No. S199384

IN THE SUPREME COURT OF CALIFORNIA

APPLE INC., a California corporation,

Petitioner,

vs.

SUPERIOR COURT OF THE COUNTY OF LOS ANGELES,

Respondent,

DAVID KRESCENT,

individually and on behalf of a class of persons similarly situated,

Real Party in Interest.

Court of Appeal Case No. B238097
Los Angeles Superior Court Civil Case No. BC463305
The Honorable Carl J. West, Presiding

APPLE INC.'S REPLY BRIEF ON THE MERITS

GIBSON, DUNN & CRUTCHER LLP
DANIEL M. KOLKEY (SBN #79102)
S. ASHLIE BERINGER (SBN #263977)
AUSTIN V. SCHWING (SBN # 211696)
TIMOTHY W. LOOSE (SBN #241037)
MOLLY CUTLER (SBN #261192)
555 Mission Street, Suite 3000
San Francisco, CA 94105
Telephone: (415) 393-8200
Facsimile: (415) 393-8306

Attorneys for Petitioner
APPLE INC.

No. S199384

IN THE SUPREME COURT OF CALIFORNIA

APPLE INC., a California corporation,

Petitioner,

vs.

SUPERIOR COURT OF THE COUNTY OF LOS ANGELES,

Respondent,

DAVID KRESCENT,

individually and on behalf of a class of persons similarly situated,

Real Party in Interest.

Court of Appeal Case No. B238097
Los Angeles Superior Court Civil Case No. BC463305
The Honorable Carl J. West, Presiding

APPLE INC.'S REPLY BRIEF ON THE MERITS

GIBSON, DUNN & CRUTCHER LLP
DANIEL M. KOLKEY (SBN #79102)
S. ASHLIE BERINGER (SBN #263977)
AUSTIN V. SCHWING (SBN # 211696)
TIMOTHY W. LOOSE (SBN #241037)
MOLLY CUTLER (SBN #261192)
555 Mission Street, Suite 3000
San Francisco, CA 94105
Telephone: (415) 393-8200
Facsimile: (415) 393-8306

Attorneys for Petitioner
APPLE INC.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page

Statutes

Other Authorities

I. INTRODUCTION

In an effort to argue that Civil Code section 1747.08 ("section 1747.08") of the Song-Beverly Credit Card Act ("Song-Beverly Act" or "Act") applies to online transactions, Plaintiff's Answer Brief propounds arguments that are irrelevant, miss the point, or are utterly contrary to fundamental rules of statutory construction:

1. Plaintiff begins with an argument that "since it is Plaintiff who prevailed on demurrer, Apple carries a heavy burden because it is presumed all facts alleged in the complaint are true." (Ans., p. 3.) However, Plaintiff's factual allegations cannot possibly control the proper interpretation of the statute.

2. Plaintiff's brief wholly fails to address Apple's point that the fraud prevention provisions in section 1747.08, which allow retailers to verify a customer's identity by inspecting the customer's credit card and photo identification, are not suited to online transactions.

3. Plaintiff's brief places great emphasis on the contention that "while the May 2011 version" of a 2011 amendment to the Act "ultimately failed to make the cut . . . the Legislature was more than clear [in that failed amendment] . . . that existing law currently applies to Internet businesses . . . ." (Ans., p. 21.) But "'[t]he declaration of a later Legislature is of little weight in determining the relevant intent of the

Legislature that enacted the law.'" (*Lolley v. Campbell* (2002) 28 Cal.4th 367, 379.) A fortiori, a declaration in a *proposed but failed amendment* of a *later* Legislature is entitled to *no* weight regarding the *prior* Legislature's intent. (*People v. Mendoza* (2000) 23 Cal.4th 896, 921.)

4. While acknowledging that "[t]he Legislature in 1991 [when section 1747.08 of the Act was enacted] could not foresee the existence of computer and Interne[t] based commerce" (Ans., p. 13), Plaintiff expends six pages on the proposition that "cases throughout the country have had no problem applying existing laws and rules to Internet based businesses . . . ." (*Id.*, p. 23.) However, whether any particular law passed *before* the Internet age should be applied *to* the Internet requires the Court to "'ascertain the intent of the lawmakers'" with respect to that law. (*People v. Cruz* (1996) 13 Cal.4th 764, 774-775.) And here, the text of section 1747.08 reflects a legislative intent to effectuate a delicate policy balance between privacy protection and fraud prevention that cannot be applied to online transactions. (Opening Br., pp. 13–14.)

5. In order to contend that the application of the Act to online commercial transactions would not promote credit card fraud (against which the statute affords protections to brick-and-mortar retailers), Plaintiff repeatedly and evasively – without any analysis – makes the contention that "[i]t is *possible* that credit card verification would fall under the exception to the Act provided in subsection (c)(3)(A) (required by contract) or (c)(4)

(required for a special purpose incidental but related to the transaction), however these exceptions are factual questions." (Ans., pp. 29-30, italics added; accord, Ans., pp. 12–13, 33–35, 48–50.) This is a complete turnabout from Plaintiff's immediately prior pleading in this Court where he asserted that Apple "does not, and did not have the right to collect personal information, even for the purposes of theft or fraud protection." (Answer to Petition for Review, p. 7.) Nor is Plaintiff's suggestion of the "possibility" of a defense reliable, since he never supports his speculation with any analysis. In any event, section 1747.08 does not contain an express provision that allows e-retailers the right to verify the cardholder's identity like the express provisions which authorize brick-and-mortar retailers to verify the cardholder's identity. And Plaintiff's position that the need for any personal identification information is a "factual question" (to presumably be determined by a jury) would engender the very uncertainty regarding verification and the use of personal information that the Act was meant to avoid.

6. Finally, in attempting to rebut Apple's position that interpreting the Act to apply to online commercial transactions will force every online retailer to apply California law, regardless of the customer's residence – in violation of the due process and dormant commerce clauses – because an online retailer cannot know that a customer is from California until the e-retailer has violated the Act by requesting the customer's address, Plaintiff

argues that "Apple . . . is in no position to complain . . . [because] it is a California corporation . . . and . . . its contracts contain a choice of law clause . . . ." (Ans., p. 42.) However, the issue before the Court is not the Act's application to any particular party, but whether the Act should be construed to apply to online commercial transactions in general.

