4 <http://www.census.gov/econ/estats/2010/2010reportfinal.pdf> [as of Feb. 4, 2013]), and it has been estimated that iTunes

alone will generate as much as $13 billion in revenue for Apple in 2013 through the sale of apps, music, movies, and e-books (see Gobry, *Apple Will Generate $13 Billion in iTunes Revenue in 2013, Says Analyst*, Business Insider, July 5, 2011 <http://www.businessinsider.com/apple-itunes-revenue-2013-2011-7> [as of Feb. 4, 2013]). Although "[s]tatutory interpretation must be prepared to accommodate technological innovation," this is only possible "if the technology is otherwise consistent with the statutory scheme." (*Slocum*, *supra*, 196 Cal.App.4th at p. 1652.) Having thoroughly examined section 1747.08's text, purpose, and history, we are unable to find the clarity of legislative intent or consistency with the statutory scheme necessary to conclude that the Legislature in 1990 intended to bring the enormous yet unforeseen advent of online commerce involving electronically downloadable products — and the novel challenges for privacy protection and fraud prevention that such commerce presents — within the coverage of the Credit Card Act.

In light of our holding today, the Legislature may wish to revisit the issue of consumer privacy and fraud prevention in online credit card transactions, just as it revisited the use of ZIP codes in the wake of our 2011 decision in *Pineda*. We cast no doubt on Krescent's claim that protecting consumer privacy in online transactions is an important policy goal, nor do we suggest that combating fraud is as important or more important than protecting privacy. We express no view on this significant issue of public policy. Our role is to determine what the Legislature intended by the statute it enacted. Here the statutory scheme, considered as a whole, reveals that the Legislature intended to safeguard consumer privacy while also protecting retailers and consumers against fraud. This accommodation of interests struck by the Legislature would not be achieved if section 1747.08 were read to apply to online transactions involving electronically downloadable products. Because we cannot make a square peg

fit a round hole, we must conclude that online transactions involving electronically downloadable products fall outside the coverage of the statute.

CONCLUSION

For the foregoing reasons, the Court of Appeal's judgment summarily denying the petition for writ of mandate or prohibition is reversed, and the matter is remanded to that court with directions to issue a writ consistent with this opinion.

LIU, J.

WE CONCUR: CANTIL-SAKAUYE, C. J.
WERDEGAR, J.
CORRIGAN, J.

DISSENTING OPINION BY KENNARD, J.

To protect consumer privacy, California statutory law prohibits retail sellers from recording the personal identification information, such as home addresses and telephone numbers, of their credit-card-using customers. (Civ. Code,[1] § 1747.08, subd. (a).) The statute does not exempt online sales of downloadable products from this prohibition, and on its face the statute applies to sales conducted over the Internet just as it does to sales conducted face-to-face or by mail or telephone. Yet the majority holds that online sales of downloadable products are not covered by the statute, thus leaving Internet retailers free to demand personal identification information from their credit-card-using customers and to resell that information to others. The majority's decision is a major win for these sellers, but a major loss for consumers, who in their online activities already face an ever-increasing encroachment upon their privacy.

Unlike the majority, I conclude that the statute means just what it says and contains no exemption, express or implied, for online sales of downloadable products. The majority's expressed concern that this plain-meaning construction of the statute leaves online sellers with no way to detect and prevent fraudulent purchases is unjustified, as I explain.

---

[1] All undesignated statutory references are to the Civil Code.

I

David Krescent filed a complaint alleging that on four occasions in 2010, he bought downloadable products from Apple, Inc. (Apple); that he used a credit card to pay for those products; and that Apple, as a condition of completing those purchases and in violation of section 1747.08, required him to provide his home address and telephone number, which he did. Krescent seeks statutory penalties for those alleged violations. He also seeks certification of a class comprising all individuals who within the year preceding the filing of the complaint purchased downloadable products from Apple, paid by credit card, and were required by Apple to give home addresses and telephone numbers.

Section 1747.08's predecessor was enacted in 1990 as former section 1747.8. (Stats. 1990, ch. 999, § 1, p. 4191.) The Legislature has since then amended the statute several times and renumbered it in 2004. (Stats. 2004, ch. 183, § 29, p. 981.) The statute prohibits sellers from recording their credit-card-using customers' "personal identification information" (§ 1747.08, subd. (a)), such as the cardholder's address and telephone number (§ 1747.08, subd. (b)). It applies to any "person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business." (§ 1747.08, subd. (a).)

