

MAY 31 2012

S199384

Frederick K. Ohlrich Clerk

IN THE SUPREME COURT OF CALIFORNIA

Deputy

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
(Related to Cases Nos. BC462492 and BC462494)

**REAL PARTY IN INTEREST DAVID KRESCENT'S
ANSWER BRIEF ON THE MERITS**

SCHREIBER & SCHREIBER, INC.

Edwin C. Schreiber, SBN 41066

Eric A. Schreiber, SBN 194851

16501 Ventura Boulevard Suite 401

Encino, California 91436-2068

Telephone: (818) 789-2577

Facsimile: (818) 789-3391

Attorneys for Plaintiff and Real Party in Interest
DAVID KRESCENT

**Supreme Court
State of California**

CERTIFICATE OF INTERESTED ENTITIES OR PERSONS

Supreme Court Case Number: S199384

Case Name: Krescent v. Apple, Inc.

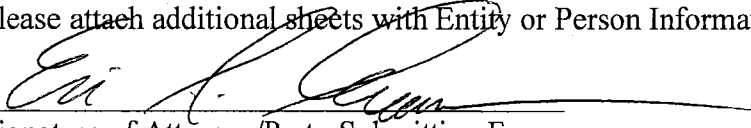
Please check the applicable box:

There are no interested entities or parties to list in this Certificate per California Rules of Court, Rule 8.208 (e) (1), (2).

Interested entities or parties are listed below:

<u>Name of Interested Entity or Person</u>	<u>Nature of Interest</u>
1.	
2.	
3.	
4.	

Please attach additional sheets with Entity or Person Information if necessary.


Signature of Attorney/Party Submitting Form

Printed Name: Eric A. Schreiber
Address: 16501 Ventura Boulevard, Suite 401, Encino, California, 91436
State Bar No: 194851
Party Represented: Plaintiff and Real Party in Interest, David Krescent

SUBMIT PROOF OF SERVICE ON ALL PARTIES WITH YOUR CERTIFICATE

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
(Related to Cases Nos. BC462492 and BC462494)

**REAL PARTY IN INTEREST DAVID KRESCENT'S
ANSWER BRIEF ON THE MERITS**

SCHREIBER & SCHREIBER, INC.
Edwin C. Schreiber, SBN 41066
Eric A. Schreiber, SBN 194851
16501 Ventura Boulevard Suite 401
Encino, California 91436-2068
Telephone: (818) 789-2577
Facsimile: (818) 789-3391

Attorneys for Plaintiff and Real Party in Interest
DAVID KRESCENT

TABLE OF CONTENTS

<u>I. INTRODUCTION AND THE RULING OF THE SUPERIOR COURT</u>	1
<u>II. ISSUE PRESENTED FOR REVIEW</u>	3
<u>III. THE STANDARD OF REVIEW</u>	3
<u>IV. STANDARDS OF STATUTORY INTERPRETATION</u>	6
<u>V. THE SONG-BEVERLY CREDIT CARD ACT AND RECENT AMENDMENTS</u>	8
<i>A. The Language of the Act Itself</i>	9
<i>B. The October 9, 2011 Amendments to the Act, Along With Prior Drafts Thereof Make the Legislature's Intent that the Act Applies to Remote Transactions Unmistakably Clear</i>	14
1. <i>The Actual Amended Act</i>	15
2. <i>The Second to the Last Version of the Act</i>	16
<i>C. The Stated Legislative Purpose of the Act Would Not be Fulfilled if Millions of Internet Transactions Were Exempted</i>	19
<u>VI. THIS COURT IN ADDITION TO MOST COURTS THROUGHOUT THE COUNTRY, HAS HELD THAT INTERNET BASED BUSINESSES ARE SUBJECT TO THE SAME RULES AND LAWS AS OTHER BUSINESSES</u>	23

VII. THE PURPOSES AND PROTECTIONS OF THE ACT WOULD BE EVISCERATED FOR MILLIONS OF CALIFORNIA CONSUMERS IF INTERNET RETAILERS ARE CARTE BLANCHE EXEMPTED FROM THE ACT 29

1. Exempting Internet Businesses Would Destroy Consumer Protection and is an Overreaching Solution to the Identity Theft and Credit Card Fraud Problem 29

2. Exempting Internet Businesses from the Act Would Lead to Inconsistent, Unfair and Absurd Results for California Consumers 31

3. Internet Businesses Like all Businesses Who Engage in Card-Not-Present Transactions Have a Whole Host of Remedies to Verify Credit Cards 35

4. There are Also Social Policy Concerns Relating to Businesses' Recording of Consumer Information, Causing as Much Concern as Identity Theft 35

A. The concern of security hacks at the business level 36

B. Merchants may misuse the data once they have it 36

VIII. APPLE'S CLAIMS BASED UPON OTHER CALIFORNIA STATUTES AND CONSTITUTIONAL CHALLENGES ARE RAISED FOR THE FIRST TIME ON APPEAL AND WERE THUS WAIVED. FURTHERMORE, SUCH CLAIMS DO NOT PREEMPT THE ACT OR OTHERWISE EXEMPT INTERNET BUSINESSES 38

*A. The Passage of COPPA Does Not, in any Way
Demonstrate an Intent to Remove the Protections of
the Song-Beverly Credit Card Act for
California Consumers* 39

*B. There is no Basis to Challenge the Act on
Constitutional Grounds Because the Act Does not
Specifically Regulate the Internet or Internet
Commerce, Rather it Applies Equally to all Businesses* 41

IX. CONCLUSION 49

TABLE OF AUTHORITIES

Federal Cases

<i>BigStar Entertainment, Inc. v. Next Big Star, Inc.</i> 105 F.Supp.2d 185 (S.D.N.Y. 2000)	25
<i>Bland v. Fessler</i> , 88 F.3d 729 (9 th Cir. 1996)	46
<i>Brookfield Communications v. West Coast Entertainment Corporation</i> 174 F.3d 1036 (9 th Cir. 1999)	25
<i>Butler v. Adoption Media, LLC</i> 486 F.Supp.2d 1022 (N.D. Cal. 2007)	26
<i>Ford Motor Company v. Texas Department of Transportation</i> 264 F.3d 493 (5 th Cir. 2002)	25-26, 43
<i>Gass v. Best Buy Co., Inc.</i> WL 538251(C.D. Cal Feb. 2012)	37-38

California Cases

<i>Contemporary Service Corp. v. Staff Pro, Inc.</i> (2007) 152 Cal.App.4th 1043	28
<i>Ferguson v. Friendfinders, Inc.</i> (2002) 94 Cal. App.4th 1255	43-44
<i>Florez v. Linens n' Things</i> (2003) 108 Cal. App.4th 447	22, 32
<i>Kwikset Corp v. Superior Court</i> (2011) 51 Cal.4th 310	46
<i>Pineda v. Williams-Sonoma Stores</i> (2011) 51 Cal.4th 524	<i>Passim.</i>
<i>People v. Western Airlines, Inc.</i> (1984) 155 Cal.App.3d 597	46
<i>Powers v. Pottery Barn, Inc.</i> (2009) 177 Cal. App.4th 1039	27

<i>Sheehan v. San Francisco 49ers, Ltd.</i> (2009) 45 Cal.4th 992	3
<i>Serrano v. Priest</i> (1971) 5 Cal.3d 584	3
<i>Snowney v. Harrah's Entertainment, Inc.</i> (2005) 35 Cal.4th	24
<i>Stockton Savings & Loan Bank v. Massanet</i> (1941) 18 Cal.2d 200	17
<i>Truta v. Avis Rent-A-Car-System, Inc.</i> (1987) 193 Cal. App.3d 802	3
<i>Vo v. City of Garden Grove</i> (2004) 115 Cal. App.4th 425	25
<i>Weatherall Aluminum Products v. Scott</i> (1977) 71 Cal.App.3d 245	28
<i>Western Oil & Gas Assn. v. Monterey Bay Unified Air Pollution Control District</i> (1989) 49 Cal.3d 408, 427, fn. 20	39

Federal Statutes

15 U.S.C. §§ 6501-6506	40
------------------------	----

California Statutes

<u>Business and Professions Code</u> § 17538.4	43-44
<u>Business and Professions Code</u> § 22575 (COPPA)	38-41
<u>Civil Code</u> §§ 1633.1-1633.17	10
<u>Civil Code</u> § 1633.15 (b)	10
<u>Civil Code</u> § 1689.5	27-28
<u>Civil Code</u> § 1770 (a)(4)	46

Civil Code § 1747.08 *Passim.*

Civil Code 1747.02 (n)(o) 15

Commercial Code § 4110 12

Secondary Authority

Hsu, Tiffany, **Los Angeles Times**, March 31, 2012,
Page B2 Breach of Credit Card Data Feared. 36
[Attached to Brief as Exhibit 1, Per CRC 8.520 (h)]

Sarno, David, **Los Angeles Times**, April 1, 2012,
Page 1, Californians Wary of Data Gathering 36
[Attached to Brief as Exhibit 2, Per CRC 8.520 (h)]

I. INTRODUCTION AND THE RULING OF THE SUPERIOR

COURT

On June 10, 2011, Plaintiff and Real Party in Interest David Krescent (“Plaintiff” or “Krescent”) filed a one cause of action class action complaint against Defendant and Petitioner, Apple, Inc. (“Apple,” “Defendant” or “Petitioner”) seeking civil penalties under Civil Code § 1747.08, also known as the Song-Beverly Credit Card Act (hereinafter referred to as the “Act”).¹ Plaintiff alleged that in the course and scope of a credit card transaction, that Apple, by and through the use of a standardized form, requested and required him to provide his address and telephone number as a condition of purchasing music and other software known as “apps”² downloaded over the Internet. The lawsuit alleged that Defendant violated the Act by requesting and requiring him to provide personal identifying information (hereinafter referred to as “PII”), which information was recorded by the Defendant in connection with a credit card transaction. Krescent further alleged that Apple did not need or use his personal information to verify his credit card for purposes of identity

¹. This action was related to *Luko v. Ticketmaster, LLC* and *Luko v. eHarmony, Inc.* in the trial court.