In sum, nothing in Plaintiff's Answer Brief rebuts Apple's critical points that the application of section 1747.08 to online transactions (i) would conflict with its statutory language and the delicate legislative balance between privacy protection and fraud prevention, (ii) would threaten to produce unintended and absurd results, including the facilitation of fraud against e-retailers who have no way to confirm the customer's right to use the credit card, (iii) cannot be reconciled with the statute's legislative history (since the Legislature did not consider the Act's application to online transactions or the different policy considerations associated therewith), and (iv) would construe the statute in a manner which raises serious questions regarding its constitutionality under the due process and commerce clauses.[1]

[1] If the Court were to rule that section 1747.08 applies to online transactions, Apple reserves the right to argue that its alleged conduct is permitted under the Act.

II. ARGUMENT

A. Section 1747.08's Text Reveals That The Legislature Never Contemplated Applying It To Online Transactions.

As described in Apple's opening brief, the text and structure of section 1747.08, read as a whole, reflects a legislative intent to effectuate a delicate policy balance between privacy protection and fraud prevention in the context of brick-and-mortar retail transactions. (Opening Br. pp. 13-23.) On the one hand, the statute prohibits merchants' collection of personal information that is not necessary to an in-person sales transaction. On the other, it authorizes the retailer to require the customer to provide his credit card and photo identification, and if the credit card is not made available, to record the cardholder's driver's license or identification card number on the credit card transaction form. (Civ. Code §§ 1747.08, subds. (a), (d).)

Plaintiff's Answer utterly fails to address this argument and indeed, ignores altogether those provisions authorizing brick-and-mortar retailers to inspect a credit card and reasonable forms of positive identification, which cannot be implemented online. Rather, Plaintiff concedes that the tools available to online merchants for credit card authorization are "*not the same tools* as those when a card is physically handed to the merchant." (Ans., p. 12, italics added.) But he *never* identifies what forms of information an e-retailer may seek to verify the cardholder's identity under section 1747.08,

only vaguely offering that "Plaintiff does not suggest that on-line merchants cannot ask for the information which is actually required to verify that the credit card is valid and not stolen . . . ." (*Ibid.*)

Having failed to address the impossibility of applying section 1747.08's policy balance to online transactions, Plaintiff argues that the statute's lead-in clause, providing that no person that accepts credit cards shall record personal identification information, "must be read as an all-inclusive prohibition on every business regardless of the form of the transaction," including online transactions. (Ans., p. 9.) The multiple flaws in Plaintiff's argument, however, are that (1) the breadth of a single *lead-in clause* cannot control the *entire statute's* interpretation, because the Legislature had no reason to *expressly* limit section 1747.08's reach, given that online transactions did not exist in 1990–1991 (as Plaintiff concedes (Ans., p. 9)), (2) the policy balance expressed in the statute cannot be applied to online transactions, and (3) the other language used in the statute shows that the Legislature never intended section 1747.08 to apply to online transactions. (See Opening Br., pp. 15–21.) In short, the language of the statute evidences a particular factual context for the transaction, which is not present in a virtual transaction in which no human interaction exists and no card or photo identification can be presented.

Specifically, Apple's opening brief explained that section 1747.08's references to (1) the customer's "writ[ing]" personal identification

information upon the credit card transaction form, including a "form which contains preprinted spaces," and (2) the cardholder's "presentation" of the credit card (among other phrases) reflected an intent to apply the statute to in-person transactions or those in which the card is physically presented. (Opening Br., pp. 15–21.) Plaintiff protests that those phrases "do not evidence an intent to exclude electronic commerce, rather, those are the words in effect for the type of commerce in existence in 1991." (Ans., p. 10.) But this simply reinforces Apple's point that the statute was written in contemplation of in-person transactions – the type of credit card transaction in existence in 1990-1991.

Plaintiff also contends that "the language used[,] such as prohibiting a retailer from writing or 'otherwise recording' the information[,] evidences an intent to prohibit all forms of recording consumer information, be it written, typed or digitally recorded." (Ans., pp. 10–11.)

To the contrary, the statute's distinction between the *cardholder* who is prohibited from being required "to write any personal identification information" (§ 1747.08, subd. (a)(1)) and the *retailer* who is prohibited from "writ[ing], caus[ing] to be written, or otherwise record[ing]" that information (*id.*, subd. (a)(2)) confirms that the Legislature envisioned an in-person transaction: The statute contemplated that a cardholder would only be requested to "write" information upon the credit card transaction form. (*Id.*, subd. (a)(1), (a)(3).) In contrast, the retailer was envisioned to

write or "otherwise record" information, such as through the use of typing or photocopying. In short, the Legislature's deliberate decision *not* to use the phrase "otherwise record" in subdivisions (a)(1) and (a)(3) – which impose restrictions on the form in which information may be requested from *customers* – confirms that the provisions directed at customers do not include other means of "record[ing]" personal information, such as the electronic entry of numbers on a keypad or screen.

Plaintiff suggests that California's Uniform Electronic Transactions Act ("CUETA") "permits a written signature or information to be virtually any electronic mark, and further defines 'record' as information that can be inscribed on any tangible medium . . . ." (Ans., p. 10, fn. 3.) But a statutory definition in an entirely *separate* and *subsequently* enacted law has no bearing on the plain meaning of the words, "record" or "write," in section 1747.08.

Despite the Act's limitation of the definition of "retailer" to a person who furnishes goods "upon presentation of a credit card by a cardholder" (§1747.02, subd. (e)), Plaintiff attempts to blur the distinction between in-person and online transactions by arguing that "a credit card can be 'presented' by and through its numbers, expiration date and name of card holder exactly as if it was physically presented. The effect is the same, a merchant is presented with either a plastic card . . . or the retailer is

presented with the card number and other card information which is submitted to the credit card company for authorization." (Ans., p. 11.)

But Plaintiff's suggestion that "the effect" of furnishing raw credit card numbers is somehow "the same" as "present[ing]" a physical credit card is untenable. Section 1747.08's language does not envision a retailer processing a credit card number without ever reviewing the actual credit card or at least a driver's license or identification card. Indeed, the Legislature specifically provided that where the customer's credit card is not made available, the retailer may record additional personal information appearing on the customer's driver's license or identification card – a protection not available to the online retailer, who cannot inspect forms of identification (or determine whether the credit card is available). (§1747.08, subd. (d).) There is no reason to believe the Legislature would have intended to force online merchants to undertake the risks of a transaction where no credit card is physically presented without the benefit of these enacted safeguards.