Apple filed a demurrer. A demurrer is, in essence, a request that the case be dismissed because the facts alleged in the complaint are insufficient as a matter of law to justify any relief. In this situation, "we review the allegations of the operative complaint for facts sufficient to state a claim for relief." (*C.A. v. William S. Hart Union High School Dist.* (2012) 53 Cal.4th 861, 866.) In support of its demurrer, Apple argued that section 1747.08 does not apply to Internet transactions, because the Internet as we know it today did not exist in 1990 when the Legislature enacted the statutory provisions at issue. Apple contended that the statute contemplates a transaction involving the *physical* presentation of a credit card (or something similar) and the recording of data from that

card onto a *paper* credit card transaction form, neither of which is possible in a transaction done electronically over the Internet.

In overruling Apple's demurrer, the trial court said it was "not prepared, at the pleading stage, to read [section 1747.08] as completely exempting online credit transactions from its reach," thus indicating that any ruling in Apple's favor would require a more developed factual record than what had been presented at that early stage of the proceedings. Apple petitioned the Court of Appeal for a writ of mandate, which the court summarily denied. This court then granted Apple's petition for review.

II

Section 1747.08's broad language (see p. 2, *ante*) applies to any "person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business." (§ 1747.08, subd. (a).) Apple comes within that definition. The Legislature made some express exceptions in the statute (*id.*, subd. (c)), but none pertains to a categorical exemption for online transactions. Nevertheless, the majority here exempts online sellers of downloadable products from complying with the statutory prohibition against a seller's recording of the personal identification information of its credit-card-using customers. The majority reasons that the Legislature could not have intended section 1747.08 to apply to such online sellers, and it repeatedly emphasizes the novelty of Internet-based commerce. (See, e.g., maj. opn., *ante*, p. 11 ["We cannot assume that the Legislature, had it confronted a type of transaction in which the standard mechanisms for verifying a cardholder's identity were not available, would have made the same policy choice as it did with respect to transactions in which it found no tension between privacy protection and fraud prevention."]; *id.*, p. 12 ["We cannot conclude that if the Legislature in 1990 had been prescient enough to anticipate online transactions involving electronically downloadable products, it would have intended section 1747.08(a)'s prohibitions to apply to such transactions despite the unavailability of section 1747.08(d)'s safeguards."]; *id.*, p. 25 ["[W]e are unable . . . to conclude that the

Legislature in 1990 intended to bring the enormous yet unforeseen advent of online commerce involving electronically downloadable products — and the novel challenges for privacy protection and fraud prevention that such commerce presents — within the coverage of the Credit Card Act."].)

No significant difference exists between a purchase conducted over the Internet and one conducted through the mail or by telephone. In both cases, the credit card is not physically presented to the seller, who nevertheless has limited ways of confirming the buyer's identity. Also, in some mail and telephone sales (as with online sales of downloadable products) the seller does not need the purchaser's mailing address for shipping purposes. Some examples: when the buyer has a gift sent to a third party's address, or pays for news, entertainment, or other information to be conveyed by telephone. (See maj. opn., *ante*, p. 16.) Although modern-day Internet commerce did not exist in 1990, when the statutory provisions at issue were enacted, by that time mail order and telephone order transactions (hereafter also referred to as MOTO transactions) were well established. (See, e.g., Winn, *Clash of the Titans: Regulating the Competition between Established and Emerging Electronic Payment Systems* (1999) 14 Berkeley Tech. L.J. 675, 688 (hereafter Winn) ["decades of MOTO transactions" preceded the advent of Internet commerce].)

Jane K. Winn (the Charles I. Stone Professor at the University of Washington School of Law) has written numerous academic publications on electronic commerce and is considered a leading international authority in that field. In the article cited above, Professor Winn observes that merchants who accepted credit cards as payment in mail order and telephone order transactions developed "sophisticated security systems . . . to keep fraud and error losses to a minimum" (Winn, *supra*, at p. 688), thus accommodating the desire of these merchants to conduct business remotely. After the Internet's emergence, the same antifraud practices that had applied to mail order and telephone

order transactions were "transferred [to the Internet] to manage risks with Internet-based commerce." (*Ibid*.)

