CLIENT ALERTS & INSIGHTS

Oldies but Not Goodies-Plaintiffs Put New Digital Spin on Song-Beverly

AUGUST 16, 2024

Over the past few months, a wave of new lawsuits has been filed in California state court against online retailers alleging violations of California's Song-Beverly Credit Card Act, Cal. Civ. Code § 1747.08 ("Song-Beverly"). The latest in a long line of "old law, new technology" privacy theories, these lawsuits claim that retailers violated Song-Beverly by requiring customers to provide their personal identification information, including their first and last name, home address, email address, ZIP code, and IP address in connection with every credit card transaction.

There is plenty of indication that Song-Beverly does not apply to online transactions. However, retailers cannot afford to ignore this growing wave of suits, which, if accepted, stands to outlaw modern-day e-commerce by preventing online retailers from collecting information necessary to process online purchases.

History of Song-Beverly

The Song-Beverly Credit Card Act prohibits retailers from requesting or requiring personal identification information as a condition for accepting a credit card as payment for goods or services and recording that information on a receipt. Enacted in 1971, long before the privatization of the Internet and the rise in e-commerce, the law does not make any reference to online credit card transactions.

Instead, Song-Beverly has historically been used in the context of in-store transactions. Most notably, in 2011, hundreds of lawsuits targeted the industry following the California Supreme Court's seminal decision in *Pineda v. Williams-Sonoma Stores Inc.*, which held that Song-Beverly prohibits retailers' collection of ZIP codes during credit card transactions.[1] The *Pineda* court's reasoning was based in part on retailers' technological ability to use customers' ZIP codes with their names to access their full address, which the retailer could then sell to other businesses.[2]

However, Song-Beverly cases largely subsided in 2015, after the California Court of Appeal held in *Harrold v. Levi Strauss* held that Song-Beverly does not apply where a reasonable consumer would understand that her information is not required to complete the transaction.[3]

The California Supreme Court's *Apple v. Superior Court* Decision

The California Supreme Court has not decided whether Song-Beverly can ever apply to online transactions. It has, however, gotten quite close.

In *Apple Inc. v. Superior Court*, the Court, considering digital purchases made in Apple's App Store, held that Song-Beverly did not apply to the purchase of *digital* media made online.[4] The Court found that "[b]ecause the statutory scheme provides no means for online retailers selling electronically

downloadable products to protect against credit card fraud, . . . the Legislature could not have intended section 1747.08 to apply to this type of transaction."[5] The Supreme Court granted Apple's petition for review and ordered the trial court to show cause why the relief sought in the petition for writ of mandate following the denial of Apple's demurrer should not be granted.[6]

A large part of the Court's analysis was focused on the fact that online transactions carry fraud risks not present in store. While the Legislature's intent in enacting Song-Beverly was to protect consumer privacy, "the Legislature did not intend to achieve privacy protection without regard to exposing consumers and retailers to undue risk of fraud."[7] The legislators who wrote Song-Beverly had concluded that brick-and-mortar retailers did not need to collect and record a customer's personal identification information due to existing procedures for verifying a customer's identity and preventing fraud, such as comparing the signature on the receipt with the signature on the back of the card, or contacting the credit card issuer to obtain approval for expensive sales.[8] These fraud prevention mechanisms do not apply online.

Moreover, Song-Beverly contains two fraud-prevention mechanisms, each of which is inapplicable in the online context: (1) allowing businesses to require cardholders to provide identification so long as none of the information contained thereon is recorded, and (2) allowing businesses to record a cardholder's driver's license or state identification number if she pays for the transaction with a credit card number but does not make the credit card available.[9]

Later Appellate Decisions

Since *Apple*, numerous courts have rejected plaintiffs' attempts to apply Song-Beverly to other forms of online transactions.

In *Ambers v. Beverages & More, Inc.* ("*BevMo*"), the California Court of Appeal extended the Apple Court's reasoning to hold that Song-Beverly did not apply to the plaintiff's online purchase of merchandise that the plaintiff subsequently retrieved at a BevMo retail store.[10] Although BevMo customers were required to present proof of identity and the credit card used to complete the online purchase as a condition to receiving the purchased merchandise at a BevMo retail store, the court found that "[t]he availability of such an ex post facto remedy is not the same as the antifraud protection provided by section 1747.08 subdivision (d) to a brick-and-mortar retail sale.[11] The court reasoned that "[l]ike the online retailer in *Apple*, BevMo had no means, without obtaining plaintiff's PII, of verifying that plaintiff was an authorized used of the credit card number entered on BevMo's Web site before the purchase transaction was completed."[12]