Plaintiff also argues that "[a]n Internet transaction is nothing more than a technologically advanced remote transaction," and that "[t]he Legislature was no doubt aware of fraud concerns associated with remote transactions (for example, telephone or facsimile orders) which existed when the Act was passed, and could have exempted such transactions, but chose not to do so." (Ans., p. 9.) However, Plaintiff cites no authority for

his assumption that the Act applies to these "remote transactions." Indeed, not a single case has applied the Song-Beverly Act to telephone or fax purchases.

Furthermore, even if such transactions are covered by section 1747.08 – an issue the Court need not reach – the risks and policy considerations associated with online transactions are materially different from those arising out of telephone and fax orders, which can be largely accommodated by the provisions of section 1747.08. Telephonic communications are person-to-person transactions, which allow requests for verification, even if the answers are not written down. (See Opening Br., p. 32, fn. 10.) More significantly, unlike online transactions, which often involve digital downloads, virtually all telephonic or fax transactions which involve credit card payments also involve the shipping or installation of the purchased merchandise, in which case subdivision (c)(4) would exempt the transaction from the prohibition against recording the customer's address. It is therefore unsurprising that those brick-and-mortar merchants who take credit card information by telephone or fax had no motivation to seek language specifically exempting such telephonic or fax transactions from section 1747.08 at the time of its enactment (even assuming it applies to them). In contrast, the anonymous nature of the virtual world and the absence of any human interaction present a significant risk of fraud, absent the ability to collect personal information.

B. Application Of A Broadly Written Statute To New Technologies Requires A Searching Evaluation Of Legislative Intent.

Plaintiff argues that "the mere fact that the Legislature could not, in 1991, possibly have even dreamed of the significance of Internet commerce today, does not mean that such transactions are not covered by the Act." (Ans., p. 28.) He contends that "cases throughout the country have had no problem applying existing laws and rules to Internet based businesses . . . ." (*Id.*, p. 23.)

However, whether an earlier enacted law should be applied to Internet-based businesses is a matter of that particular law's legislative intent, which, after all, is the ultimate determinant of any statutory interpretation. (See *People v. Cruz*, *supra*, 13 Cal.4th 764, 774-775.) And where the language and policy expressed in the text of a law demonstrate that it should *not* be applied to an unforeseen technological advance, such an application would be contrary to the goal of statutory construction, which is "to 'ascertain the intent of the lawmakers so as to effectuate the purpose of the law.'" (*Ibid.*)

Thus, when a new technology raises *new policy concerns*, the courts have found that they are *not* "the proper bod[ies] to determine whether and how to incorporate this technology." (*Ni v. Slocum* (2011) 196 Cal.App.4th 1636, 1653; see also *People v. Gerber* (2011) 196 Cal.App.4th 368, 379,

386 [declining to extend child pornography statutes to the superimposed photographs of children's faces onto sexually explicit images of adults].)

For example, in *Ni v. Slocum*, *supra*, 196 Cal.App.4th at pages 1650–1651, the Court of Appeal concluded that an electronic signature could not be used to endorse an initiative petition under the Elections Code because the Legislature had never considered the policy issues and opportunities for fraud that would arise from construing the statute to allow for electronic signatures:

> It is most persuasive to us that the Legislature did not anticipate the use of electronic signatures when it drafted the statute and has since taken no action that can be construed as approving them for this purpose. When the Legislature first required voters personally to affix information to an initiative petition in 1933, electronic signatures were not even a twinkle in the eyes of Messrs. Hewlett and Packard. Necessarily, the legislators who enacted the language intended that voters would write directly on a paper copy of the petition, since there was no other means for a voter personally to affix information to a petition.
>
> * * *
>
> Evaluating the policy issues arising from the use of the Internet for petition endorsement and accommodating this technology within the existing signature validation process is outside the proper scope of our task. Because there is no evidence the Legislature has ever considered these questions, let alone affirmatively approved the use of electronic signatures in connection with initiative petitions, we should hesitate to mandate their acceptance by judicial fiat.

(*Ibid.*)

In contrast, in the cases that Plaintiff cites at pages 24-25 of his Answer Brief as evidence of previously enacted provisions that were

applied to new technologies, there was no meaningful distinction between the traditional and online conduct with respect to the policy at issue. (E.g., *Snowney v. Harrah's Entertainment, Inc.* (2005) 35 Cal.4th 1054, 1065 [Nevada casino's use of its website advertising and reservation services to specifically target residents of California established a substantial connection with California for purposes of California's long-arm statute]; *Vo v. City of Garden Grove* (2004) 115 Cal.App.4th 425, 434 [for purposes of the First Amendment, there is "no rationale" to treat cafés offering Internet access differently from traditional businesses]; *Brookfield Communications, Inc. v. West Coast Entertainment Corp.* (9th Cir. 1999) 174 F.3d 1036, 1066 [firm's use of a competitor's trademark in the domain name of its web site creates the very type of confusion the trademark laws are designed to prevent]; *BigStar Entertainment, Inc. v. Next Big Star, Inc.* (S.D.N.Y. 2000) 105 F.Supp.2d 185, 207 [same].)

In contrast, here, there is a significant difference between online and brick-and-mortar transactions when it comes to determining what information must be transmitted to verify the cardholder's identity and to guard against credit card fraud because in an online transaction, neither the credit card, the cardholder, nor the cardholder's photo identification can be viewed. Moreover, under section 1747.08, where the cardholder does *not* make the credit card available or where the card must be inserted in a device outside of merchant's presence, personal identification information

can be recorded. (§1747.08, subds. (c)(3)(B), (d).) But section 1747.08 was not tailored to make this authorization available for online transactions, although the credit card is not made available in those types of transactions either. In short, the proper policy balance between fraud prevention and privacy protection in the unique context of online transactions must be determined by the Legislature, not the judiciary, in the first instance. (*Ni v. Slocum*, *supra*, 196 Cal.App.4th at p. 1653.)

Finally Plaintiff argues that *Powers v. Pottery Barn, Inc.* (2009) 177 Cal.App.4th 1039, shows that "uses of technology can, in fact, violate the [Song-Beverly] Act, even though not specifically mentioned therein." (Ans., p. 27.) However, *Powers* merely held that the CAN-SPAM Act (15 U.S.C. § 7701 et seq.) *did not preempt* plaintiff's claim that a retailer improperly asked for her e-mail address under the Song-Beverly Act because "Song-Beverly does not expressly regulate any Internet activity, let alone use of 'electronic mail to send commercial messages.'" (*Id.* at p. 1045.)