². For purposes of this brief the terms “apps” (a term generally used as shorthand for applications) shall refer to a variety of software programs and products which are downloaded to a computer, mobile phone or other mobile device with an Internet connection.

theft or fraud protection, and that because this was a digital download, nothing was physically shipped to Krescent. Plaintiff sought civil penalties up to the legal maximum of \$250 for the first transaction, and up to \$1,000 for each subsequent transaction (Exh. 3, pgs. 21-30).

On December 7, 2011 the Trial Court (Los Angeles Superior Court, Complex Division) concurrently heard Apple, Ticketmaster and eHarmony's demurrers to their respective complaints. The theory of the demurrers was that the Act does not apply to remote transactions such as those transacted over the Internet, but rather, the Act applies only to face-to-face, brick-and-mortar in person transactions at retail stores. After opposition and hearing, the Trial Court (the Honorable Carl J. West [now retired]) overruled the demurrers in all three related matters (Exh. 30, pgs. 573-581). Each of the defendants individually filed petitions for writ of mandate in the Court of Appeal (Second Appellate District, Division Eight), all of which were summarily denied. Thereafter, this Court granted review in all three cases by its Order dated March 21, 2012. On March 28, 2012, this Court issued a further Order deeming the Apple case the lead case and staying the Ticketmaster and eHarmony cases pending further order or decision of this Court. Krescent hereby submits this answer brief on the merits in response to Apple's opening brief.

II. ISSUE PRESENTED FOR REVIEW

This case presents only one issue for review:

Does the Song-Beverly Credit Card Act of 1971 (Civil Code §1747 et seq.), which prohibits retailers from recording a customer's personal identification information when the customer uses a credit card in a transaction, preclude on-line retailers from obtaining and recording a purchaser's address and telephone number as a prerequisite to accepting a credit card as payment for a purchase of an item that does not need to be shipped to the purchaser?

III. THE STANDARD OF REVIEW

In the instant case, 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 (*Sheehan v. San Francisco 49ers, Ltd.* (2009) 45 Cal.4th 992, 996). The scope of a demurrer is limited to the four corners of the complaint and those issues for which the Court may properly take judicial notice. A general demurrer can only test the legal sufficiency of a complaint, and the Court must consider all material facts plead to be true. (*Serrano v. Priest* (1971) 5 Cal.3d 584, 591). A complaint which states a cause of action on any theory will defeat a general demurrer (*Truta v. Avis Rent-A-Car-System, Inc.* (1987) 193 Cal. App.3d 802). Therefore, every inference must be given to the facts plead in Krescent's complaint, and Apple must demonstrate that even if every fact

in Plaintiff's complaint is true, Krescent would still be unable to state any facts sufficient to constitute a cause of action under the Act.

All of the following facts plead in the complaint must be presumed true:

1. That Apple is a business that accepts credit cards for business transactions;

2. That Plaintiff navigated his computer cursor to Apple's on-line iTunes store and as a requirement of his credit card purchase, was required to fill out Apple's preprinted form, and was required to provide Apple with his telephone number and address, and that Apple, as a policy, requires consumers to provide their telephone numbers and addresses as a condition of accepting credit card payments;

3. Plaintiff further alleged on information and belief that Apple was neither required by contract or by any law for the purposes of the credit card transaction, to record Plaintiff's telephone number or address;

4. Plaintiff further alleged that Apple does not need or use, and did not need or use his telephone number to verify his credit card, and further Apple did not need or use Krescent's address for shipping anything to him, because the entire transaction was accomplished by a digital download; and

5. Finally, that Apple kept or otherwise maintained a record of the Plaintiff's personal information. (*See* Complaint, Exh. 3, pgs. 22-24, 26-29).

Thus, for purposes of this petition, all of the following allegations of

Krescent's complaint are presumed true:

1. That Apple is a business that accepts credit cards;
2. That in connection with a credit card transaction, Apple through the use of a preprinted form requested and required Plaintiff to provide Apple with his telephone number and address as a condition of purchasing electronic media downloads from Apple, and that there was nothing to be shipped to Krescent. Krescent also alleged that Apple recorded this information;
3. Apple is not required by contract, or federal or state law to collect Krescent's personal information. Furthermore, Apple did not need Plaintiff's personal information for any special purpose incidental to the transaction; and
4. That Apple **did not need or use Plaintiff's personal information (especially his phone number) to verify the authenticity of Krescent's credit card (i.e. fraud or identity theft protection).**

Therefore, Apple must demonstrate that even if it requested/required Krescent's personal information consisting of his telephone number and address as a condition of accepting a credit card payment, which it subsequently recorded, **and** that it was not required to collect this information by either contract or law, **and** that Apple did not need or use Krescent's address or telephone number to verify his credit card, that Apple is not, under any circumstance liable under the Act, because all Internet based businesses are completely exempt from the Act.

IV. STANDARDS OF STATUTORY INTERPRETATION

As this Court recently discussed the Song-Beverly Credit Card Act in *Pineda v. Williams-Sonoma Stores* (2011) 51 Cal.4th 524 (“*Pineda*”), it is best to adopt this Court’s views regarding how this statute is to be interpreted. In *Pineda* this Court noted;

We independently review questions of statutory construction. (*Imperial Merchant Services, Inc. v. Hunt* (2009) 47 Cal.4th 381, 387, 97 Cal.Rptr.3d 464, 212 P.3d 736.) In doing so, we look first to the words of a statute, “because they generally provide the most reliable indicator of legislative intent.” (*Hsu v. Abbata* (1995) 9 Cal.4th 863, 871, 39 Cal.Rptr.2d 824, 891 P.2d 804.) We give the words their usual and ordinary meaning (*Lungren v. Deukmejian* (1988) 45 Cal.3d 727, 735, 248 Cal.Rptr. 115, 755 P.2d 299), while construing them in light of the statute as a whole and the statute's purpose (*Walker v. Superior Court* (1988) 47 Cal.3d 112, 124, 253 Cal.Rptr. 1, 763 P.2d 852). “In other words, ‘**we do not construe statutes in isolation, but rather read every statute ‘with reference to the entire scheme of law of which it is part so that the whole may be harmonized and retain effectiveness.’**”’ (*Smith v. Superior Court* (2006) 39 Cal.4th 77, 83, 45 Cal.Rptr.3d 394, 137 P.3d 218.) **We are also mindful of “the general rule that civil statutes for the protection of the public are, generally, broadly construed in favor of that protective purpose.”** (*People ex rel. Lungren v. Superior Court* (1996) 14 Cal.4th 294, 313, 58 Cal.Rptr.2d 855, 926 P.2d 1042 (Lungren); see Florez, supra, 108 Cal.App.4th at p. 450, 133 Cal.Rptr.2d 465 [liberally construing former § 1747.8, now § 1747.08].) “If there is no ambiguity in the language, we presume the Legislature meant what it said and the plain meaning of the statute governs.” (*People v. Snook* (1997) 16 Cal.4th 1210, 1215, 69 Cal.Rptr.2d 615, 947 P.2d 808.) “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.” (*Murphy v. Kenneth Cole Productions, Inc.* (2007) 40 Cal.4th 1094, 1103, 56 Cal.Rptr.3d 880, 155 P.3d 284.) Our discussion thus begins with the

words of section 1747.08. (*Id.* at 529-30, emphasis added).

Later,

There are several reasons to prefer this latter, broader interpretation over the one adopted by the Court of Appeal. **First, the interpretation is more consistent with the rule that courts should liberally construe remedial statutes in favor of their protective purpose** (*Lungren*, supra, 14 Cal.4th at p. 313, 58 Cal.Rptr.2d 855, 926 P.2d 1042), **which, in the case of section 1747.08, includes addressing “the misuse of personal identification information for, inter alia, marketing purposes.”** (*Absher v. AutoZone, Inc.* (2008) 164 Cal.App.4th 332, 345, 78 Cal.Rptr.3d 817 (*Absher*).) **Such an interpretation would vitiate the statute's effectiveness.** Moreover, that the Legislature intended a broad reading of section 1747.08 can be inferred from the expansive language it employed, e.g., “concerning” in subdivision (b) and “any personal identification information” in subdivision (a)(1). (Italics added.) **The use of the broad word “any” suggests the Legislature did not want the category of information protected under the statute to be narrowly construed.** (*Id.* at 532-33, emphasis added).

Therefore, the key issues to be addressed in examining the Act are its plain language, its remedial purpose of protecting consumer information, and preventing retailers from acquiring more information than they need to complete transactions. Finally, if necessary, an examination of the legislative history to further determine intent in case of an ambiguity.

**V. THE SONG-BEVERLY CREDIT CARD ACT AND RECENT
AMENDMENTS**

The language of the Act, legislative history, comments, subsequent amendments, and California case law all demonstrate the purpose of the Act is to protect consumer privacy, and to prevent retailers from acquiring and recording any more information than is necessary to complete a credit card transaction.

This Court was certain to note,

However, the legislative history of the Credit Card Act in general and section 1747.08 in particular demonstrates the Legislature intended 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 535-36, emphasis added).

In *Pineda* this Court went to great lengths to discuss the fact that retailers are forbidden from acquiring any more consumer information than is necessary to complete a credit card transaction. Thus, in *Pineda*, even the request for a zip code alone, which was unnecessary to complete a credit card transaction, and which allowed a retailer to use that information along with the consumer's name and credit card number to look up information for marketing purposes violated the Act.

An analysis of all of the following demonstrates that it is unmistakably clear that the Act applies to all businesses, whether they are brick-and-mortar,

remote, or in some cases, both.

A. The Language of the Act Itself

The opening line of the Act states,

(a) 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:** (*emphasis added*).

The language of the Act must be read as an all-inclusive prohibition on every businesses regardless of the form of the transaction; hence the incredibly broad language with no limitations. While Internet based transactions did not exist in 1991 when the most recent significant version of the Act was enacted (until the 2011 gas station amendment, discussed *infra*), facsimile and telephone transactions did exist. An Internet transaction is nothing more than a technologically advanced remote transaction. The 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. The all-inclusive language of the Act makes it clear that no retailer, whether the transaction is in person or remote, has the right to collect personal information not required to complete the transaction, as a condition of a credit card purchase.