The Law Revision Commission's comment on Evidence Code section 450 allows reliance on academic publications like Professor Winn's article: "Under the Evidence Code, as under existing law, courts may consider whatever materials are appropriate in construing statutes . . . . That a court may consider legislative history, *discussions by learned writers in treatises and law reviews*, materials that contain controversial economic and social facts or findings or that indicate contemporary opinion, and similar materials is inherent in the requirement that it take judicial notice of the law. In many cases, the meaning and validity of statutes . . . can be determined only with the help of such extrinsic aids. . . ." (Italics added.)[2]

Although Professor Winn's factual assertions are not part of the meager record before us, further development of the factual record could establish those assertions beyond question. By holding in Apple's favor and ending the litigation, the majority precludes such further development of the record.

Succinctly put, the similarity between online transactions and mail order or telephone order transactions belies the majority's insistence that its holding exempting online sellers such as Apple from compliance with section 1747.08 is necessary to protect these sellers from consumer fraud.

---

[2] I note the majority's reliance on assertions of fact in various publications. (See maj. opn., *ante*, p. 6, citing Frischmann, *Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market* (2001) 2 Colum. Sci. & Tech. L.Rev. 1, 20; maj. opn., *ante*, pp. 24-25, citing *New Models of NeXT Computer Lauded; Users, Analysts Praise Changes in Hardware, Software*, Rocky Mountain News (Sept. 23, 1990) p. B8, Isaacson, Steve Jobs (2011) pp. 211–237, 293–294, and Gobry, *Apple Will Generate $13 Billion in iTunes Revenue in 2013, Says Analyst*, Business Insider, July 5, 2011 <http://www.businessinsider.com/apple-itunes-revenue-2013-2011-7> [as of February 4, 2013].)

The majority's focus on fraud protection for sellers is at odds with this court's recent statement in *Pineda v. Williams-Sonoma Stores, Inc.* (2011) 51 Cal.4th 524 that section 1747.08's "*overriding purpose* was to 'protect the personal privacy of consumers who pay for transactions with credit cards.' [Citation.]" (*Pineda*, *supra*, at p. 534, italics added.) That "robust" consumer protection (*id*. at p. 536), at the heart of section 1747.08, is now largely relegated to the dust heap. As a result of the majority's decision, online sellers of downloadable products can collect unlimited personal information concerning their credit-card-using customers and sell that information to, or share it with, other companies, which, for marketing purposes, can then construct detailed consumer profiles. The majority concedes that "[t]he Legislature may believe [existing privacy protections] are inadequate and, if so, may enact additional protections" (maj. opn., *ante*, p. 2), but the majority overlooks the fact that the Legislature *already did* enact additional protections. It enacted section 1747.08. The majority eviscerates those protections by rejecting the plain meaning of the statute. The majority's policy-driven construction of the statute contradicts its claim that "[i]t is not our role to opine on this important policy issue" (maj. opn., *ante*, p. 3) and "we express no view on this significant issue of public policy" (*id*., p. 25).

Moreover, application of section 1747.08 to sellers of downloadable products would not prevent these sellers from taking protective measures against fraud. Because of the remote nature of the Internet transaction, the buyer cannot physically present a credit card to the seller. This is why in that situation the seller is expressly permitted under the second sentence of section 1747.08's subdivision (d), added in 1995, to record the number appearing on the buyer's driver's license or similar identification.[3] And a different provision of the same statute allows online sellers of downloadable products to

---

[3] This statutory provision indicates that, contrary to the majority's assertion, section 1747.08 was intended to apply to remote transactions, not just face-to-face transactions.

collect personal identification information about a cardholder if "contractually obligated" to do so (§ 1747.08, subd. (c)(3)(A)), thus providing another layer of protection against fraud — depending on the terms of the contracts between the seller, the payment processor, the merchant bank, and the bank that issued the credit card.[4]

A final point: The majority states that when the Legislature wants to regulate online businesses, it must do so expressly, as it did in the California Online Privacy Protection Act of 2003. (Maj. opn., *ante*, p. 23.) Under that reasoning, the civil rights protections of the Unruh Civil Rights Act (§ 51) would not apply to online businesses because that act does not refer to those businesses expressly; similarly, under the majority's reasoning the Commercial Code would not apply to online businesses because the code does not mention those businesses expressly.