C. Nothing In The Act's 2011 Amendment Implies That Online Transactions Are Subject To The Act.

Plaintiff argues that the 2011 amendment to section 1747.08, enacted by Assembly Bill No. 1219, "along with prior drafts thereof[,] make the Legislature's intent that the Act applies to remote transactions unmistakably clear." (Ans., p. 14; capitalization omitted.) Plaintiff's

contention that the *2011 amendment*, and a prior rejected amendment thereto, reflects the Legislature's intent in enacting section 1747.08 in *1990-1991* is contrary to the rules of statutory construction and common sense: "'The declaration of a later Legislature is of little weight in determining the relevant intent of the Legislature that enacted the law.'" (*Lolley v. Campbell*, *supra*, 28 Cal.4th at p. 379.)

Assembly Bill No. 1219 authorizes gas stations to collect ZIP codes – a form of personal identification information – at automated gas pumps. (§1747.08, subd. (c)(3)(B); see Opening Br., pp. 36-40.) That amendment did nothing to expand the reach of the Song-Beverly Act to cover online transactions. Indeed, even Plaintiff admits that Assembly Bill No. 1219 "ultimately only added the gas station exemption and nothing more[.]" (Ans., p. 19.)

Yet, Plaintiff argues that "because the Legislature specifically granted gas stations an exemption to use personal information solely to verify credit cards . . . , it stands to reason that because no other business received this exemption, the mere fact that a transaction is remote does not provide a *carte blanche* exemption to the Act's requirements. There is no meaningful difference between swiping the magnetic strip at an unattended fuel pump, and typing a credit card number, expiration date, cardholder name and potentially a CCID." (Ans., pp. 14–15.)

First, there are meaningful differences between automated gas pump transactions and online transactions: In an automated gas pump transaction, the cardholder has physical possession of the card, and the retailer is capable of seeing the customer, whether because an employee is at the gas station or because there is video surveillance of the pump. Despite these safeguards (which are not available for online transactions), section 1747.08, subdivision (c)(3)(B), also authorizes the collection of personal identification information (i.e., a component of the cardholder's address) for automated pump transactions. By contrast, online transactions have none of the foregoing safeguards, and yet Plaintiff would preclude Apple from requesting any personal identification information to verify the supposed cardholder's identity, including the unseen cardholder's address.

More fundamentally, Plaintiff's argument that the specific exemption for automated gas pumps means that online transactions are covered is based on a flawed premise. He presumes that the Song-Beverly Act applies to all "remote transactions" (a term invented by Plaintiff in an effort to cover both gas pumps and the Internet) and then argues that by creating an exemption for one transaction, the Legislature affirmed the statute's coverage to another type of transaction. But, as noted above, the Act's language and legislative history demonstrate that it was never intended to apply to online transactions in the first place; therefore, an

exemption for one type of brick-and mortar transaction (gas pumps) does not imply coverage for virtual transactions.

Plaintiff also argues that "[e]ven more instructive that the Legislature . . . believes that the Act has, at all times applied to card-not-present transactions, including Internet transactions, is the second to final version of the 2011 amended Act." (Ans., p. 16.) Plaintiff points to the version of Assembly Bill No. 1219, as amended on May 17, 2011, which states that the amendments are made "to clarify existing law" and "recognize, in part, legitimate business practices designed to address the increased potential for identity theft that results if the cardholder is not present or the credit card does not function correctly." (Ans., p. 16, citing Assem. Bill No. 1219 (2011–2012 Reg. Sess.) amended May 17, 2011.) Plaintiff contends that "its words, especially combined with the Legislature's clarification language make it obvious that the Act was, at all times designed to apply both to in-person and card-not-present transactions." (Ans., p. 18.)

The argument is fatally flawed because this amendment was never enacted, as Plaintiff himself acknowledges. (Ans., pp. 17-18 ["these proposed sections ultimately did not make the final cut of the Act"].) "'"[U]npassed bills, as evidences of legislative intent, have little value." [Citations.]' . . . Contrary to [plaintiff's] assertion, the Legislature's failure to enact the amendments . . . 'demonstrates nothing about what the

Legislature intended' when it previously enacted [the] section . . . with the language we are now construing. . . . 'We can rarely determine from the failure of the Legislature to pass a particular bill what the intent of the Legislature is with respect to the existing law.'" (*People v. Mendoza*, *supra*, 23 Cal.4th 896, 921.)[2]

Finally, Plaintiff argues that the Legislature must have intended the Song-Beverly Act to cover online transactions because it made some passing statements in the committee reports addressing earlier versions of Assembly Bill No. 1219 regarding the potential application of the Act to online transactions. (Ans., pp. 19-20.) Plaintiff observes that "the Legislature noted" with respect to "a May 10, 2011 proposed amendment" that "'the current version of the bill sweeps too broadly in effectively removing on-line and telephonic transactions from the scope of the existing law's protection . . . .'" (*Ibid.*, quoting Assem. Com. on Judiciary, Analysis of Assem. Bill No. 1219 (2011–2012 Reg. Sess.) as amended May 4, 2011.)

First, Plaintiff's attribution of these statements to "the Legislature" is misleading. These are one analyst's comments, prepared for the Assembly Judiciary Committee regarding the May 4, 2011 amendment to Assembly

---

[2] Plaintiff's reference to the May 17, 2011 amendment as the "second to final version of the 2011 amended Act" (Ans., p. 16) is also erroneous. The May 17, 2011 amendment was not the second to last version of the statute; the statute was amended four more times before it was enrolled.

Bill No. 1219.[3] (RJN, Ex. G, Assem. Com. on Judiciary, Analysis of Assem. Bill No. 1219 (2011–2012 Reg. Sess.) as amended May 4, 2011.)

More importantly, the analyst's stray comments in *2011* regarding the statute's legislative intent in *1990–1991* (20 years earlier) can have no bearing on whether the Legislature intended section 1747.08 to cover online transactions. Statements or actions of a *subsequent* Legislature (much less an analyst) cannot evidence a previous Legislature's intent. (*Marina Point, Ltd. v. Wolfson* (1982) 30 Cal.3d 721, 735, fn. 7 [unpassed bills have little value as evidence of the intent underlying the legislation of an earlier legislative session].) The 2011 Legislature "ha[d] no authority to interpret a statute. That is a judicial task. The Legislature may define the meaning of statutory language by a present legislative enactment which, subject to constitutional restraints, it may deem retroactive. But it has no legislative authority simply to say what it *did* mean." (*Del Costello v. State of California* (1982) 135 Cal.App.3d 887, 893, fn. 8.)