Apple argues words such as “write” “credit card form” and “preprinted spaces” demonstrate an intent to apply the Act only to in-store face-to-face transactions. This is demonstrably untrue. In 1991, the Internet was not generally used at all, let alone for significant, every day commerce. Thus, words such as “write,” “record” and “pre-printed”³ 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. It should also be noted that, for example, to engage in a remote transaction, such as a telephone or fax catalog order, a consumer would likely have to fill out such form in writing. Similarly, the language used such as prohibiting a retailer from writing or “otherwise

³. California’s Uniform Electronic Transactions Act (CUETA), Civil Code §§ 1633.1-1633.17, both 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 including one stored electronically. Therefore a consumer can write information by typing and submitting over a computer which is given the identical legal effect as writing such information down on paper. Under CUETA a consumer’s providing of information over the Internet is no different than writing such information down on a piece of paper which the merchant then keeps or records.

Civil Code § 1633.15 (b) is instructive on this very issue, “. . . . an electronic record is received when the electronic record enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information (without question PII in the Act qualifies under the definition of “information” under CUETA) of the type sent in a form capable of being processed by that system and from which the recipient is able to retrieve the electronic record.”

recording” the information evidences an intent to prohibit all forms of recording of consumer information, be it written, typed or digitally recorded.

Furthermore, there is no substantive difference between having a consumer hand write information with a pen on a paper form, or asking the customer to input information on a digital field via a typed transaction which is then submitted to the merchant, especially since the adoption of CUETA. The result is the same under either scenario, the customer provides his or her information to the merchant, which the merchant then records for its own purposes. Many retailers employ a digital pad at a register where a customer must input information (for example, a pin pad at a gas pump to verify a zip code, or a small electronic screen at a cash register where a customer swipes a card and then electronically inputs information). Clearly, Apple cannot argue that a merchant can escape the Act’s requirements by having a customer digitally input information as opposed to the consumer writing such information with a pen.

Finally, 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 (with a magnetic strip with the credit card information), or the retailer is presented with the card number and other card information which is submitted to the credit card company for authorization. An on-line consumer *presents* his

or her credit card by providing all of the information printed on the card to the on-line merchant. Thereafter, the on-line merchant engages in the same process of contacting the credit card company, and, if the card is accepted, capturing the credit and sending the good or service to the consumer. By way of a parallel example, Commercial Code § 4110 permits electronic presentment of negotiable instruments. Subsection (a) notes, that parties may enter into an agreement “providing that presentment of an item may be made by transmission of an image of an item or **information describing the item**. . . rather than delivery of the item itself.” (Emphasis added). Without question, if electronic transmission of an image or information describing a negotiable instrument is acceptable in lieu of physical presentment, then providing all of the relevant information of a credit card sufficient to permit a charge to effect a purchase is an acceptable method of presentment of a credit card. Under California law, “presentment” need not be the physical act of handing a credit card over to a merchant, providing enough information to allow a credit card to be charged is also presentment.

On-line merchants are provided various tools for credit card authorization, even if not the same tools as those when a card is physically handed to the merchant. 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—however, what Plaintiff does suggest is that

Apple, like many other Internet retailers is overreaching by asking for significantly more information than is required to actually verify the credit card, and is then using that information for far more than mere credit card verification. Plaintiff has alleged that Apple is using the excuse of credit card verification to obtain consumer's personal information for its own marketing or other business purposes.

The Legislature cannot be presumed to be prognosticators of technological innovations in commerce. The Legislature in 1991 could not foresee the existence of computer and Internet based commerce and presuming this form of commerce to eventually exist. However, the Legislature did purposefully select broad language in the Act to include all future forms of commerce. An Internet retailer is still a retailer, and the basic nature of the transaction is the same, the purchase of goods or services with a credit card. While Plaintiff's transaction was more technologically advanced, Plaintiff is still a consumer, paying Apple, a merchant, with his credit card. This is the very type of transaction covered by the Act regardless of its form, be it in person, over the phone, via a fax order, or over the Internet.

There is no evidence that the Legislature intended this protection to be afforded only to those consumers who physically visits a retail store. Rather, the Act, a consumer protection statute designed to be interpreted broadly in favor of consumers, is designed with robust consumer protection in mind, and

the Act's purpose would be seriously hindered, rather than furthered, by exempting millions of transactions merely because they occur over the Internet rather than in person. The most basic rule of statutory construction is to view the act as a whole, giving intent to its stated purpose. Here, the purpose of the Act is to prevent overbroad information requests by merchants, and the only interpretation of the Act that provides consumers protection and prevents merchants from asking for any more information than is necessary to accomplish its statutory goal, is to hold that the Act applies equally to all businesses, including those that operate over the Internet.

B. The October 9, 2011 Amendments to the Act, Along With Prior Drafts Thereof Make the Legislature's Intent that the Act Applies to Remote Transactions Unmistakably Clear

While the October 9, 2011 amendments to the Act appear to only deal with motor fuel dispensers, the actual language demonstrates the Legislature's intent to reaffirm that all transactions, either remote or face-to-face, are included under the Act's protection. This is demonstrated in two ways: 1. the amendments solely apply to pay-at-the-pump transactions, which includes gasoline islands with no attendant or person present; and 2. because the Legislature specifically granted gas stations an exemption to use personal information solely to verify credit cards and for no other purpose, 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.⁴

1. The Actual Amended Act

Subsection (3)(B) of the 2011 amendment to the Act, in creating a special exemption for motor fuel dispensers, notes,

The person. . . accepting the credit card in a sales transaction at a retail motor fuel dispenser or retail motor fuel payment island **automated cashier** uses the personal identification information solely for prevention of fraud, theft, or identity theft or uses the personal information for any of these purposes concurrently with a purpose permitted under paragraph (4).⁵

-
4. For purposes of this brief the term CCID refers to a credit card identification number, generally a three or four digit number in addition to the credit card number itself imprinted on the back of a credit card, used to prove a cardholder is in actual physical possession of the card for a “card not present” transaction. This is a common form of protection used against credit card fraud.
5. It should also be noted that Civil Code 1747.02 (n)(o) (the definition section) notes that a “retail motor fuel dispenser” is a device that can use a **remote electronic payment system, where an employee or agent of the seller is not present.** This provides further evidence that remote (card not present) transactions are and have always been covered by the Act, as motor fuel dispensers are the only type of remote transaction under the Act which allows personal information to be requested for card verification, identity theft and fraud prevention. Naturally, if all remote transactions were exempt, there would be no need at all to create this special exemption.

Naturally, if **all** cases of identity theft or fraud protection for remote transactions were already and automatically exempted from the Act, there would be no need to create a special exception for motor fuel dispensers. Similarly, the motor fuel island exception applies to automated cashiers as well, which is, in essence, virtually identical to a remote transaction (such as an Internet transaction, or self-checkout at a store) because it is done remotely by computer, as opposed to an in-person purchase. This provides further evidence that the Act applies, and has always applied to all forms of transactions, whether in-person or remote.

2. The Second to the Last Version of the Act

Even more instructive that the Legislature, without question 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. This prior May 17, 2011 version of the amended Act, makes all of the following crucial points:

Proposed subsection (i) notes,

It is the intent of the amendments made by this act adding this subdivision to **clarify existing law**. These clarifying amendments continue to protect personal identification information while allowing and recognizing the legitimate need for a person. . . to use personal information for the purposes authorized by this section. These amendments 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.

[Krescent RJN, tab “A”, pg. 7 Emphasis added].

As a matter of statutory interpretation under California law, when the Legislature uses such “clarification” language, it is not making a prospective, nor a retrospective amendment, but rather, stating what the law is, and has always been (*Stockton Savings & Loan Bank v. Massanet* (1941) 18 Cal.2d 200, 204). Thus, in clarifying, the Legislature noted, without doubt that the Act has **always** applied to card-not-present transactions, including those conducted over the Internet.

Additionally, proposed subsection (c)(3)(B) notes,

The person . . . accepting the credit card uses the personal identification information **solely** for prevention of fraud, theft, or identity theft or uses the personal information for any of these purposes concurrently with a purpose permitted under paragraph (4). [Krescent RJN, tab “A”, pg. 5 Emphasis added].

Furthermore proposed subsection (c)(6) [Krescent RJN, tab “A”, pg. 6] is specially designed for face-to-face situations where the credit card does not properly function or is not electronically readable, then the merchant is permitted to obtain personal information, and then immediately delete or destroy it. Naturally, if the Act only applied to in-person transactions, there would be no need to create a special subsection specifically designed to deal only with face-to-face transactions.

While these proposed sections ultimately did not make the final cut of the Act (the language solely creates a special exception for motor fuel

dispensers), 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.⁶ There would be no need to even consider rules regarding remote transaction identity theft protection prohibitions if the Act did not apply to card-not-present transactions. Similarly, if the Act applied **only** to face-to-face transactions, there would be no need to include a special subsection for face-to-face transactions. Rather the inclusion of these specialized subsections is further evidence that the Legislature believes the Act applies to **all** forms of credit card transactions, not simply those done in person.

The Amended Act, as well as those prior versions of the Act under consideration by the Legislature make it unmistakably clear, the Act has at all

⁶ In discussing whether or not there has always been an exemption in the Act for collection of PII for the purposes of fraud prevention, the Legislature noted in the 2011 amendments to the Act,

Specifically, ZIP codes are also used for fraud prevention purposes, or at a basic level, as part of the shipping address for an online internet transaction. 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.

While the courts may determine in current litigation, in response to the Pineda case, that such an exemption has always existed, this bill creates an express exemption. (Apple RJN, tab "H", page 3).

times applied to **all** credit card transactions, including those transacted in person, those done with an automated cashier, or computer, and those done remotely, such as fax, phone or Internet.