III

As noted (see p. 6, *ante*), this court recently held unanimously that the Legislature's "overriding" purpose in enacting section 1747.08's prohibition against a seller's recording of a credit-card-using customer's personal identification information was to protect a consumer's right to privacy. (*Pineda v. Williams-Sonoma Stores, Inc.*, *supra*, 51 Cal.4th at p. 534.) Whether to limit or to broaden that right is a power that belongs exclusively to the Legislature. The majority here trespasses upon the Legislature's domain by going far beyond the statute's plain language in order to

---

[4] The majority notes that real party in interest Krescent's complaint alleges that Apple is not contractually obligated to collect personal identification information. (Maj. opn., *ante*, p. 15.) True. But the question here is not whether Apple *availed itself* of the fraud-prevention provisions that the statute offers; rather, the question is whether the statute *offers* some fraud-prevention possibilities. Therefore, that specific allegation of the complaint is not relevant here. That Apple has voluntarily chosen to do business in a way that precludes it from using the antifraud provisions that the Legislature has provided cannot support the majority's justification for a general exemption from the statute.

judicially graft upon the statute an exemption for online sellers such as Apple so they need not comply with section 1747.08. Unlike the majority, I would affirm the Court of Appeal's judgment summarily denying the petition for writ of mandate, thus upholding the trial court's overruling of Apple's demurrer.

KENNARD, J.

WE CONCUR:

BAXTER, J.
JONES, J.*

* Presiding Justice of the Court of Appeal, First Appellate District, Division Five, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

DISSENTING OPINION BY BAXTER, J.

I respectfully dissent.

Section 1747.08 of the Civil Code[1] was enacted to prevent any retailer such as defendant Apple Inc. from collecting and exploiting the personal identification information of consumers who use credit cards to make their purchases. Plaintiff's complaint sufficiently states a cause of action under this statute: it alleges that defendant required and recorded plaintiff's address and telephone number as a condition to his online purchases of electronically downloadable products, and that defendant's actions were not otherwise permitted by the statute. In holding to the contrary, the majority relies on speculation and debatable factual assumptions to carve out an expansive exception to section 1747.08 that leaves online retailers free to collect and use the personal identification information of credit card users as they wish.

I.

Because this case comes to us on a demurrer, "we review the allegations of the operative complaint for facts sufficient to state a claim for relief. In doing so, we treat the demurrer as admitting all material facts properly pleaded. ' "Further, we give the complaint a reasonable interpretation, reading it as a whole and its parts in their context." ' [Citations.]" (*C.A. v. William S. Hart Union High School Dist.* (2012) 53 Cal.4th 861, 866.)

---

1 All further statutory references are to this code unless otherwise indicated.

Plaintiff seeks statutory penalties for defendant's alleged violations of section 1747.08, a statute enacted to " 'protect the personal privacy of consumers who pay for transactions with credit cards.' " (*Pineda v. Williams-Sonoma Stores, Inc.* (2011) 51 Cal.4th 524, 534 (*Pineda*); see *Archer v. United Rentals, Inc.* (2011) 195 Cal.App.4th 807, 827.) Subdivision (a) of section 1747.08 (section 1747.08(a)) provides: "Except as provided in subdivision (c), no person, firm, partnership, association, or corporation that accepts credit cards for the transaction of business shall do any of the following: [¶] . . . [¶] (2) Request, or require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to provide personal identification information, which the . . . corporation accepting the credit card . . . records upon the credit card transaction form or otherwise." For purposes of the statute, subdivision (b) of section 1747.08 (section 1747.08(b)) defines "personal identification information" as "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number." Subdivision (c) of section 1747.08 (section 1747.08(c)) states in pertinent part that section 1747.08(a) does not apply if, among other things, the person or entity accepting the credit card is contractually obligated to provide personal identification information in order to complete the credit card transaction (§ 1747.08(c)(3)(A)), or is obligated by federal or state law or regulation to collect and record such information (§ 1747.08(c)(3)(C)), or requires the information "for a special purpose incidental but related to the individual credit card transaction, including, but not limited to, information relating to shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders" (§ 1747.08(c)(4)).