Section 1747.08's plain language, the policy judgments embodied therein, and its legislative history in 1990-1991 all demonstrate that the Legislature never intended to cover online transactions. The 2011

---

[3] Plaintiff erroneously indicates that these statements appear "in a May 10, 2011 proposed amendment." (Ans., p. 19.) In fact, they are comments by the Assembly Judiciary Committee in a *May 10, 2011 report* discussing the *May 4, 2011 amendment* to Assembly Bill No. 1219. (RJN, Ex. G, Assem. Com. on Judiciary, Analysis of Assem. Bill No. 1219 (2011-2012 Reg. Sess.) as amended May 4, 2011.)

Legislature's decision to partially exempt transactions at an automated gas pump, or statements regarding unpassed amendments, did nothing to expand the coverage of the statute.

D. Plaintiff's Policy Arguments Are Unfounded.

In section VII of his brief, Plaintiff argues that "[e]xempting Internet businesses would destroy consumer protection and is an overreaching solution to the identity theft and credit card fraud problem." (Ans., p. 29.)

This argument is both specious and a mere tautology: It is a tautology to claim that if the Act does not apply to online commercial transactions, consumers will not be protected by the Act. And the argument that privacy protection should be given more weight than fraud prevention is a policy judgment not tailored to the issue of the proper statutory construction. The relevant rule for statutory construction is that a statute should be interpreted so as to """avoid anomalous or absurd results."""" (*Pineda v. Williams-Sonoma Stores, Inc.* (2011) 51 Cal.4th 524, 533.)

Apple's opening brief explained that interpreting section 1747.08 to apply to online transactions would harm consumers by facilitating the very fraud that subdivision (d), which authorizes requests for personal information for in-person transactions, and subdivision (c)(3)(B), which authorizes the use of ZIP Codes at automated gas pumps, is designed to prevent. (See Opening Br., pp. 24-28.) Indeed, Plaintiff acknowledges that "credit card fraud and identity theft are problems of great concern" (Ans., p.

29), but makes no effective argument as to how this problem would be addressed if the square peg of section 1747.08 is inserted into the round hole of online transactions.

Instead, all that Plaintiff can muster is his evasively worded speculation that "[i]t is *possible* that credit card verification would fall under the exception to the Act provided in subsection (c)(3)(A) (required by contract), or (c)(4) (required for a special purpose incidental but related to the transaction), however these exceptions are factual questions." (Ans., pp. 29-30; italics added.) Of course, anything is "possible," and this equivocation sharply contrasts with Plaintiff's prior pleading in this Court that Apple "does not . . . have the right to collect personal information, even for purposes of theft or fraud protection." (Answer to Petition for Review, p. 7.) Plaintiff's phrasing is clearly designed to preserve his right to sue companies on the ground that no such exception can be applied. In any event, Plaintiff cites no case authority and offers no analysis to support his newfound agnosticism that verification of the cardholder's identity *may* come within these exceptions. Finally, even if these exceptions authorized online anti-fraud and verification measures, Plaintiff's position that the need for any particular personal information is a "factual question" to be determined by a jury would engender uncertainty and add significant transaction costs to verifying cardholder identity in e-commerce transactions – a cost that section 1747.08 does not impose on brick-and-

mortar retailers, which are given the *express authority* to examine photo identifications and under specified circumstances, to request and record ZIP codes or driver's license numbers. (E.g., §1747.08, subds. (c)(3)(B), (d).)

Plaintiff also claims that if the Act does not apply to online transactions, e-retailers "will be able to request any information from credit card consumers they wish, including . . . sensitive information such as social security numbers, maiden names, or a whole host of other personal information . . . ." (Ans., pp. 30–31.) However, Apple, Ticketmaster, eBay, and other online retailers do not request such "sensitive" information, even though they do not believe that the Act applies to online transactions. Moreover, as any economics course teaches, market competition provides a restraint against the type of abuses of which Plaintiff complains because consumers need not do business with a competitor with distasteful practices. Finally, the proper remedy to the risk of excessive requests for information is to go to the Legislature, which can tailor a solution after considering the relevant facts and policies – something that did not occur in 1990-1991 with respect to online transactions.

Midway through his "policy" arguments, Plaintiff finally invokes a rule of statutory construction – the rule that an ambiguous statute should be construed to avoid an interpretation that would lead to absurd or anomalous results. (Ans., pp. 31-34.) To do this, Plaintiff submits a hypothetical where a consumer purchases a shirt with a credit card at a retail store, by

telephone or facsimile, and via an online transaction. (Ans., pp. 31-32.) He notes that the store cannot get the customer's address unless the address "qualif[ies] under the 'special purpose' exception found in [section 1747.08, subdivision (c)(4)], as the store needs an address to ship the shirt." (Ans., p. 32.) Plaintiff suggests that it is appropriate to treat the transactions similarly because the same purchase is involved. (Ans., p. 32.)

However, Plaintiff's hypothetical ignores the materially different means for authenticating the cardholder's identity in these scenarios, thereby warranting different treatment: Whereas the retail store has an opportunity to review the physical credit card, compare the signature on the back of the card to the customer's actual signature, and compare the cardholder's name and face to a form of positive identification, the online retailer has no ability to either question the customer nor examine the credit card and photo identification. Treating materially different transactions differently does not lead to an absurd result.

Plaintiff also attempts to draw a parallel between online retailers and self-checkout stands at brick-and-mortar retail locations, such as those common at grocery stores. (Ans., pp. 33-34.) He claims that "a self-checkout is virtually identical to an Internet purchase." (*Id.*, p. 33.) But in a self-checkout, the customer has *physical possession* of a credit card *and* must insert it into a device, eliminating the significant risk extant in online transactions that the cardholder may have stolen the account information

from the cardholder. Further, unlike an online transaction, a store can and often does post a clerk to supervise self-checkout locations to monitor transactions and look for suspicious behavior.

Finally, Plaintiff argues that "[w]hile Apple may offer concern that information is necessary to prevent identity theft, there are equal policy concerns regarding any business' retention of significant amounts of consumer information," citing the risk of hacking. (Ans., pp. 35-36.) There are multiple problems with Plaintiff's argument. First, the risk that hackers may engage in fraud using stolen credit card information is precisely why online merchants need to verify the unseen cardholder's identity. Plaintiff's concern favors Apple's position. Second, Plaintiff's solution to his concern over the retention of consumer information is to strip online retailers of any tools to prevent fraudulent credit card transactions, which is a policy decision that the Legislature has not made in connection with brick-and-mortar transactions. And third, the theoretical possibility of a security breach does not mean that the Legislature intended to prevent all collection of personal identification information in online retail transactions. To the contrary, it is clear that the Legislature expects that online retailers will collect such information. That is, after all, precisely why the Legislature enacted California Online Privacy Protection Act to govern the collection of such information. (Bus. & Prof. Code, §§ 22575 et seq.) It is also why the Legislature passed the Security Breach

Notification law in Civil Code section 1798.82 et seq. to govern how companies handle security breaches. Consumers have specified remedies against companies that do not meet their security obligations.