C. The Stated Legislative Purpose of the Act Would Not be Fulfilled if Millions of Internet Transactions Were Exempted

In originally passing the Act, the Legislature noted:

In practice, it often does not work that way. Credit card consumers should be entitled to the same privacy rights as those enjoyed by cash consumers, except to the extent required by credit card issuers to permit a retailer to complete a transaction.

AB 2920 seeks to protect the personal privacy of consumers who use credit cards to purchase goods or services by prohibiting retailers from requiring consumers to provide addresses, telephone numbers and other personal information that is unnecessary to complete the transaction and that the retailer does not need. (Apple RJN, tab “A” pg. 4).

More importantly, in a May 10, 2011 proposed amendment, in response to the lawsuits filed after *Pineda*, and when deciding to amend the Act (which ultimately only added the gas station exemption and nothing more) the Legislature noted,

.... Instead, the bill [an amendment to the Song-Beverly Act proposed in response to *Pineda* which originally contemplated a card “physically presented” requirement] currently in print would 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.

The bill in print would also expressly state that a retailer may collect personal identification information for purposes of preventing fraud, theft, and identity theft. However, as noted in the analysis, 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; and the provision that authorizes the collection of the information for purposes of fraud and theft prevention does not adequately limit the use and retention of information collected. Therefore the Committee analysis recommends a number of amendments so that the bill does not, unintentionally, undermine the important consumer protections of the Song-Beverly Act. (Apple RJN, tab "G" pg. 1, Underline in original, other emphasis added).

Later, the author of the proposed amendment noted,

Apparently to ensure that retailers could collect zip codes in order to prevent potential fraud when a card is swiped at an outside pump, or ships goods when a product is purchased on-line, the current language of the bill amends existing law to effectively provide that the provision prohibiting the collection of personal identification information to instances where a cardholder "physically presents" a credit card to a retailer, or merchant (page 2, line 4 of the bill in print.) This change to existing law, if allowed to stand, WOULD EFFECTIVELY REMOVE ON-LINE AND TELEPHONIC TRANSACTION FROM THE PROTECTION OF THE EXISTING STATUTE. ACCORDING TO THE SPONSOR, THIS WAS NOT THE BILL'S INTENT. Therefore, as noted in the proposed amendments below, the Committee strongly recommends that this language come out of the bill. (*Id.* at pg. 5, Bold caps added, underline only in original).

Were the May 2011 proposed amendments, as opposed to the final (October) version of the amendments to the Act passed, there would be no issue at all as the law would undisputedly apply to Internet transactions. However, as is more than clear from the proposed bill's author, the Legislature

believes the Act has always applied to all transactions, including remote ones, and wanted to absolutely ensure such protections were not removed by subsequent amendments to the Act. As far as the Legislature is concerned, the Act applies to Internet businesses and is gravely concerned that on-line consumers are entitled to privacy and that Internet businesses do not misuse the information, even if it is initially legitimately collected for fraud prevention.

As was further noted,

. . . . However, this provision does not impose any limits on what the retailer can do with the information once it is collected or how long the information may be retained. Therefore, as noted in the amendments listed below, the Committee strongly recommends that a clause be added to this provision stating that the information may only be recorded, stored, or retained to the extent necessary to effectuate the authorized purpose and thereafter deleted, discarded or destroyed. (*Ibid.*, Emphasis in original).

Therefore, while the May 2011 version of the amended Act ultimately failed to make the cut, instead resulting solely in a gas station exemption, the Legislature was more than clear both that existing law currently applies to Internet businesses, and that it is deeply concerned with abuse of such information by Internet businesses, if unchecked.

Furthermore, this Court and Court of Appeal are all in agreement that the stated purpose of the Act is to prevent merchants from acquiring any more information than is absolutely necessary to complete a credit card transaction. In *Pineda*, this Court held,

However, the legislative history of the Credit Card Act in general, and section 1747.08 in particular, demonstrates the Legislature intended to provide robust consumer protections by prohibiting retailers from soliciting and recording information about the cardholder that is unnecessary to the credit card transaction. Plaintiff's interpretation of section 1747.08 is the one that is most consistent with that legislative purpose. (*Pineda* at 536).

Virtually every Court of Appeal opinion is in accord, for example:

Our inquiry begins with the California Assembly Committee on Finance and Insurance, Background Information Request on Assembly Bill No. 2920 (1989–1990 Reg. Sess.): “AB 2920 seeks to protect the personal privacy of consumers who use credit cards to purchase goods or services by prohibiting retailers from requiring consumers to provide addresses, telephone numbers and other personal information that is *unnecessary to complete the transaction and that the retailer does not need.*” (*Florez v. Linens n’ Things* (2003) 108 Cal. App.4th 447, 452, emphasis in original).

Both the Legislature and the Courts all agree that the Act’s important consumer protection goals cover all businesses who accept credit cards. The purpose of the Act is to prevent merchants from overreaching in their personal information requests, and without question, exempting a significant portion of such transactions simply because they are transacted on-line would vitiate the Act’s protection for the majority of California consumers.

**VI. THIS COURT IN ADDITION TO MOST COURTS
THROUGHOUT THE COUNTRY, HAS HELD THAT INTERNET
BASED BUSINESSES ARE SUBJECT TO THE SAME RULES AND
LAWS AS OTHER BUSINESSES**

Apple spends much time of its brief arguing that because the Legislature did not have remote or Internet commerce in mind when it passed the Act in 1991, the Act must, therefore, only apply to brick and mortar stores which were the predominant form of commerce in 1991. The Legislatures lack of clairvoyance cannot be used as an argument that it only intended to regulate forms of commerce in effect in 1991. Indeed the opening section of the Act broadly states that the Act applies to all businesses. In this regard, it must be remembered that a credit card transaction over the Internet is simply a more advanced way for a merchant to sell goods or services to a consumer.

Changes in technology do not change the essence of the transaction. Indeed, cases throughout the country demonstrate that statutes apply in far greater scope than originally intended. Furthermore, cases throughout the country have had no problem applying existing laws and rules to Internet based businesses, many of which laws were passed when the idea of an interconnected network of computers transmitting data at an incredible rate over a series of cables (or even through the air itself) seemed to be pure science fiction.

For example, in *Snowney v. Harrah's Entertainment, Inc.* (2005) 35 Cal.4th 1054 (a case successfully argued by Plaintiffs' counsel in this case), this Court had no difficulty in unanimously extending traditional rules of minimum contacts under California's long arm statute to the defendant's Internet web presence. It is without question that when California's long arm statute was drafted, the Legislature never contemplated that people would one day transact business over the Internet yet, courts have all but unanimously held that purposeful availment over the Internet can form a basis of personal jurisdiction using a long arm statute. In noting that the Internet is subject to the same traditional rules of law as any other business, this Court held,

We need not, however, decide on a particular approach here because defendants' Web site, by any standard, establishes purposeful availment. By touting the proximity of their hotels to California and providing driving directions from California to their hotels, defendants' Web site specifically targeted residents of California. (See *Burger King*, supra, 471 U.S. at p. 472, 105 S.Ct. 2174.) Defendants also concede that many of their patrons come from California and that some of these patrons undoubtedly made reservations using their Web site. As such, defendants have purposefully derived a benefit from their Internet activities in California (*id.* at p. 473, 105 S.Ct. 2174), and have established a substantial connection with California through their Web site (*id.* at p. 475, 105 S.Ct. 2174). In doing so, defendants have "purposefully availed [themselves] of the privilege of conducting business in" California "via the Internet." (*Enterprise Rent-A-Car Co. v. U-Haul International, Inc.* (E.D.Mo.2004) 327 F.Supp.2d 1032, 1042–1043 [holding that a Web site that specifically targeted the forum state and its residents established purposeful availment].) (*Id.* at 1064–65).

Numerous other areas of law have similarly treated Internet businesses the same as any other business, for example:

1. Freedom of speech. Internet businesses are entitled to the same protections as traditional businesses, *Vo v. City of Garden Grove* (2004) 115 Cal. App.4th 425 (“We perceive no rationale by which CyberCafes should be accorded less protection than any of these older or more traditional businesses.” [*Id.* at 433]);

2. Infringement. In *BigStar Entertainment, Inc. v. Next Big Star, Inc.* 105 F.Supp.2d 185 (S.D.N.Y. 2000), the District Court stated,

This Court sees no reason why the approach to that assessment would be substantially different were the doctrine to be applied to the facts of this case and an infringement claim arising out of trademarks used for commerce conducted through the Internet. (*Id.* at 207).

Similarly, the Ninth Circuit had no problem holding that traditional Lanham Act infringement tests apply on an extremely similar basis to Internet based claims as well, such as was the case in *Brookfield Communications v. West Coast Entertainment Corporation* 174 F.3d 1036 (9th Cir. 1999).

3. Consumer Protection. Federal Courts have not hesitated to hold that consumer protection laws, even ones that do not specifically mention Internet businesses, still apply to business, even if they conduct their transactions over the Internet—even exclusively over the Internet. In *Ford Motor Company v. Texas Department of Transportation* 264 F.3d 493 (5th Cir. 2002), the Fifth

Circuit had no problem upholding a Texas law which prohibited automobile manufacturers from acting as dealers in Texas, which statute prevented Ford from directly marketing preowned cars to Texas residents over the Internet.

The Court noted,

When considering laws that **directly regulate internet activities, this alleged need for uniformity may well prevail.** However, application of this principle in circumstances like the instant case would lead to absurd results. **It would allow corporations or individuals to circumvent otherwise constitutional state laws and regulations simply by connecting the transaction to the Internet.** Section 5.02C (c) serves as a prohibition on **all** forms of marketing and sales by manufacturers, not just those conducted on the Internet. In the absence of Congressional legislation § 5.02C (c)'s incidental regulation of internet activities does not violate the Commerce Clause. (*Id.* At 505, emphasis added).

Additionally, and of critical importance is *Butler v. Adoption Media, LLC* 486 F.Supp.2d 1022 (N.D. Cal. 2007), holding that the Unruh Act applied to an Internet only business located in Arizona. In *Butler*, the Court held,

The court then noted that the Unruh Act is an anti-discrimination statute that contains no reference to Internet-content distribution, and thus, on its face, places no burden on interstate commerce. (*Id.* at 1053).

