



### California Supreme Court: Online Retailers May Require Personal Info for Electronic Downloads

Online retailers do not violate California's credit card privacy law by requiring consumers to provide personal information, including their addresses and phone numbers, as a condition of accepting credit card payments for electronic downloads, the California Supreme Court ruled Feb. 4, 2013. A split court issued the ruling in [Krescent v. Apple Inc.](#), a putative class action against Apple by a consumer who purchased downloads from Apple's iTunes Store. The court held that California's Song-Beverly Credit Card Act does not apply to online credit card purchases that are delivered electronically. The ruling stands in contrast to the court's 2011 ruling in [Pineda v. Williams-Sonoma Stores, Inc.](#), in which the same court concluded that ZIP codes constitute personal identification information within the meaning of the statute and that the Act prohibits retailers from requesting or recording this information as a condition of credit card sales for physical goods during face-to-face transactions at "a traditional brick-and-mortar business."

Plaintiff David Krescent sued Apple, individually and on behalf of a putative class of similarly situated individuals, for alleged violations of the Act, alleging that he purchased media downloads from Apple on various occasions and that, as a condition of completing the credit card transactions and receiving those downloads, Apple required him to provide his telephone number and address. Krescent also alleged that Apple records customers' personal information, but that the company is not contractually or legally obligated to collect customers' telephone numbers or addresses in order to complete credit card transactions and does not require this information for any special purpose incidental but related to credit card transactions, such as shipping or delivery. The complaint also alleged that even if credit card processing companies did require a valid billing address or credit card identification number to complete a transaction, under

no circumstance would they require plaintiff's telephone number to complete his transaction, and therefore Apple did not need plaintiff's phone number to complete a media download transaction.

Apple sought to have the case dismissed, arguing that the Act did not apply to online transactions and for the court to hold otherwise would undermine fraud detection and prevention efforts. The lower court declined to adopt Apple's argument. Acknowledging that Apple's argument with respect to preventing credit card fraud had appeal, the trial court noted that the Act is silent on exempting online credit card transactions and the court was therefore not prepared, at this preliminary stage, to read the Act as completely exempting online credit transactions from its reach. While the lower court suggested that resolution of the issue by an appellate court might materially assist the resolution of the litigation, the Court of Appeal, the intermediate appellate court, denied Apple's petition for review. The California Supreme Court then granted the company's petition for review.

After reviewing the statute, the California Supreme Court concluded that the language did not conclusively resolve the issue, noting that the legislature enacted the Act in 1990 and did not contemplate online or Internet transactions at that time, and that an examination of the entire statutory scheme was necessary to determine whether it is "applicable to a transaction made possible by technology that the legislature did not envision." According to the court, the purpose of the Act clearly is to protect consumer privacy – to prevent retailers from collecting information not otherwise necessary for credit card transactions, because of existing fraud

*This publication may constitute "Attorney Advertising" under the New York Rules of Professional Conduct and under the law of other jurisdictions.*

protection procedures, leading consumers to believe that this personal information was required to complete the transactions and then be used for unsolicited marketing purposes later. In the case of online purchases, however, those identification and fraud protection mechanisms are not available to the retailer. “Unlike a brick-and-mortar retailer, an online retailer cannot visually inspect the credit card, the signature on the back of the card, or the customer’s photo identification.” As a result, the court could not conclude that if the legislature in 1990 had been able to anticipate online transactions involving electronically downloadable products, it would have intended the Act’s prohibitions to apply to those transactions, despite the unavailability of those safeguards.

Because the statutory scheme and legislative history make clear that the legislature’s concern was that retailers have some mechanism by which to verify that a person using a credit card is authorized to do so, and because no mechanism would exist in the context of online purchases of electronically downloadable products if the Act applied to those transactions, the court concluded that the legislature could not have intended the Act to apply to these transactions.

Addressing the three dissenting justices, who argued that the ruling represents “a major win for these sellers but a major loss for consumers, who in their online activities already face an ever-increasing encroachment upon their privacy,” the four justices in the majority countered that “[t]hese ominous assertions, though eye-catching, do not withstand scrutiny.” Specifically citing the California Online Privacy Protection Act and the federal Telephone Consumer Protection Act and related regulations, the court reasoned that existing state and federal privacy laws limited the collection and use of personally identifiable information for unwanted commercial solicitation.