Plaintiff argues, without any supporting authority, that online merchants have enough information to prevent fraud without collecting personal identification information because they can request a card account number, the expiration date, the cardholder's name, and the CCID. (Ans., p. 35.) But Plaintiff ignores the ease with which criminals can obtain this basic information, including through "phishing," "sniffing," hacking, and "bot" scams. (Opening Br., pp. 24–25.)

In short, unlike brick-and-mortar transactions, the only effective means that an online e-retailer has to prevent fraud is to ask the customer for personal identification information that a fraudster would have difficulty obtaining, namely, the cardholder's billing address and telephone number. Indeed, the "collection of personal information in an online . . . transaction may be the only means of verifying a customer's identity in order to prevent credit card fraud." (*Mehrens v. Redbox Automated Retail LLC* (C.D.Cal. Jan. 6, 2012, No. 11-2936) 2012 WL77220 at p. *3; *Saulic v. Symantec Corp.* (C.D.Cal. 2009) 596 F.Supp.2d 1323, 1335.)

E. Enactment Of The COPPA Further Suggests That Section 1747.08 Does Not Govern Online Transactions.

Apple's opening brief argued that section 1747.08, when considered in light of the California Online Privacy Protection Act ("COPPA"), also suggests that section 1747.08 does not govern online commercial transactions. (Opening Br., pp. 41-45.) Under the COPPA, "[a]n operator of a commercial Web site or online service that collects personally identifiable information . . . shall conspicuously post its privacy policy on its Web site . . . ." (Bus. & Prof. Code, § 22575, subd. (a).)

While Plaintiff argues that the Song-Beverly Act should apply to online transactions because COPPA is not as harsh against online retailers as the Song-Beverly Act would be (Ans., pp. 39-40), Plaintiff's desire for large penalties is not a reason to extend the Song-Beverly Act to online transactions. To the contrary, the Legislature made COPPA less restrictive than the Song-Beverly Act precisely because of the different considerations associated with commercial websites, including out-of-state websites.

Plaintiff argues that "[t]he passage of COPPA does not . . . demonstrate an intent to remove the protections of the Song-Beverly Credit Card Act . . . ." (Ans., p. 39; capitalization omitted.) But this argument erroneously assumes that the Song-Beverly Act granted "protections" to online consumers, which begs the question. Moreover, the enactment of COPPA evidences that section 1747.08 should not apply to online

transactions because it demonstrates that the Legislature adopted a strikingly different policy balance when regulating out-of-state websites. Indeed, the Legislature passed COPPA to deal with the online collection of personally identifiable information because it did not believe existing law regulated the privacy practices of online business entities. (See Opening Br., p. 43.)

F. Construing The Song-Beverly Act To Apply Only To In-Person Transactions Avoids Serious Constitutional Questions.

1. Waiver.

Plaintiff argues that Apple's arguments in support of its interpretation of section 1747.08 that the statute should be construed to avoid serious constitutional questions have been waived because "Apple did not offer these theories in its demurrer," citing *Western Oil & Gas Assn. v. Monterey Bay Unified Air Pollution Control District* (1989) 49 Cal.3d 408, 427, fn. 20 ("*Western Oil*"). (Ans., p. 39.) But *Western Oil* merely stands for the proposition that "[a] party may not for the first time on appeal change its theory of relief." (*Western Oil*, supra, 49 Cal.3d at p. 427, fn. 20.) Apple is not attempting to change its "theory of relief." It is simply providing additional support for the statutory construction argument that it has made from the outset. The rule against waiver has never precluded a party from raising additional points in support of a previously raised legal issue.

In any event, "an appellate court has discretion to consider an issue raised for the first time on appeal if it presents a pure question of law on undisputed evidence, such as the applicability of a statute." (*Mitchell v. United Nat. Ins. Co.* (2005) 127 Cal.App.4th 457, 470–471.)

Here, the issues are properly before the Court and fully briefed by both sides. Moreover, Plaintiff's position would have the effect of straitjacketing the Court from considering all relevant rules of statutory construction in determining the correct interpretation of section 1747.08, thereby risking an erroneous ruling. Plaintiff's waiver argument must be rejected on grounds of absurdity.

2. Applying The Act To Online Transactions Would Violate The Due Process Clause.

Apple's opening brief demonstrated that construing the Act to cover online transactions would offend due process: Either the e-retailer must ask for personal identification information to determine whether the customer is a California resident – which would violate the Act before the e-retailer has notice that the Act applies – or the merchant must not ask for personal identification information from anyone, even where legal to do so, because the requisite notice whether California law applies cannot be obtained without violating the law. (Opening Br., pp. 45-48.)

Plaintiff does not seriously contest that a merchant that conducts business with citizens nationwide must be able to determine which

jurisdiction's laws apply. (Ans., 42.) Instead, Plaintiff argues that "[w]ith respect to due process, Apple assumes (in the absence of any precedent) that merely asking the state of a consumer's residence will violate the Song-Beverly Act." (Ans., p. 44.)

But in *Pineda, supra,* 51 Cal.4th 524, 531, this Court held that a cardholder's address "should be construed as encompassing not only a complete address, but also its *components*" and held that therefore even a ZIP code could not be requested and recorded. Plaintiff cannot seriously dispute that the customer's state of residence is also a component of an address. After all, the United States Postal Service includes the state as part of its definition of an address, as does a California driver's license. There is simply no principled basis drawn from the statutory text to claim that personal identification information includes any component of the cardholder's address, even the ZIP code, but not the state of residence.

Nonetheless, Plaintiff attempts to reassure e-retailers that they will be able to determine which law applies to the numerous online transactions in which they engage because "it is entirely *possible* that simply asking for the state of residence would qualify under the subsection (c)(4) defense . . . ." (Ans., p. 45; italics added.) However, even if (notwithstanding *Pineda*) e-retailers could request the consumer's state of residence without violating section 1747.08, such an arrangement would facilitate fraud by anyone willing to assert California residency. Plaintiff's argument

necessarily assumes that no one committing credit card fraud would ever stoop to falsely claiming California residency in order to be relieved of having to provide the information necessary to verify his or her identity. And if the e-retailer asked for additional address information to confirm the purported cardholder's claim of California residency, it would unequivocally conflict with section 1747.08's prohibition against collecting the cardholder's address. (§1747.08, subd. (b).)