Plaintiff's complaint contains the following allegations, some of which are based on information and belief. Plaintiff purchased media downloads from defendant on various occasions in 2010. Defendant's Web site would not permit plaintiff to obtain his purchases by credit card unless he first provided his telephone number and address. Such

personal information was not required by the credit card processing company to complete the transaction. But even if the credit card processing company required a valid billing address and credit card identification number, under no circumstance would plaintiff's telephone number be required to complete the purchase transaction. Defendant "records each consumer's personal information, including, but not limited to a telephone number and address, in line with each credit card transaction, and keeps records of such personal information." Defendant "is not contractually obligated to provide a consumer's telephone number and/or address in order to complete the credit card transaction," nor is defendant required to record such personal information under federal or state law or regulation or for any incidental purpose such as shipping.

Assuming the truth of these allegations, they establish that defendant required and recorded plaintiff's personal identification information when plaintiff used his credit card to make purchases, and that none of the exceptions listed in section 1747.08(c) applied, at least as to some of the information taken. Accordingly, plaintiff's complaint adequately states a cause of action for violation of section 1747.08.

II.

The majority implicitly agrees that defendant's conduct falls within the plain terms of section 1747.08(a). (See maj. opn., *ante*, at p. 7.) The majority holds, however, that plaintiff was not entitled to protection of his personal identification information because online credit card purchases of electronically downloadable products are categorically exempt from the statute's application. (Maj. opn., *ante*, at pp. 2, 12, 26.) Although recognizing this is a question of statutory construction, the majority reaches a result that is contrary to the terms, purpose, and legislative history of section 1747.08.

The rules governing statutory construction are uncomplicated and settled. When construing a statute, our goal "is to ascertain the intent of the lawmakers so as to effectuate the purpose of the statute." (*Estate of Griswold* (2001) 25 Cal.4th 904, 910.) We look first to the language of the statute, mindful that the words " ' "should be given

the meaning they bear in ordinary use. [Citations.]" ' " (*Dicampli-Mintz v. County of Santa Clara* (2012) 55 Cal.4th 983, 992.) Judicial construction, and judicially crafted exceptions, are appropriate only when literal interpretation of a statute would yield absurd results or implicate due process. (*Cassel v. Superior Court* (2011) 51 Cal.4th 113, 124; *In re C.H.* (2011) 53 Cal.4th 94, 107.) Otherwise, a statute "must be applied in strict accordance with [its] plain terms." (*Cassel*, at p. 124.) " ' "Only when the statute's language is ambiguous or susceptible of more than one reasonable interpretation, may the court turn to extrinsic aids to assist in interpretation." [Citation.]' " (*In re Ethan C.* (2012) 54 Cal.4th 610, 627.) Under no circumstance, however, may the court " 'under the guise of construction, rewrite the law or give the words an effect different from the plain and direct import of the terms used.' [Citation.]" (*Dicampli-Mintz*, at p. 992.) In this regard, the court " ' "must assume that the Legislature knew how to create an exception if it wished to do so . . . . [Citation.]" ' " (*Ibid.*)

Section 1747.08(a) contains language broadly stating that "no person, firm, partnership, association, or corporation that accepts credit cards" shall request or require the cardholder to provide personal identification information and cause it to be recorded. Section 1747.08(a) flatly states its proscriptions shall apply "[e]xcept as provided in subdivision (c)." Section 1747.08(c) lists various business-related reasons for which the requesting, requiring, or recording of personal identification information does not violate section 1747.08(a). Virtually all of these exceptions could apply either in online credit card purchase transactions, or in face-to-face purchase transactions occurring at brick-and-mortar establishments.[2] There is nothing in subdivision (a), (b), or (c) suggesting a

---

[2] E.g., section 1747.08(c)(1) (credit card used as deposit to secure payment); section 1747.08(c)(2) (cash advance transactions); section 1747.08(c)(3)(A) (personal identification information contractually required to complete the credit card transaction); section 1747.08(c)(3)(C) (information required by federal or state law or regulation);

(footnote continued on next page)

literal construction of section 1747.08 would implicate due process or result in absurd consequences.

Subdivision (d) of section 1747.08 (section 1747.08(d)) lists one additional proviso to the statute's application. It clarifies that no person or entity subject to the statutory proscriptions is prohibited "from requiring the cardholder, as a condition to accepting the credit card as payment in full or in part for goods or services, to provide reasonable forms of positive identification," such as a driver's license or other form of photo identification, "provided that none of the information contained thereon is written or recorded." (*Ibid.*) Section 1747.08(d) further provides that if the cardholder uses a credit card number to pay for the transaction without making the "card available upon request to verify the number, the cardholder's driver's license number or identification card number may be recorded." Unlike section 1747.08(c), section 1747.08(d) makes no allowance for the recording of a cardholder's address or telephone number. Instead, it permits retailers to require presentment of reasonable forms of positive identification, and when the credit card itself is not made available, to write down a license number or other photo identification card number.

