# California Consumer Class Actions: What *CashCall* Means for Businesses in Privacy Cases

January 2015

This article is from Skadden's *2015 Insights* and is available at skadden.com/insights.


Contributing Partner

**Lisa Gilford**
Los Angeles





Four Times Square
New York, NY 10036
212.735.3000

**skadden.com**


The California Invasion of Privacy Act (CIPA) imposes criminal penalties on anyone who intentionally "eavesdrops upon or records [a] confidential communication" in California without the consent of all parties to the communication. CIPA also contains a private right of action, which has led to several recent class actions against companies with call monitoring procedures designed solely to improve customer service. Even businesses using the ubiquitous disclosure "This call may be monitored for quality purposes" have become embroiled in costly litigation in California when the disclosure was not given for outgoing or returned calls with a customer. But a recent California court of appeals ruling sets the bar higher for class certification in these cases, bringing good news for defendants facing CIPA claims.

## The CashCall Case

In 2011, a California court of appeals in *Kight v. CashCall, Inc. (CashCall II)*, 200 Cal. App. 4th 1377 (2011), held that CIPA prohibits a company from monitoring or recording its customer service calls unless consent is obtained from each person on the call. The company's recorded call monitoring disclosure stated, "This call may be monitored or recorded for quality control purposes," but the court found that such a disclosure would not necessarily inform a caller that "this call *and all future calls*" between the company and a caller would be monitored or recorded. At the trial court, *CashCall* had secured summary judgment based on its argument that two employees — the individual speaking to the customer and a supervisor listening to the conversation for quality assurance — count as a single party under the statute, but the court of appeals held that even when an unannounced listener is employed by the same company, liability would apply so long as the communication was "confidential." In remanding the case, the court also specified that plaintiffs would have to show that they had an "objectively reasonable expectation" that their conversations would not be secretly monitored, which was a question of fact dependent on numerous specific factors.

Following that decision, *CashCall* won a trial court ruling decertifying the putative class, which the same California court of appeals affirmed. In *Kight v. CashCall, Inc. (CashCall III)*, 231 Cal. App. 4th 112 (2014), the court ruled that although CIPA's "confidential communication" requirement was an objective test, the test required an evaluation of the totality of the circumstances regarding the reasonableness of an individual plaintiff's belief. In clarifying that the existing law applied to the facts of each case, the court concluded that class treatment was inappropriate when every putative class member would be required to litigate numerous and substantial questions about his or her individual right to recover on an alleged failure to disclose call monitoring.

## What Companies Should Consider in 2015

While *CashCall III* may help constrain costly class actions against companies for alleged failures to disclose call monitoring, individual plaintiffs may still seek civil penalties and the state may seek to impose a $2,500 fine for each violation. Accordingly, companies should continue to consistently provide callers (whether inbound or outbound) with call monitoring or recording disclosures. If an automated disclosure cannot be provided, companies also should train call center operators to provide the disclosure live.

Additionally, although the *CashCall* cases dealt with call monitoring or recording, the underlying California law speaks to the broader issue of eavesdropping on a "confidential communication." As such, and because customer and consumer outreach increasingly happens online, companies should consider providing — if they are not already — monitoring or recording disclosures during live chats and virtual agent or collaborative browsing sessions.