Plaintiff also argues that Apple "is in no position to complain about being subject to California's consumer protection laws" because it is "a California corporation . . . and . . . its contracts contain a choice of law clause (California law) . . . ." (Ans., p. 42.) But the proper construction of a statute is not dependent upon a particular retailer's choice-of-law provisions. This Court's construction of section 1747.08 will apply to all online retailers, many of whom may not be California corporations or may operate with contracts that do not contain choice-of-law provisions. And those entities that do select a particular state's law to govern their customer relationships are not necessarily guaranteed that the specified forum's law will apply: Courts find the choice-of-law agreement to be unenforceable where, inter alia, the chosen law fundamentally conflicts with California law and California has a materially greater interest in the determination of the issue. (See *Washington Mutual Bank v. Superior Court* (2001) 24 Cal.4th 906, 917-919.)

None of Plaintiff's suggestions, therefore, change the fact that an online retailer will not be able to determine whether the Song-Beverly Act applies to a transaction unless the retailer violates the Act by requesting the state of residence. That scenario is much different from *Ferguson v. Friendfinders, Inc.* (2002) 94 Cal.App.4th 1255 (*Ferguson*), which Plaintiff cites in his Answer. (Ans., p. 44.) The statute at issue in *Ferguson* – Business and Professions Code section 17538.4 – applied only when a business sent unsolicited commercial emails to California residents via equipment located in California. (*Ferguson*, *supra*, 94 Cal.App.4th at p. 1258.) Because the business itself would be able to ascertain whether the emails were being sent from equipment located in California, and because existing lists of email addresses sorted by geographic location allowed the email senders to determine the location of the recipients, the court concluded that the statute did not fun afoul of the dormant commerce clause since the geographic limitations were effective to ensure that the statute did not regulate out-of-state transactions. (*Id.* at pp. 1265–1266.) By contrast, in this case, Plaintiff identifies no effective means for an e-retailer to determine where its customer is located without asking the customer for that information – which would constitute a violation of the Act before the e-retailer receives notice that the Act applies.

3. Applying The Act To Online Transactions Would Impermissibly Regulate Interstate Commerce.

Apple's opening brief also demonstrated that interpreting the Act to cover online transactions would raise serious questions whether section 1747.08 violated the commerce clause: Either the effect of such an interpretation would be for California to impermissibly regulate out-of-state retailers, who are unable to determine whether any particular customer is a California resident and thus would need to apply California law to every transaction. (Opening Br., pp. 49-53.) Or the application of section 1747.08 to online transactions would impose a clearly excessive burden on commerce under the *Pike* balancing test because the obligation to exempt self-designated California residents from providing personal identification information would facilitate fraud by anyone willing to assert California residency and further, because the prohibition on recording such information would interfere with the online retailers' maintenance of business records necessary to demonstrate their compliance with other states' tax laws. (*Id.*, pp. 54-59.)

Plaintiff contends that "it cannot be argued that the Act discriminates against out-of-state businesses, because collection of unnecessary [personal identification information] is forbidden to all merchants." (Ans., pp. 45-46.) But Plaintiff misconceives the test for discrimination in interstate commerce. The ban covers statutes that have "the undeniable effect of

controlling commercial activity occurring wholly outside the boundary of the State." (*Healy v. Beer Institute* (1989) 491 U.S. 324, 337; Opening Br., pp. 48-50.) Here, the application of section 1747.08 to online transactions would have the practical *effect* of governing all online purchases wholly outside the State because the only way for an e-retailer to comply with the Act, short of requesting the customer's address (in whole or in part) and thereby violating the law, is to apply California law to every transaction. (See Opening Br., pp. 50-51.)

Regarding the *Pike* balancing test – the alternative test under the commerce clause invoked by Apple – Plaintiff contends that "there is little or no burden on interstate commerce" "[i]f . . . Apple under the language of the Act (as a defense) can ask for information, so long as it is actually used to verify a credit card, and for no other purpose." (Ans., p. 47.) But this position contradicts Plaintiff's earlier position that Apple did not have the right to collect personal identification information for purposes of fraud prevention. (Answer to Petition for Review, p. 7.) Further, Plaintiff's contention is equivocal and conditional (i.e. "*[i]f* . . . Apple under the language of the Act (as a defense) *can* ask for information") upon which he does not expand. Finally, nowhere does the Act provide the type of express provisions allowing verification that are afforded to brick-and-mortar stores.

Plaintiff also contends that "*Ferguson* and *Ford Motor Company* [*v. Texas Dept. of Transportation* (5th Cir. 2001) 264 F.3d 493] have correctly determined the standard; a consumer protection law that incidentally regulates merchants that transact business with all 50 states merely because of their use of the Internet does not violate the commerce clause. If the rule were otherwise, all merchants would be able to . . . avoid consumer protection laws of all 50 states by claiming an inability to comply with any of them." (Ans., p. 45.) First, Apple never argued that the relevant test was an "incidental" regulation of commerce or that the mere difficulty in complying with multiple state laws itself establishes a clearly excessive burden under the *Pike* balancing test. Instead, Apple's point is that section 1747.08's facilitation of fraud by anyone willing to assert California residency (if the statute applies to e-retailers) and the statute's interference with online retailers' maintenance of business records necessary to demonstrate their compliance with other states' tax laws (because they could not support their determination of the purchaser's jurisdiction with an address) establishes a clearly excessive burden.

Moreover, unlike here, the burden imposed on interstate commerce in *Ferguson* was minimal. (*Ferguson, supra*, 94 Cal.App.4th at p. 1269.) The statute in *Ferguson* only required that those sending unsolicited commercial emails (i) establish a toll-free number or return e-mail address, (ii) include a statement in the e-mail informing the recipient of the toll-free

number or return address (by which the sender could be notified to stop sending further e-mails), and (iii) place particular letters in the subject line of the email, the cost of which "'is appreciably zero in terms of time and expense.'" (*Ibid.*) And because the statute only applied when equipment in California was used, "our Legislature ensured that the statute would not reach conduct occurring 'wholly' outside the state." (*Id.* at p. 1265.)