Had section 1747.08(d) been written to *require* retailers to demand and visually inspect a cardholder's driver's license or other photo identification card as a condition of accepting a credit card, then one might reasonably infer the proscriptions of section 1747.08(a) could have no application to online credit card transactions given the asserted impossibility of complying with the statutory commands. As it stands, however, section 1747.08(d) is merely permissive and thus poses no barrier or difficulty to an online

---

(footnote continued from previous page)

section 1747.08(c)(4) (information necessary for special purpose incidental but related to the individual credit card transaction, such as shipping, servicing, or installation).

retailer's compliance with the entirety of the statute. Moreover, section 1747.08(d) does not, in any event, permit the recording of addresses or telephone numbers for card-not-present purchases at brick-and-mortar establishments.[3] Finally, there is nothing in this or any other subdivision in section 1747.08 that requires retailers, of any sort, to accept credit cards for purchases when they deem the risk of fraud or identity theft unacceptable. Hence, the statutory terms reflect a legislative determination that heightened privacy interests in personal information such as addresses and telephone numbers outweigh the necessity or usefulness of such information for any supposed fraud prevention purpose in card-not-present transactions.

In sum, applying section 1747.08(a) to online retailers flows logically from the plain meaning of the statute, is not absurd, and fully promotes the legislative objective to protect the personal identification information of credit card users against exploitation by retailers. Under these circumstances, we are bound to construe section 1747.08 "in strict accordance with [its] plain terms." (*Cassel v. Superior Court*, *supra*, 51 Cal.4th at p. 124.)

Undeterred by the plain language of section 1747.08, the majority emphasizes the substantive provisions of section 1747.08 were first enacted "almost a decade before online commercial transactions became widespread." (Maj. opn., *ante*, at p. 6.) From this the majority posits "[w]e cannot assume that the Legislature, had it confronted a type of transaction in which the standard mechanisms for verifying a cardholder's identity were not available, would have made the same policy choice as it did with respect to transactions in which it found no tension between privacy protection and fraud prevention." (*Id*. at p. 11.) The majority views section 1747.08(d) as demonstrating "the

---

3 Consistent with this conclusion, the majority concedes "section 1747.08(d) does not permit Apple to collect a billing address in the course of an online transaction." (Maj. opn., *ante*, at p. 14.)

Legislature's intent to permit retailers to use and even record personal identification information when necessary to combat fraud and identity theft" (maj. opn., *ante*, at p. 12), but finds such provision has no application to online transactions because "an online retailer cannot visually inspect the credit card, the signature on the back of the card, or the customer's photo identification" (*ibid.*). According to the majority, the Legislature did not intend for section 1747.08 to apply to online credit card transactions, "[b]ecause the statutory scheme provides no means for online retailers . . . to protect against credit card fraud . . . ." (Maj. opn., *ante*, at pp. 15-16.)

Even assuming resort to extrinsic aids is appropriate, the majority bases its construction of section 1747.08 on two critical, but flawed, assumptions. The first assumption is that the legislative intent underlying the statute is not limited to protecting consumer privacy, but also extends to protecting consumers *and retailers* from "undue risk of fraud." (Maj. opn., *ante*, at p. 10.) The second is a factual assumption — that the personal identification information defendant allegedly demanded and recorded here, i.e., cardholder addresses and telephone numbers, are "necessary to combat fraud and identity theft" in online credit card transactions. (Maj. opn., *ante*, at p. 12.) As demonstrated below, there is no legislative source to support the former assumption, and no factual basis in the complaint or judicially noticeable materials to support the latter.

The language of section 1747.08 reflects its underlying purpose is to safeguard consumer privacy by prohibiting any person or entity from requiring, requesting, or recording personal identification information when such information is unnecessary to complete a credit card transaction. That section 1747.08 has no primary antifraud purpose is demonstrated by its terms: the statute does not purport to require retailers to take antifraud measures; nor does it condition its protections on a retailer's ability to protect against credit card fraud.