The *Butler* Court then applied the Unruh Act to the defendant, an Internet based business. The Unruh Act was passed many years before the Internet existed or was contemplated, yet the *Butler* Court had no problem determining that the Unruh Act's protections applied to California residents who used the defendant's Internet web site. Therefore, traditional laws need

not have considered the use of the Internet; rather, Internet based businesses are subject to the same rules and laws as any other business.

The Court of Appeal in examining the Song-Beverly Act has begun to determine that uses of technology can, in fact, violate the Act, even though not specifically mentioned therein. In *Powers v. Pottery Barn, Inc.* (2009) 177 Cal. App.4th 1039, the Court of Appeal had no problem determining that a request for an email address violated the Act. While *Powers*, at its heart is an opinion that holds that the Can-Spam (a Federal law) does not preempt the Song-Beverly Act, *Powers* also, implicitly affirmed the trial court's other ruling that the request for an email address violated the Song-Beverly Act. The Act does not specifically state that a merchant is prohibited from asking for an email address (an email address is not included in the specific definition of personal information and did not exist in any meaningful form when the Act was passed), nor did the Legislature apparently "consider" whether or not asking for an email address is a violation of the Act, yet the Court of Appeal had no problem finding that asking for an email address is a request for personal information in violation of the Act.

Furthermore, the law is rife with examples of statutes expanding greatly in scope as to the original intent. For example the Home Solicitation Act (Civil Code § 1689.5), or the now commonly used SLAPP motions. The Home Solicitation Act with its three day right of rescission was generally meant to

allow homeowners to avoid the nuisance of door-to-door peddlers, yet it applies to any contract signed in a consumer's home, even if the customer initiated the call (*see e.g. Weatherall Aluminum Products v. Scott* (1977) 71 Cal. App.3d 245). Similarly, the original intended purpose of the anti-SLAPP law was to prevent lawsuits designed to prevent interference with Constitutional rights (*see e.g., Contemporary Service Corp. v. Staff Pro, Inc.* (2007) 152 Cal. App.4th 1043, 1053), yet, as this Court is aware, SLAPP motions now have an incredibly broad use, well beyond the original intended purpose.

Therefore, 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. The Legislature could have limited the Act, and could have stated the Act does not apply to any transaction where the merchant does not actually physically obtain the credit card (or to simply exempt remote or card not present transactions), yet the Legislature deliberately chose not to do so, instead opting for as broad a protection as possible. Thus, even though Internet commerce did not exist in any realistic form when the Act was passed, does not mean that a more technologically advanced form of a purchase transaction is excluded.

**VII. THE PURPOSES AND PROTECTIONS OF THE ACT WOULD
BE EVISCERATED FOR MILLIONS OF CALIFORNIA CONSUMERS
IF INTERNET RETAILERS ARE CARTE BLANCHE EXEMPTED
FROM THE ACT**

*1. Exempting Internet Businesses Would Destroy Consumer Protection
and is an Overreaching Solution to the Identity Theft and Credit Card Fraud
Problem*

Admittedly, credit card fraud and identity theft are problems of great concern. However, of equal concern is overreaching by merchants seeking far too much information for their own marketing or other business purposes. Apple is, if anything, disingenuous in its request for complete exemption from the Act, when a limited purpose information request (e.g. the right to request **only** as much information as is actually required to verify a credit card, and nothing more, and using such information only for that purpose and no other) will satisfy the goals of fraud and identity theft protection, much like the gas station exception.⁷ It is possible that credit card verification would fall under

7. It should be noted that in opposition to the demurrer, by and through an offer of proof, to support an amended complaint if necessary, Plaintiff's counsel submitted a declaration stating that he did not believe that Apple or any other business currently uses a phone number to verify a credit card under any circumstance. This assertion was based upon research done with credit card processing companies. While this does not rise to the level of evidence presented at trial, it without question presents some evidentiary support that companies

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. Apple, like any other defendant would have the burden of proving by actual evidence that a business actually needs and uses each specific piece of information requested (e.g. telephone number, address, zip code only, etc.) for credit card verification, and uses such PII only for that purpose and no other. Naturally, if the (c)(3)(a) or (c)(4) exceptions to the Act were read to permit credit card verification as necessary to complete the transaction, it would not be the proper subject of demurrer and would require an evidentiary hearing or trial to determine what, if any, information each business uses for credit card verification, and that each piece of information requested or required is actually used for the purpose of credit card verification, *and nothing else*.

If Internet businesses are deemed wholly exempt from the Act, then they will be able to request any information from credit card consumers they wish, including not only information such as address and phone number, but also

do not simply ask for consumers' personal information solely for credit card verification and no other purpose, because it appears phone numbers are not used for credit card verification. Naturally if Internet based companies request, require and record information such as a phone number which is unnecessary to verify the credit card, they have without question violated the Act. (Exh. 21, pgs. 388-390).

sensitive information such as social security numbers, maiden names, or a whole host of other personal information absolutely unnecessary to the simple purpose of buying a good or service on-line. This would also allow the business to do anything it wishes with the information, including marketing, sharing with partners, or even selling the information to the highest bidder. Without the protections of the Act, credit card consumers would face the Hobson's choice of providing an Internet retailer with a host of personal information the retailer does not need, knowing the retailer can make any use of the information it wishes if the consumer chooses to make a purchase from an on-line retailer.

2. Exempting Internet Businesses from the Act Would Lead to Inconsistent, Unfair and Absurd Results for California Consumers

Why should a consumer give up all of his or her rights of privacy simply because he or she chooses to shop from the convenience of a computer as opposed to driving to a retail store? A purchase of goods or services from an Internet retailer is still the same basic transaction as a retail store, the consumer pays money for goods or services. The following hypotheticals illustrate how unfair it would be to permit merchants who use the Internet to be exempt from the Act:

A customer wishes to purchase the identical shirt with his or her credit card from a department store which sells via retail stores, a phone/fax catalog,

and an Internet website:

1. The customer can walk into the store and purchase the shirt with his or her credit card. It is beyond question that the retail store would not be permitted to ask the customer for his or her telephone number or address prior to payment via credit card, regardless of reason (*see Florez v. Linens n' Things* (2003) 108 Cal. App.4th 447);

2. The customer can place a phone or facsimile order for the shirt from the store's catalog. As written, the Act forbids the retail store from asking for a phone number or address, however, the address may very well qualify under the "special purpose" exception found in (Civil Code § 1747.08 (c)(4)), as the store needs an address to ship the shirt.

3. The customer can visit the retailer's Internet commercial web site and order the shirt on-line. As written, the Act forbids the retailer from asking for a phone number or address, however, the address may very well qualify under the "special purpose" exception found in (Civil Code § 1747.08 (c)(4)), as the merchant needs an address to ship the shirt.

Under scenarios 2 and 3, unless the retailer's credit card processing company requires the retailer to provide a billing phone number for security and the transaction cannot be completed without it, there is no valid reason for the retailer to ask the customer for his or her phone number. Indeed, even Apple must concede that it cannot ask for an address or phone number from

any credit card consumer who makes a purchase in one of Apple's numerous retail stores. The need for personal information is far less compelling in Apple's web site situation since every on-line purchase is downloaded, and there is no need to have any physical goods shipped to an address.

Take a second hypothetical, a customer in a retail store has the right to either make a purchase at a cashier, or use the self-checkout line (many stores now have devices where a consumer can scan items and pay directly without the use of a cashier to process their transaction at all).

1. It is without question that a cashier cannot ask the customer for a phone number or address in line with a credit card purchase;

2. What if after using a self-checkout, the computer asks the customer to input his or her phone number and address on the computer screen before paying with a credit card?

The transaction in scenario 2 (self checkout with a personal information request) is still in a brick and mortar store, yet there is no opportunity for a cashier to "verify" the card by the request for a driver's license, or to "inspect" the purchase to see if something appears wrong. If anything, a self-checkout is virtually identical to an Internet purchase—it is a purchase that is not made face to face, but is made through a computer interface. Thus, the place of purchase (whether in store or over a computer) cannot be, in and of itself, conclusive of a merchant's right to request information. If certain information

is necessary for credit card verification, it is likely exempt under the statute, however, if the information requested exceeds what the merchant needs to complete the transaction, the Act is violated.

Exempting Internet businesses from the Act would lead to absurd and unfair results. Under hypothetical 1, the same consumer buying the same item from the same retailer using the same credit card would in the case of having to drive to the store, be able to make his or her purchase without providing the merchant information the merchant did not need to complete the transaction, yet, should the consumer chose to purchase the identical item at home, then the consumer would be required to provide the merchant with a host of personal information, even information the merchant clearly does not need to process and complete the transaction. It is understandable that a remote transaction may require providing some more information to verify the credit card, but clearly not to the extent most merchants request. For example, suppose (as Plaintiff has plead in the complaint), the merchant's website does not need or use the consumers telephone number or address to verify the credit card. Providing this unnecessary information serves no purpose other than to build the merchant's marketing list, and possibly line its pockets by selling or bartering the information. If Internet businesses are exempt, then all consumers who chose the convenience of on-line shopping are required to trade their privacy for such convenience.

3. Internet Businesses Like all Businesses Who Engage in Card-Not-Present Transactions Have a Whole Host of Remedies to Verify Credit Cards

Generally, a merchant processing a remote transaction is offered a whole host of verification checkpoints exclusive of personal information when processing a transaction including: 1. The card number; 2. The expiration date; 3. The cardholder's name (or name on the credit card) and 4. The CCID. In some circumstances, possibly more information may be needed or used to verify the credit card, yet, as this is a demurrer, there is no evidence in the record to support any claims that Apple or any other merchant, actually uses PII to verify credit cards or prevent identity theft or fraud.