Here, by contrast, the burden on interstate commerce is significant: A retailer who does not have the ability to request personal identification information from an online purchaser is uniquely vulnerable to fraudulent transactions, thereby impacting the price and availability of goods nationwide. Moreover, because e-retailers will not be able to determine which State's law applies without risking a violation of the Act, either California law would have to be applied to every transaction (which would further heighten the cost and burden of fraudulent transactions), or e-retailers would cease doing business with California residents because of the increased risk of fraud. Either is a much greater burden than the mere inclusion of some additional language in an unsolicited, commercial email, which was the case in *Ferguson*, and is a burden that outweighs any putative benefit of construing the Act to apply to online transactions.

Plaintiff suggests that "[t]here is nothing in the record that the request of an address *and* phone number is standard practice for Internet businesses, and that it would be difficult to either change such requests or

modify the website when dealing with California consumers. The same is true for the alleged sales tax issue, as, if a state requires the collection of addresses for sales tax purposes, such information request would qualify as a statutory defense under (c)(3)(C) (state or federal law)." (Ans., p. 48.)

However, it is not that any particular state *requires* the collection of *addresses* for sales tax purposes, but that a retailer must maintain adequate documentation to support its determination of which state's law applies. (Opening Br., p. 58.) Likewise, the issue is not whether a request for an address *and* phone number is standard practice, but whether section 1747.08 can properly be applied to e-retailers without depriving them of the right to verify the cardholder's identity through the collection of *any* personal identification information. Finally, the burden on interstate commerce does not depend on whether the retailer is able to change its requests or its website, but upon the impact of prohibiting the collection of personal identification information.

In sum, Plaintiff's arguments do not avoid the difficult constitutional questions raised by applying the Song-Beverly Act to online transactions. This Court should interpret the Act in a way that avoids these due process and commerce clause problems by finding that the Act does not apply to online transactions.

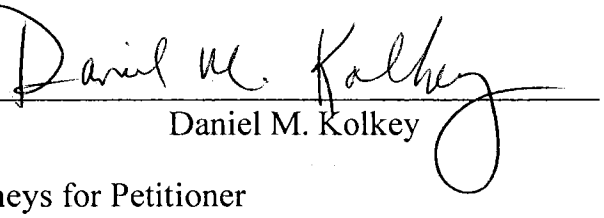
III. CONCLUSION

For the reasons set forth in its briefs, Petitioner Apple respectfully requests that this Court determine that section 1747.08 does not apply to online transactions and direct the Court of Appeal to reverse the trial court's order overruling its demurrer.

Respectfully submitted,

DATED: June 20, 2012

GIBSON DUNN & CRUTCHER LLP

By: 
Daniel M. Kolkey

Attorneys for Petitioner
APPLE INC.

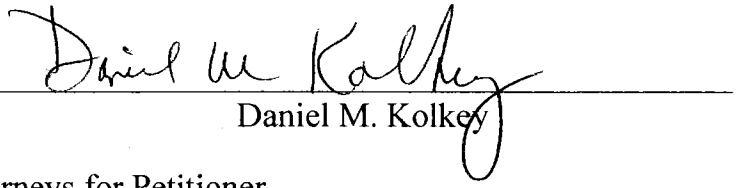
CERTIFICATE OF COMPLIANCE
PURSUANT TO RULE 8.520(c), CALIFORNIA RULES OF COURT

In accordance with rule 8.520(c), California Rules of Court, the undersigned hereby certifies that this Reply Brief on the Merits contains 8,388 words, as determined by the word processing system used to prepare this brief, excluding the tables, the cover information, the signature block, and this certificate.

Respectfully submitted,

DATED: June 20, 2012

GIBSON, DUNN & CRUTCHER LLP

By: 
Daniel M. Kolkey

Attorneys for Petitioner
APPLE INC.

PROOF OF SERVICE

I, Carol Dickerson, declare as follows:

I am employed in the County of San Francisco, State of California; I am over the age of 18 and am not a party to this action; my business address is Gibson, Dunn & Crutcher LLP, 555 Mission Street, Suite 3000, San Francisco, CA 94105. On June 20, 2012, I served the within:

APPLE INC.'S REPLY BRIEF ON THE MERITS

by placing a true copy thereof in an envelope addressed to each of the persons named below at the address shown on the next page in the following manner:

SEE ATTACHED SERVICE LIST

X **BY OVERNIGHT DELIVERY:** I placed a true copy in a sealed envelope addressed as indicated above, on the above-mentioned date, for collection and overnight delivery by an express service carrier pursuant to Gibson, Dunn & Crutcher's practice. I am familiar with Gibson, Dunn & Crutcher's practice in its above-described San Francisco office for the collection and processing of correspondence for distribution by Federal Express, UPS, and/or U.S. Postal Service Overnight Mail. Pursuant that practice, envelopes placed for collection at designated locations during designated hours of this office are delivered to an authorized courier or driver authorized by the express service carrier to receive documents in an envelope or package designated by that carrier, with delivery fees paid or provided for, on that same day in the ordinary course of business.

I certify under penalty of perjury that the foregoing is true and correct, that the foregoing documents(s) were printed on recycled paper, and that this Certificate of Service was executed by me on June 20, 2012, at San Francisco, California.

Carol Dickerson

SERVICE LIST

VIA FEDERAL EXPRESS

Edwin Schreiber, Esq.
THE LAW OFFICES OF SCHREIBER & SCHREIBER
16501 Ventura Boulevard, Suite 401
Encino, California 91436
Tel: (818) 789-2577

Representing: **Brian Luko**, individually and on behalf of a class of person similarly situated;
David Krescent, individually and on behalf of a class of person similarly situated

Sheldon Eisenberg, Esq.
Kristopher S. Davis, Esq.
DRINKER BIDDLE & REATH LLP
1800 Century Park East, Suite 1400
Los Angeles, California 90067
Tel: (310) 203-4000

Representing: **eHarmony, Inc.**

William A. Delgado, Esq.
Eileen M. Ahern, Esq.
WILLENKEN WILSON LOH & DELGADO LLP
707 Wilshire Boulevard, Suite 3850
Los Angeles, California 90071
Tel: (213) 955-9240

Representing: **Ticketmaster L.L.C.**

Clerk of the Court
Court of Appeal, Second Appellate District
Division Eight
Ronald Reagan State Building
300 South Spring Street
2nd Floor, North Tower
Los Angeles, California 90013
Tel: (213) 830-7000

Clerk of the Court
Los Angeles Superior Court
Central Civil West Courthouse
600 S. Commonwealth Avenue
Los Angeles, California 90005
Tel: (213) 351-8610