The legislative history is in accord. As we recently explained in our unanimous opinion in *Pineda, supra*, 51 Cal.4th 524, the Legislature enacted the predecessor to

section 1747.08 in order "to provide robust consumer protections by prohibiting retailers from soliciting and recording information about the cardholder that is unnecessary to the credit card transaction." (*Pineda*, at p. 536.) The precise concern prompting the Legislature's action was that retailers were acquiring this additional but unnecessary personal information " 'for their own business purposes — for example, to build mailing and telephone lists which they can subsequently use for their own in-house marketing efforts, or sell to direct-mail or tele-marketing specialists, or to others.' " (*Id*. at pp. 534-535.)[4]

Significantly, neither *Pineda* nor the legislative history itself mentions a legislative intent to protect retailers from undue risk of fraud. That is not surprising, because the Legislature enacted the consumer privacy protections with the understanding that a retailer was *not* put at risk of loss from fraud, so long as the retailer complied with the card issuer's operating procedures for credit card transactions. (See Dept. of Consumer Affairs, Enrolled Bill Rep. on Assem. Bill No. 2920 (1989-1990 Reg. Sess.) July 21, 1990, p. 2 (Enrolled Bill Report) ["the credit card issuer guarantees payment to the retailer if proper procedures are followed (even if the consumer does not pay the credit card company)"].) Thus, notwithstanding counsel's factual assertions at oral argument (see maj. opn., *ante*, at p. 13), the relevant legislative history undercuts the majority's theory that retailer protection was a principal objective of section 1747.08.

Although the legislative history discloses a concern about credit card fraud, such concern pertained specifically to the circumstance that recordation of unnecessary personal information posed a fraud risk to the *cardholder*, not the retailer, because the information could be used "in conjunction with the credit card number to order goods by

---

4 At this stage in the proceedings, defendant has not filed an answer or given an explanation as to why it collects the addresses and telephone numbers of cardholders and what it does with such information.

phone or mail and charge it to the cardholder" or "to apply for other sources of credit in the cardholder's name." (Enrolled Bill Rep., *supra*, at p. 2 ["By the time the subterfuge is discovered, the consumer's credit and credit history could be severely damaged."].) Yet, despite this awareness in 1990 that credit cards were being used to "order goods by phone or mail" (*ibid.*), the Legislature provided no exception to section 1747.08's applicability for mail order and telephone order (MOTO) purchases.

Like retailers that accept credit cards for online purchases, those that accept credit cards for MOTO transactions have no opportunity to visually inspect a driver's license or other forms of photo identification as allowed by section 1747.08(d). That online and MOTO retailers appear similarly situated in this regard renders implausible the majority's theory that the Legislature would not have intended "section 1747.08(a)'s prohibitions to apply to [online] transactions despite the unavailability of section 1747.08(d)'s safeguards." (Maj. opn., *ante*, at p. 12.) The majority offers no reason, cogent or otherwise, why the Legislature, having enacted section 1747.08's privacy protections without an exception for MOTO transactions, would not also contemplate applicability of the statutory protections to other card-not-present transactions such as those occurring online.

The majority additionally views section 1747.08(d) as demonstrating "the Legislature's intent to permit retailers to use and even record personal identification information *when necessary to combat fraud and identity theft*." (Maj. opn., *ante*, at p. 12, italics added.) But again, neither the language nor the history of section 1747.08 indicates this to be the case, and we may assume the Legislature knew how to create such an exception had it intended to do so. (*Dicampli-Mintz v. County of Santa Clara*, *supra*, 55 Cal.4th at p. 992.) In any event, this matter comes to us on a demurrer, and there is nothing in the record from which we may discern that both cardholder addresses and telephone numbers are necessary to combat online fraud and identity theft. Because the necessity issue is a factual one that appears open to reasonable debate, it seems a

particularly inappropriate basis for sustaining a demurrer and judicially limiting the plain reach of section 1747.08.

Finally, the majority views the enactment of the California Online Privacy Protection Act of 2003 (Bus. & Prof. Code, § 22575 et seq.; COPPA) as signifying that "when the Legislature intends to address online transactions, it does so unambiguously." (Maj. opn., *ante*, at p. 23.) This conclusion appears incongruous with the majority's express acknowledgement that courts do not rely on "wooden construction of [statutory] terms" when "construing statutes that predate their possible applicability to new technology." (*Id*. at pp. 7-8; see also *id*. at p. 8 [" 'Drafters of every era know that technological advances will proceed apace and that the rules they create will one day apply to all sorts of circumstances they could not possibly envision.' "]; e.g., *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423 [holding that petitioners' Web sites qualify as periodical publications under the California reporter's shield law].)