The Ninth Circuit, in *Ambers v. Buy.com*, relied on the *Apple* and *BevMo* decisions, and the lack of any contrary California authority, to conclude that Song-Beverly did not apply to online transactions where a retailer ships the merchandise to the customer.[13] When comparing the case to *Ambers v. BevMo*, the Court held that "the case for obtaining a telephone number to verify the transaction here is even stronger because Buy.com shipped the DVDs to Ambers rather than allowing him to retrieve them at a retail store."[14] It reasoned that while "[i]t was at least theoretically possible that in-person verification of Ambers' identity was available to the merchant in *BevMo* because he came to pick up the alcohol," "Ambers never showed his face to the retailer and therefore never presented any opportunity for it to verify the transaction in person."[15]

Additional Reasons Song-Beverly Shouldn't Apply Online

If plaintiffs in these new cases are able to overcome the hurdle presented by *Apple* and its progeny, they will still need to establish that the information being collected are "personal identification information" under Song-Beverly. While some of the information at issue (phone number, mailing address) are identified as PII in the statute, others (IP address) are a much less clear. (Courts are split on this question, with some courts finding that IP addresses identify computers rather than consumers[16] and other courts finding that IP addresses are similar to zip codes, which can identify consumers and thus may violate the Act.[17])

Plaintiffs will also need to establish that the information does not fall within an exception to Song-Beverly, for personal information requests that are "incidental but related to the individual credit card transaction, including, but not limited to, information relating to shipping, delivery, servicing, or installation of the purchased merchandise, or for special orders."[18] This may be a challenge for plaintiffs, as there are several common-sense reasons why an online retailer would request a customer's information. For example, retailers use customer information to send an electronic receipt and shipping confirmation, verify the identity of the cardholder, ship the ordered product, and communicate with the customer regarding the sale and delivery. Similarly, while an IP address may not be needed for the transaction itself, an online retailer cannot operate a website without obtaining a consumer's IP address.

In response, plaintiffs counter that some of this information is not actually necessary to complete a purchase, or, alternatively, that retailers are using the information both for order-fulfillment purposes *and unrelated marketing purposes*, which they claim fall outside the exception. This raises interesting but yet-to-be-decided questions about whether, e.g., a retailer violates Song-Beverly where customers are required to agree to a privacy policy laying out the retailer's practices.

Conclusion

If the plaintiffs prevail in these new cases, the impact on retailers could be substantial. Nearly all retailers require contact information for credit card transactions to send a receipt and manage orders, shipping, and delivery. And every website *needs* to collect IP addresses in order to function. Determining proper protective measures can be difficult in this context, where (a) the courts have not issued any decisions in these new cases, and (b) Plaintiffs' theories, if accepted, could seismically shift e-commerce in such a way that small interim measures may seem pointless. However, we highly recommend consulting counsel experienced in this space to help balance business realities against potential (though also maybe unlikely) legal risk in this changing landscape.

For more information, please contact a member of Benesch's **Litigation Practice Group** or **Retail & E-Commerce** industry team.

[1] *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 536 (2011).

[2] *Id.*

[3] *Harrold v. Levi Strauss & Co.*, 236 Cal. App. 4th 1259, 1268 (2015).

[4] *Apple Inc. v. Superior Ct.,* 56 Cal. 4th 128, 150 (2013).

[5] *Id.* at 143.

[6] *Id.* at 150.

[7] *Id.* at 139.

[8] Sen. Com. on Judiciary Analysis of Assem. Bill No. 2920 (1989-1990 Reg. Sess. as amended June 27, 1990, p. 3.

[9] Cal. Civ. Code § 1747.08(d).

[10] *Ambers v. Beverages & More, Inc.*, 236 Cal. App. 4th 508, 516 (2015).

[11] *Id.*

[12] *Id.* at 515.

[13]*Ambers v. Buy.com*, 617 F. App'x 728, 730 (9th Cir. 2015).

[14] *Id.*

[15] *Id.*

[16] *See e.g.*, *Johnson v. Microsoft Corp.*, No. C06-0900RAJ, 2009 WL 1794400, at *4 (W.D. Wash. June 23, 2009) (finding, in the context of interpreting the Windows XP End User License Agreement, that the IP addresses did not constitute personal information because the IP addresses identified computers. "In order for 'personally identifiable information' to be personally identifiable, it must identify a person."); *see also In re Nickelodeon Consumer Priv. Litig.,* 827 F.3d 262, 289 (3d Cir. 2016) (finding that an IP address did not constitute personally identifiable information in the context of the federal Video Privacy Protection Act, 18 U.S.C. § 2710 because "the linkage of information to identity becomes too uncertain, or too dependent on too much yet-to-be-done, or unforeseeable detective work.") (internal citation and quotation marks omitted).

[17] *See Hernandez v. Restoration Hardware, Inc.*, 4 Cal. 5th 260, 264 (2018).

[18]Cal. Civ. Code § 1747.08(c)(3)-(4).