4. There are Also Social Policy Concerns Relating to Businesses' Recording of Consumer Information, Causing as Much Concern as Identity Theft

The Legislature has already conducted a careful balancing when passing the Act, and it has decided the amount of information a business may request and record—only as much as is absolutely necessary to complete the transaction, and nothing more. While 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:

A. The concern of security hacks at the business level

The news is filled with recent articles of major corporations having their data hacked and countless pieces of consumer personal information stolen. For example, a recent article notes massive hacker attacks on large companies such as Citigroup, Google and Sony, resulting in the theft of millions of consumers' information (**Los Angeles Times**, Tiffany Hsu, March 31, 2012, Page B2 Breach of Credit Card Data Feared). Without question there is a danger to corporate retention of consumer information, as corporate files are a large storehouse of information, that, if hacked, allows criminals (or dishonest employees) to efficiently obtain data on large numbers of consumers at once, rather than having to steal information on an individual basis. Therefore, while Apple suggests that it needs information to combat identity theft and fraud (a claim vigorously disputed by Plaintiff), in fact, retention of data centrally stored serves as a treasure trove of information ripe for theft by criminals.

B. Merchants may misuse the data once they have it

A recent Los Angeles Times article may sum up consumers' fears best:

The vast majority of Californians surveyed in a state-wide poll are worried about the data collected by Internet and smartphone companies, and most said they distrust even firms known for their ardent fans and tens of millions of daily users. . . . [the] poll also said they were wary of firms collecting personal information without their knowledge and were concerned that personal data could become public or be harvested to sell them products. (**Los Angeles Times**, David Sarno, April 1, 2012, Page 1, Californians Wary of Data Gathering).

Another goal of the Act is to prevent not only the acquisition of consumer information, but the misuse (such as marketing purposes) as well. Consumers are often given a Hobson's choice when purchasing from an Internet retailer—provide significant amounts of personal information in order to obtain the good or service desired, or walk away from the transaction. It is no secret that the consumer is likely to be bombarded by emails, mailed solicitations, or possibly calls at home all seeking future business. Perhaps this information will also be sold or bartered with the merchant's "preferred partners," or simply sold to the highest bidder(s).

Targeted consumer information is a valuable commodity. While a consumer may wish to provide this information voluntarily (e.g. in exchange for coupons, to join a discount club, or perhaps they wish to receive future offers), it is unfair to require PII be provided when it is unnecessary. For example, as was discussed in *Gass v. Best Buy Co., Inc.* WL 538251(C.D. Cal Feb. 2012),

Plaintiffs explain to the Court that customers' PII is valuable. Plaintiffs quote FTC Commissioner Pamela Jones Harbour as follows: "Many consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit."

Arguably the situation presented in this case is precisely what the California Legislature intended. Before the Act, companies could gather PII from their customers for free, by conditioning the completion of a

credit card transaction on the customer's provision of PII. After the passage of the Act, a business that wishes to collect PII from its customers must give the customer some incentive to provide it. Many companies have done what Best Buy has chosen to do—offer to essentially “buy” PII from customers for coupons and discounts. Many customers will decide this is a worthwhile trade and provide their PII willingly. Other customers will decide to safeguard their PII and refuse the offer. (*Id.* at *12, fn. 7).

Consumer privacy can and will be violated if Internet merchants are exempt from the Act. A consumer should not be forced to walk away from a transaction solely because he or she does not want to be bombarded with future marketing efforts, or the knowledge that their private information may very well end up in the hands of various other companies. This is why the Act exists, and this is why the Court must also hold that it applies to Internet based businesses.

VIII. APPLE'S CLAIMS BASED UPON OTHER CALIFORNIA STATUTES AND CONSTITUTIONAL CHALLENGES ARE RAISED FOR THE FIRST TIME ON APPEAL AND WERE THUS WAIVED. FURTHERMORE, SUCH CLAIMS DO NOT PREEMPT THE ACT OR OTHERWISE EXEMPT INTERNET BUSINESSES

Apple offers two theories for the first time on appeal, (1) that COPPA occupies the issue of Internet information requests, and (2) that there are Constitutional challenges to applying the Act to Internet businesses. At the outset, Apple did not offer these theories in its demurrer presented to the Trial

Court (Exh. 25, pgs. 410-427). Therefore, as arguments offered for the first time on appeal, they are waived and cannot be advanced for the first time in this Court (*Western Oil & Gas Assn. v. Monterey Bay Unified Air Pollution Control District* (1989) 49 Cal.3d 408, 427, fn. 20). It should be noted with regards to the Constitutional issues, in its reply brief in support of its demurrer, Apple stated,

However unwise such a decision may be, Defendants reserve, but do not challenge in this demurrer, the Legislature's powers to impose regulations such as the Act on internet retailers. This demurrer simply asks the Court to follow the Legislature's intent, and Plaintiffs' contention that the Legislature *could* have chosen to apply the Act to internet retailers does not mean that the Legislature intended to do so. (Exh. 25, pg. 421, emphasis in original).

Even if these new arguments are considered, they are not persuasive.

A. The Passage of COPPA Does Not, in any Way Demonstrate an Intent to Remove the Protections of the Song-Beverly Credit Card Act for California Consumers

Passed in 2003 COPPA (Business and Professions Code § 22575 et seq.) is a law with few teeth. It merely states that Internet web sites must state what information is collected, and what privacy policy is then in place regarding the information collected. It further states that violations can be corrected within 30 days of notice of a violation, and notes that the law can be violated either negligently or intentionally. There is no remedy provided in the statute. Nowhere does this law state that Internet retailers are allowed to collect

information that is otherwise prohibited by other laws. COPPA's only requirement is that a privacy policy be posted and nothing more. Thus, COPPA does not provide specific permission to collect PII, it merely requires collectors to post a privacy policy. Similarly, consumers are provided no remedy for the failure of web site operators to adhere to this law. COPPA is hardly a comprehensive regulatory scheme relating to all data collection over the Internet, rather, it provides one basic requirement—if a business wishes to collect information, it must post a privacy policy, nothing more and nothing less. COPPA provides no statement that a business can collect any information it wants, whether otherwise prohibited by law or not, by merely posting its privacy policy.

Contrast this law with the Song-Beverly Credit Card Act, specifically designed to prevent any merchants from asking for more information than is necessary to complete a credit card transaction. A specific law, designed to prevent a specific information request in credit card transactions. Indeed, the laws have very little, if any, interplay at all. The fact that an Internet web site is required to post a privacy policy as to the data it collects is not a “blessing” to collect any information it wants. Certain information cannot be collected under either state or federal law (for example, information pertaining to minors under the age of 13 [15 U.S.C. §§ 6501-6506]), and clearly COPPA cannot trump the provisions of other statutes. For example, if California passes the

Social Media Privacy Act (SB 1349 [prohibiting prospective employers from asking for social media passwords]), the mere fact that an employer who accepts job applications on-line also has a privacy policy would not then give that employer a right to collect social media personal information because it is otherwise prohibited by law. Here, the Song-Beverly Act forbids the collection of any PII not necessary to complete a credit card transaction.⁸ Therefore, because businesses are forbidden by the Act from collecting certain PII, the mere fact that a business posts a privacy policy does not then permit such forbidden PII to be collected.

B. There is no Basis to Challenge the Act on Constitutional Grounds Because the Act Does not Specifically Regulate the Internet or Internet Commerce, Rather it Applies Equally to all Businesses

Holding that Internet businesses may not ask for any more information than is necessary will neither result in a credit card identity theft Armageddon, nor will it place a substantial burden on interstate commerce. Federal Courts have already examined this argument and resoundingly rejected it on the very

⁸. If anything, the Legislature's concern for ensuring that the amended 2011 version of the Act (which occurred almost eleven years after COPPA's passage) did not remove the Act's protection for on-line consumers, demonstrates that the Legislature does not believe COPPA occupies the legislative field of Internet information, and that the Song-Beverly Credit Card Act protects the information of on-line credit card consumers. (See Apple RJN, tab "G" pgs. 5-6).

basic premise that if such arguments were permitted, all businesses would simply take to the Internet to avoid a whole host of consumer protection laws. A merchant that chooses to transact business with citizens of all 50 states is responsible for complying with the laws of all 50 states, Internet or not. Apple, of all corporate defendants is in no position to complain about being subject to California consumer protection laws, it is a California corporation, has its principal place of business in California, and most importantly, its contracts contain a choice of law clause (California law) and a choice of venue clause (California) (Exh. 3, pg. 25). Therefore, every contract Apple enters into is based upon California law, and all suits against Apple by any person nationwide must be brought in California. It can (at least for purposes of demurrer as there is no evidence before the Court) be fairly said that because Apple's principal place of business is in California, every transaction, even those done over the Internet have a connection to, if not, are wholly located in California.

Federal and state courts have drawn a distinction between a law designed to regulate the Internet itself, versus a law that is a state-specific consumer protection law that incidentally affects Internet commerce. While there may be Constitutional issues relating to a law that seeks to regulate the Internet (an issue that is not present here), no such concerns arise when dealing with a consumer protection law that tangentially affects Internet businesses.

In *Ford Motor Company v. Texas Department of Transportation* 264 F.3d 493 (5th Cir. 2001), the Fifth Circuit had no problem upholding a Texas law which prohibited automobile manufacturers from acting as dealers in Texas, which statute prevented Ford from directly marketing preowned cars to Texas residents over the Internet. The Court noted,

When considering laws that **directly regulate internet activities, this alleged need for uniformity may well prevail.** However, application of this principle in circumstances like the instant case would lead to absurd results. **It would allow corporations or individuals to circumvent otherwise constitutional state laws and regulations simply by connecting the transaction to the Internet.** Section 5.02C (c) serves as a prohibition on **all** forms of marketing and sales by manufacturers, not just those conducted on the Internet. In the absence of Congressional legislation § 5.02C (c)'s incidental regulation of internet activities does not violate the Commerce Clause. (*Id.* At 505, emphasis added).