COPPA's disclosure requirements do nothing to restrict an online retailer's use of a consumer's personal identification information; nor do they prevent the sharing or sale of such information. True, consumers who are not satisfied with a retailer's posted privacy policy may always decline to purchase the retailer's products. But today's decision deprives consumers of section 1747.08's additional safeguards, which in contrast to COPPA make retailers bear the burden of privacy protection. The majority's interpretation of section 1747.08 foists this burden onto consumers, leaving consumers unable to freely use their credit cards for online purchases without surrendering their personal identification information.

III.

Pure and simple, a literal interpretation of section 1747.08 that includes online credit card transactions within its scope promotes the Legislature's intent to scrupulously protect the privacy of credit card users and is not absurd. This interpretation is also consistent with our unanimous opinion in *Pineda, supra*, 51 Cal.4th 524, which

recognized that section 1747.08's "overriding purpose was to 'protect the personal privacy of consumers who pay for transactions with credit cards' " (*Pineda*, at p. 534) and "to provide robust consumer protections by prohibiting retailers from soliciting and recording information about the cardholder that is unnecessary to the credit card transaction" (*id*. at p. 536). I see no reason to depart from *Pineda*'s conclusion that protecting consumer privacy is the "evident purpose of the statute." (*Ibid*.)

If defendant and other retailers wish to demonstrate that section 1747.08 is ill-suited to the online industry because the collection of personal identification information presently serves a valid antifraud function, they may make their case to the Legislature. Unlike this court, the Legislature would have the opportunity to take evidence on the issue, to weigh the antifraud utility of such information against the potential of its misuse and exploitation, and, if appropriate, to craft a balanced statutory exception that preserves the privacy interests of consumers while responding to legitimate antifraud and identity theft concerns of online retailers. Unfortunately, today's decision relies on speculation and debatable factual assumptions to wholly strip online credit card users of the statutory consumer privacy protections, leaving online retailers free to require personal identification information as a condition of credit card acceptance and to use such information for whatever purposes they wish. Rather than fashioning such an expansive exception to section 1747.08, this court should have given effect to its plain terms and left it to the Legislature to address defendant's claims of competing policy interests.

BAXTER, J.

WE CONCUR:

KENNARD, J.
JONES, J.*

---

* Presiding Justice, Court of Appeal, First Appellate District, Division Five, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

See next page for addresses and telephone numbers for counsel who argued in Supreme Court.

Name of Opinion Apple, Inc. v. Superior Court

Unpublished Opinion
Original Appeal
Original Proceeding XXX
Review Granted
Rehearing Granted

Opinion No. S199384
Date Filed: February 4, 2013

Court: Superior
County: Los Angeles
Judge: Carl J. West

Counsel:

Gibson, Dunn & Crutcher, Daniel M. Kolkey, S. Ashlie Beringer, Austin V. Schwing, Timothy W. Loose and Molly Cutler for Petitioner.

Willenken Wilson Loh & Delgado, William A. Delgado and Eileen M. Ahern for Ticketmaster LLC as Amicus Curiae on behalf of Petitioner.

Drinker Biddle & Reath, Sheldon Eisenberg and Kristopher Davis for eHarmony, Inc., as Amicus Curiae on behalf of Petitioner.

Sidley Austin, Mark E. Haddad, David R. Carpetner; Paul Hastings, Thomas P. Brown and Kristin M. Hall for eBay, Inc., Walmart.com USA, LLC, California Retailers Association and NetChoice as Amici Curiae on behalf of Petitioner.

No appearance for Respondent.

Schreiber & Schreiber, Edwin C. Schreiber and Eric A. Schreiber for Real Party in Interest.

Counsel who argued in Supreme Court (not intended for publication with opinion):

Daniel M. Kolkey
Gibson, Dunn & Crutcher
555 Mission Street, Suite 3000
San Francisco, CA 94105
(415) 393-8200

Eric A. Schreiber
Schreiber & Schreiber
16501 Ventura Boulevard, Suite 401
Encino, CA 91436-2068
(818) 789-2577