In sum, the California Supreme Court concluded: “Having thoroughly examined [the Act’s] text, purpose, and history, we are unable to find the clarity of legislative intent or consistency with the statutory scheme necessary to conclude that the legislature in 1990 intended to bring the enormous yet unforeseen advent of online commerce involving electronically downloadable products – and the novel challenges for privacy protection and fraud prevention that such commerce presents – within the coverage of the Credit Card Act.” According to the court, the legislature intended to safeguard consumer privacy while also protecting retailers and consumers against fraud, and “this accommodation of interests” would not be achieved if the court read the Act to apply to online transactions involving electronically downloadable products. “Because we cannot make a square peg fit a round hole, we must conclude that online transactions involving electronically downloadable products fall outside the coverage of the statute.”

For more information about the content of this alert, please contact [Michael Mallow](#) or [Michael Thurman](#).

This alert is a publication of Loeb & Loeb and is intended to provide information on recent legal developments. This alert does not create or continue an attorney client relationship nor should it be construed as legal advice or an opinion on specific situations.

Circular 230 Disclosure: To ensure compliance with Treasury Department rules governing tax practice, we inform you that any advice contained herein (including any attachments) (1) was not written and is not intended to be used, and cannot be used, for the purpose of avoiding any federal tax penalty that may be imposed on the taxpayer; and (2) may not be used in connection with promoting, marketing or recommending to another person any transaction or matter addressed herein.

© 2013 Loeb & Loeb LLP. All rights reserved.

For more information about Loeb & Loeb's Consumer Protection Department, please contact:

ARTHUR W. ADELBERG	AADELBERG@LOEB.COM	202.618.5020
ROBERT M. ANDALMAN	RANDALMAN@LOEB.COM	312.464.3168
MARK D. CAMPBELL	MCAMPBELL@LOEB.COM	310.282.2273
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
DARLENE M. CHO	DCHO@LOEB.COM	310.282.2168
AURELE A. DANOFF	ADANOFF@LOEB.COM	310.282.2398
THERESA L. DAVIS	TDAVIS@LOEB.COM	312.464.3188
PATRICK N. DOWNES	PDOWNES@LOEB.COM	310.282.2352
ERIC GUERRERO	EGUERRERO@LOEB.COM	310.282.2214
EMILY R. HAUS	EHAUS@LOEB.COM	312.464.3126
JESSICA M. HIGASHIYAMA	JHIGASHIYAMA@LOEB.COM	310.282.2072
DEREK K. ISHIKAWA	DISHIKAWA@LOEB.COM	310.282.2364
MICHAEL W. JAHNKE	MJAHNKE@LOEB.COM	212.407.4285
JENNIFER A. JASON	JJASON@LOEB.COM	310.282.2195
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
BENJAMIN KING	BKING@LOEB.COM	310.282.2279

LIVIA KISER	LKISER@LOEB.COM	312.464.3170
RICHARD M. LORENZO	RLORENZO@LOEB.COM	212.407.4288
MICHAEL MALLOW	MMALLOW@LOEB.COM	310.282.2287
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
FIONA P. MCKEOWN	FMCKEOWN@LOEB.COM	310.282.2064
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
JAY K. MUSOFF	JMUSOFF@LOEB.COM	212.407.4212
JERRY S. PHILLIPS	JPHILLIPS@LOEB.COM	310.282.2177
RACHEL RAPPAPORT	RRAPPAPORT@LOEB.COM	310.282.2367
CHRISTINE M. REILLY	CREILLY@LOEB.COM	310.282.2361
AMANDA J. SHERMAN	ASHERMAN@LOEB.COM	310.282.2261
MICHAEL B. SHORTNACY	MSHORTNACY@LOEB.COM	310.282.2315
MEREDITH J. SILLER	MSILLER@LOEB.COM	310.282.2294
DENISE A. SMITH-MARS	DMARS@LOEB.COM	310.282.2028
WALTER STEIMEL, JR.	WSTEIMEL@LOEB.COM	202.618.5015
MICHAEL A. THURMAN	MTHURMAN@LOEB.COM	310.282.2122
LAURAA. WYTSMA	LWYTSMA@LOEB.COM	310.282.2251
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960