The Song-Beverly Credit Card Act is not an attempt to regulate the Internet, it is a consumer protection statute that applies equally to all businesses. California Courts of Appeal are in accord. For example in *Ferguson v. Friendfinders, Inc.* (2002) 94 Cal. App.4th 1255, the Court of Appeal had little problem holding that a corporation that sent unsolicited misleading e-mails was in violation of **Business and Professions Code § 17538.4.** The Court, in conducting an analysis under the dormant Commerce Clause (there, against an out of state business, unlike Apple who is a California business), held that California's law regulating the sending of misleading

unsolicited emails violated Business and Professions Code § 17538.4. The Court determined that section 17538.4 did not regulate “the Internet or Internet use per se” rather it regulated entities that do business in California, or sent emails to California residents (*Id.* at 1264). The Court further noted,

. . . . That respondents consider section 17538.4's requirements inconvenient and even impractical does not mean that the statute violates the Commerce Clause. Further, if respondents choose to comply with section 17538.4 all the time (so they can avoid having to determine whether they are corresponding with California residents via equipment located in California), that is their business decision. Such a business decision simply does not establish that section 17538.4 controls conduct occurring wholly outside California. (*Id.* at 1265).

Finally, the Court of Appeal noted that the law in question supported a significant local interest, of which California had a substantial interest in protecting its citizens from deceptive unwanted junk e-mail, and there was virtually no burden on interstate commerce.

Apple's due process and interstate commerce concerns are much like the ones argued above in *Ferguson*, and which arguments have been otherwise resoundingly rejected. With 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. There is no precedent to support this concern, as no court has ever held that merely asking the state of residence violates the Act. It would appear that many of the concerns, even those in *Pineda* are not present when a retailer merely asks for the state of residence,

as such information would be unlikely to help with building a marketing profile. Moreover, it is entirely possible that simply asking for the state of residence would qualify under the subsection (c)(4) defense, as it may very well be considered reasonably necessary for a merchant to inquire into the state of residence (with nothing more) to determine if the law even applies.⁹ Therefore, concerns about Internet regulation and due process relating to each user's residence are unfounded and do not come close to the level of a Constitutional deprivation of due process of law.

With respect to burdens on the Commerce Clause, *Ferguson* and *Ford Motor Company supra* 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, by mere virtue of taking their business on-line, be able to avoid consumer protection laws of all 50 states by claiming an inability to comply with any of them.

Further, it cannot be argued that the Act discriminates against out-of-state businesses, because collection of unnecessary PII is forbidden to all

⁹ It is also likely that because of Apple's choice of law and choice of venue contract provisions that the Act applies to every transaction Apple enters into with a United States resident, completely allaying this concern all together.

merchants. Similarly, Apple is a California business that has chosen to apply California law to its contracts so it, of all businesses, cannot be heard to complain about having to comply with California law. For example, Civil Code § 1770 (a)(4) forbids deceptive representations about geographic origin (e.g. “Made in the USA” such as was the case in *Kwikset Corp v. Superior Court* (2011) 51 Cal.4th 310) and subsection (a)(11) and (12) forbids advertising unassembled furniture without stating it is unassembled or noting an assembly price. It is possible other states do not have such prohibitions or protections, yet clearly, a merchant, be it by sending catalogs or transacting business on-line must comply with these laws when dealing with California residents. Thus, a merchant cannot claim immunity from existing state laws merely by claiming it will be held to the standards of many different states. If the merchant wishes to do business with California residents, it must comply with existing consumer protection laws, and cannot claim a Constitutional defense based upon its decision not to comply with existing law (*see e.g. Bland v. Fessler*, 88 F.3d 729 (9th Cir. 1996), *certiorari denied* 117 S.Ct. 513, 519; *People v. Western Airlines, Inc.* (1984) 155 Cal.App.3d 597, *certiorari denied* 105 S.Ct. 815).

Indeed, its “geography” argument is precisely the argument that was rejected in *Ferguson*. Like the analysis in *Ferguson*, without question any incidental burden on interstate commerce (with a California business) is

heavily outweighed by California's strong interest in preventing the overbroad request, and misuse of consumers' private personal information by merchants. Apple need not apply California law to every transaction (even though, by contract it has chosen to do so). There is no case holding that a merchant cannot ask for the state of residence (or that merely inquiring into state of residence would not fall under a statutory defense to the law), and if the resident is a California one, adjust its information requests accordingly.

Furthermore, under the *Pike* balancing test, it is beyond question California has a strong interest in protecting its consumers' private information from overreaching merchants. This could not be more clear than in the language of the Act itself and in the judicial opinions including this Court's recent *Pineda* decision. Conversely, there is little or no burden on interstate commerce. If, as is suggested below, 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, then there is no burden whatsoever. Conversely, if Apple is exempt, it can ask for any information it wants, whether necessary to the transaction or not, and make any use of such information in any way it wants—in direct contrast to the policy goals promoted by the Act. If the Act does not apply to the Internet or on-line businesses, millions of California consumers will lose all rights of privacy by transacting their business on-line. Apple has demonstrated no burden it will suffer by

having to either determine the state of residence before asking for personal information, or having to limit its requests solely to that information that is permissible by law.

There 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). If Apple were required to collect and maintain (an address but possibly not a phone number) information for tax purposes, clearly, such conduct is permitted as a defense under the Act.

Apple has presented no information that a landslide of fraud would occur by persons lying to Apple about their state of residence (generally over the purchase of a \$.99 app) so that a thief would not have to provide any further information in a stolen credit card scheme. Furthermore, as Plaintiff has suggested, Apple may have a defense to the Act if the information requested is reasonably necessary for the completion of a credit card transaction. As such, to the extent Apple can prove to a trier of fact that it actually needs and uses each piece of information to verify a credit card is not stolen, it is entitled to such information. Asking for a complete exemption,

however, is not the answer. If Apple were permitted, under the statute to: 1. verify the state of residence to ensure the law applies (choice of law contractual provisions notwithstanding); and 2. use all of such information to prevent credit card fraud or theft (likely as a statutory defense under subsection (c)(4)), then there would be no Constitutional concern whatsoever, because Apple, or any other business would have no issue verifying the state of residence.

IX. CONCLUSION

Applying the Song-Beverly Credit Card Act to Internet businesses like all other businesses will not result in the identity theft Armageddon Apple suggests. Quite the contrary the Act will protect consumers like it always has—from merchants requesting more information than they need to actually complete the credit card transaction, nothing more, nothing less. As drafted, the Complaint alleges Apple did not need Plaintiff's telephone number or address to complete his purchase of digitally downloaded apps often costing less than a dollar each. Plaintiff has alleged that Apple did not, in fact need or use his telephone number or address to verify Plaintiff's credit card for identity theft or fraud protection—this must be presumed true.

This notwithstanding, Plaintiff does not mean to suggest that an Internet business may never ask for an address or possibly a phone number, but, it may only do so when absolutely necessary to verify a credit card. Merchants are entitled to statutory defenses in the event of a contractually imposed obligation

to collect PII, or if the collection is required for a special purpose incidental but related to the transaction. Verification of state of residence (to determine if the law even applies) and identity theft protection may very well qualify under one of these defenses. If a merchant can demonstrate that the merchant's credit card processing company requires the collection of such data by contract or can demonstrate that each and every requested piece of PII is related to the transaction and reasonably necessary to verify the credit card, and that the PII is actually used by the merchant for credit card verification (and not also used for other improper purposes such as marketing or sale to other businesses) then the merchant may very well have a defense under the Act. However, the Complaint has alleged Apple did not use Plaintiff's PII for credit card verification, but instead, used his PII for Apple's own business purposes. Permitting Internet businesses to obtain more information than is necessary will allow these merchants to acquire as much data as they wish (forcing consumers into a take it or leave it choice to provide more information than they want, forego the convenience of an Internet based purchase or quit the transaction all together), and to make any use of the data they wish, including marketing or even the sale or barter of consumers' private information.

Exempting all Internet businesses would allow them to collect more data than is necessary from consumers and make any use of it they wish—which is clearly inapposite to the goals of the Act—preventing merchants from

obtaining any more information than is necessary to complete the transaction. If Apple did not actually use David Krescent's telephone number and/or address to verify his credit card, then why should Apple be allowed to require Krescent to provide that information, potentially making all sorts of uses of the data, many of which Krescent would prefer Apple not do. The answer is that under the Act, Apple is not permitted to request or require such information unless it can make a showing that it actually needed and used each and every piece of information requested to verify the authenticity of the credit card.

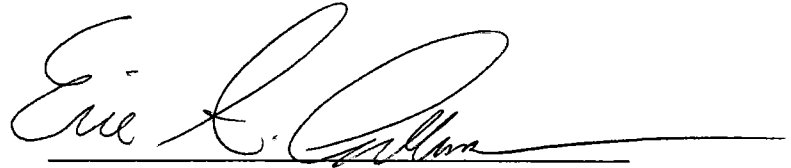
The Act was written broadly, covering all credit card purchase transactions. The Legislature intended to provide robust consumer protection by preventing just the type of conduct alleged here, requesting and requiring more information than is necessary to complete a credit card transaction. Millions of consumers who chose the convenience of Internet shopping will lose out on these protections if Internet businesses are permitted to request or require consumers to turn over all kinds of information unnecessary to complete their transactions. The Trial Court was absolutely correct in determining that the Song-Beverly Credit Card Act applies to all businesses who accept credit cards, even those that transact their business remotely over the Internet. This Court must uphold the goals and purposes of the Act, and hold that the Song Beverly Credit Card Act applies to all forms of credit card transactions, including those conducted over the Internet.

Therefore, the ruling of the Trial Court must be affirmed. Plaintiff respectfully requests that he recover his costs of this proceeding.

Respectfully Submitted,

DATED: May 29, 2012

SCHREIBER & SCHREIBER, INC.

A handwritten signature in black ink, appearing to read "Eric A. Schreiber", written over a horizontal line.

ERIC A. SCHREIBER, Attorneys for
PLAINTIFF AND REAL PARTY IN
INTEREST DAVID KRESCENT
individually, and on behalf of a class of
persons similarly situated

[← Back to Original Article](#)

Visa, MasterCard warn of possible data breach

The companies don't specify how many credit card holders could be affected. None will be held liable, Visa says.

March 31, 2012 | By Tiffany Hsu and E. Scott Reckard, Los Angeles Times

MasterCard Inc. and Visa Inc. warned that some of the data in their cardholder accounts may have been breached.

MasterCard said that it had notified banks, as well as law enforcement, of a potential problem with a third party "U.S.-based entity."

An independent data security organization is conducting a forensic review, MasterCard said. The company's own systems haven't been compromised. Visa said the same.

"MasterCard is concerned whenever there is any possibility that cardholders could be inconvenienced and we continue to both monitor this event and take steps to safeguard account information," the company said Friday in a statement, without specifying how many cards might be at risk.

Visa said in a statement that it had handed over affected account numbers to card issuers who would, if necessary, reissue cards. Cardholders won't be held responsible for fraudulent purchases, Visa said.

Earlier, the blog Krebs on Security wrote that MasterCard and Visa had told banks that the "major breach" could involve more than 10 million card numbers compromised between Jan. 21 and Feb. 25. The post noted that the affected information could be used to make counterfeit cards.

Last year, hackers attacked large amounts of consumer information at firms including Citigroup, Google and Sony.

MasterCard and Visa don't directly issue credit cards; they process card transactions for the banks that do.

The Privacy Rights Clearinghouse, a San Diego nonprofit organization, tallied more than 535 data breaches last year involving more than 30.4 million sensitive records. The organization, which publishes a chronology of known data breaches, said it has added up an "alarming" total of 543 million compromised records in the United States since 2005.

Director Beth Givens said that number was only a "sampling." Not all data breaches come to the attention of news organizations, she said, and many states have no requirement that companies report breaches to an official clearinghouse.

tiffany.hsu@latimes.com

scott.reckard@latimes.com

latimes.com/news/local/la-fi-privacy-poll-20120331,0,2763981.story

latimes.com

USC Dornsife / Times poll

Tech firms' data gathering worries most Californians, poll finds

Trust is low even for the most widely used Internet and smartphone companies, such as Google, Facebook, Twitter and Apple.

By David Sarno, Los Angeles Times

8:04 AM PDT, March 31, 2012

advertisement

California's high-tech firms make the world's most popular smartphones, social networks and search engines, but there's one asset they're struggling to build: trust.

The vast majority of Californians surveyed in a statewide poll are worried about the data collected by Internet and smartphone companies, and most said they distrust even firms known for their ardent fans and tens of millions of daily users.

Many of those surveyed in the latest USC Dornsife/Times poll also said they were wary of firms collecting personal information without their knowledge and concerned that personal data could become public or be harvested to sell them products.

The results of the survey, which draw a stark picture of the public's attitude on privacy, come as policymakers ramp up efforts to pass laws aimed at protecting personal information on users' whereabouts, interests and social activity. In recent months, federal lawmakers have held numerous hearings about the need for privacy laws, and Obama administration officials recently renewed their call for Congress to pass online privacy legislation.

"It reaffirms my opinion that privacy is a big deal — and it's becoming a bigger deal," Rep. Joe L. Barton (R-Texas) said of the poll results. Barton, who cosponsored a privacy bill pending in Congress, said lawmakers are "gaining ground" in their years-long battle to write data privacy into law.

The findings of the survey, conducted for the USC Dornsife College of Letters, Arts and Sciences and the Los Angeles Times, were consistent with a poll released last month by the Pew Research Center, which found that 68% of respondents did not approve of targeted Internet advertising if it meant having their online behavior tracked and analyzed. Pew has said that nearly 3 in 4 Americans now use search engines, and two-thirds use social networks. Nearly half of adults in the U.S. own smartphones.

The USC Dornsife/Times poll revealed that the rise of digital culture is mirrored by Californians' sense of the technology industry's importance to the state economy, with 65% of those surveyed saying the technology business was more economically important than the state's other marquee industry, entertainment.

But the increasingly central role of technology in the lives of consumers did little to inspire trust in Silicon Valley's star companies. Respondents were asked to rate six on whether they trusted the companies to be responsible with personal data. On a 10-point scale, with zero meaning no trust and 10 meaning complete trust, none scored above five, and most hovered around three.

Apple was highest with a mean score of 4.6, followed by Google at 3.8. LinkedIn scored 3.0, while online video site YouTube was rated 2.8. Facebook was next to last, with a score of 2.7, only slightly above Twitter at 2.4.

"I thought the ratings were strikingly low," said Linda DiVall, the president and founder of American Viewpoint, one of the polling firms that conducted the survey. "If I were involved with the branding image of those companies, I would be very concerned."

DiVall said that the public tends to have low regard for most government, religious and business institutions — but that people give the lowest ratings to organizations with which they have the least direct contact. In the case of companies like Apple, Facebook and Google, however, many consumers use their devices and websites every day.

The poll was conducted by telephone March 14-19 with 1,500 registered California voters. It has a margin of sampling error of plus or minus 2.9 percentage points.

None of the companies mentioned in the survey would comment on the results of the poll.

But Linda Woolley, a representative of the Digital Advertising Alliance, an industry marketing consortium supported by hundreds of Internet, automotive, financial and healthcare firms, said the poll results were not telling the whole story.

"If somebody came up to me on the street and said, 'Are you concerned about online data practices?' I'd say yes," she said. But, she said, most people would be thinking of problems like identity theft and credit card fraud rather than what most firms use the data for: to more efficiently sell people products they want.

"I don't care whether you're in the hotel business or the travel business, or selling soap — every company is talking about personalization," she said. "What data enables you to do is cater to the customer and really make them feel like you're taking care of them."

Of those who said they were concerned about data privacy, one-quarter said they were most uneasy about their personal information being collected without their permission or knowledge, while 21% said they were more worried about their information becoming public. A smaller group, 18%, said their chief concern was either that companies could use their personal information to make money or that they would sell it to marketers. Nearly one-third said they were equally concerned by all of these

possibilities.

Andrew Hanson, 23, a warehouse manager in San Clemente, said he believed companies' use of personal data worked in consumers' favor.

"I don't look at it as an invasion of privacy. I look at it as almost like extreme marketing," he said. "They're just trying to get advertising out there, and if anything, it's helping me out."

But most were wary about the growing ability of companies to monitor — and monetize — a variety of consumer behaviors.

"What I do is nobody's business but my own as long as I'm a law-abiding citizen," said Gloria Maldonado, 70, a retired teacher in Redwood City. "I'm very concerned about the overreach."

Privacy controversies continue to trip up the companies most closely associated with the digital revolution.

In March, when Google rolled out a privacy policy that allowed it to collect and share user data from across its search engine, email, video, mapping and other services, the move was widely criticized. The critics included a group of federal lawmakers who questioned whether Google's users would be able to prevent the company from collecting data about them.

In February, popular social media services including Twitter, Foursquare and Instagram acknowledged that they were reaching into users' smartphones and grabbing personal contact information without explicit permission. Many of the companies changed the way their applications worked to make the data collection optional.

And last April, researchers discovered that Apple's iPhone kept a detailed log of its precise whereabouts, storing up to a year's worth of user location data. The company altered the phone's software so it stored a much smaller cache of location data.

Conscious of the rising tide of privacy snafus, legislators have proposed more than a dozen privacy bills, but none has made it through Congress.

Rep. Edward J. Markey (D-Mass.), who along with Barton of Texas introduced a bill last May to protect the personal information of children online, acknowledged that widespread privacy concerns have not stopped millions from using the services that are monitoring their online activity.

"People drove automobiles before there were seat belts or air bags," Markey said. "But as time progresses, in the same way you can have both automobiles and safety, you can have the Internet and privacy — and I think that day is arriving."

david.sarno@latimes.com

Copyright © 2012, Los Angeles Times

WORD COUNT CERTIFICATION

1. I am an attorney duly licensed to practice law before all courts of the State of California. I am employed by Schreiber & Schreiber, Inc., and am one of the attorneys representing Plaintiff and Real Party in Interest David Krescent in the above-captioned matter. I make this certification pursuant to California Rules of Court, Rule 8.520 (c)(1) which requires all answer briefs on the merits to be less than 14,000 words in length.

2. On May 29, 2012, I had my computer perform a word count, which indicated that the Plaintiff and Real Party in Interest's Answer Brief on the Merits is 13,094 words in length.

Dated: May 29, 2012

A handwritten signature in black ink, appearing to read "Eric A. Schreiber", with a long horizontal line extending to the right.

Eric A. Schreiber, attorney for Plaintiff
and Real Party in Interest, David Krescent

Attorneys for Defendant in *Luko v. eHarmony*

Sheldon Eisenberg
Drinker, Biddle & Reath, LLP
1800 Century Park East, Suite 1400
Los Angeles, California 90067


Clerk of the Court
Court of Appeal, Second Appellate District, Division Eight
300 South Spring Street, Second Floor, North Tower
Los Angeles, California 90013

Clerk of the Court
Los Angeles Superior Court
Central Civil West Courthouse, Department 309
Los Angeles, California 90005

X Via U.S. Mail: I am "readily familiar" with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with the U.S. postal service on that same day with postage thereon fully prepaid at Encino, California in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

I declare under penalty of perjury under the laws of the State of California that the above is true and correct

Executed May 30, 2012 at Encino, California.


Raquel Matsubayashi

PROOF OF SERVICE BY MAIL

STATE OF CALIFORNIA)
COUNTY OF LOS ANGELES)

I am employed in the County of Los Angeles, State of California. I am over the age of 18 years and not a party to this action; my business address is 16501 Ventura Boulevard, Suite 401, Encino, California 91436.

On May 30, 2012, I served the foregoing document described as ANSWER BRIEF ON THE MERITS on the interested parties in this action by placing a true copy thereof enclosed in a sealed envelope in the United States mail at Encino, California, addressed as follows:

Attorneys for Defendant/Petitioner in *Krescent v. Apple*

Daniel M. Kolkey
Austin V. Schwing
Gibson Dunn & Crutcher LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105

David M. Walsh
Adam M. Sevell
Paul Hastings LLP
515 South Flower Street, 25th Floor
Los Angeles, California 90071

Attorneys for Defendant in *Luko v. Ticketmaster*:

William A. Delgado
Michael C. Lieb
Willenken Wilson Loh & Delgado, LLP
707 Wilshire Boulevard, Suite 3850
Los Angeles, California 90071