Advertising Law

May 24, 2012

In This Issue

Manatt Partner Ivan Wasserman Invited to Speak at ABA's Food & Supplements Workshop

On June 12, 2012, the American Bar Association's Section of Litigation will host its second annual Food & Supplements Workshop.

Regulatory issues are becoming increasingly complex for supplement and food producers, and to help these companies mitigate potential risks, Manatt partner Ivan Wasserman will participate in a presentation titled **"So How Did Walnuts Become Drugs? Compliance Issues for Companies that Sell Supplements & Functional Foods."** The session will examine key issues facing the industry and offer tips for these companies to protect themselves from an FDA or FTC action. Other participants on the panel include Jeffrey Bram (General Counsel and Vice President, Science and International Business, Garden of Life), B. Keith Clark (Chief Operating Officer and Chief Legal Officer, Mannatech) and Paul Coates (Director, Office of Dietary Supplements, NIH).

The event will take place in Downers Grove, Illinois. For more information or to register for this event, click here.

back to top

FTC Brings Contempt Motion Against Largest Third-Party Billing Company

The Federal Trade Commission filed a motion in the United States District Court for the Western District of Texas seeking a civil contempt order against Billing Services Group Limited (BSG), a billing aggregator comprised of seven different entities.

The FTC alleges that BSG unlawfully placed over $70 million in fraudulent "cramming" charges on consumers' phone bills in violation of a permanent injunction. It is asking the court to impose over $52.6 million in fines on BSG.

According to the motion, BSG violated a 1999 permanent injunction by

Newsletter Editors

Linda A. Goldstein
Partner
Email
212.790.4544

Jeffrey S. Edelstein
Partner
Email
212.790.4533

Marc Roth
Partner
Email
212.790.4542

Practice Area Links

Practice Overview
Members

Upcoming Events

June 12, 2012
Celesq CLE Advertising Law Webinar
Topic: "Privacy Update: Formulating Privacy Policies and Practices for Compliance with the FTC's Final Report and Guidelines"
Speaker: Jeff Edelstein
For more information

June 12, 2012
ABA Section of Litigation's 2nd Annual Food & Supplements Workshop
Topic: "So How Did Walnuts Become Drugs? Compliance Issues for Companies that Sell Supplements & Functional Foods"
Speaker: Ivan Wasserman
Downers Grove, IL
For more information

June 19, 2012
***The National Law Journal's* 2012 Complex Litigation Breakfast Series**
Topic: "Developments & Considerations in False Advertising Claims"
Speaker: Chris Cole
New York, NY
For more information

June 19-20, 2012
ACI's 3rd Annual Conference on Litigating and Resolving Advertising Disputes
Topic/Speaker: "Buckle Up: We're Headed to Trial," Chris Cole
Topic/Speaker: "Defining Advertising Injury: Protecting Coverage Rights When the Company is Sued for False or Misleading Advertising," Steve Raptis
Topic/Speaker: "Developing a Strategy to Combat the Uptick in Litigation Challenging the Marketing and Labeling of Food Products," Linda Goldstein
New York, NY
For more information

July 24–27, 2012
15th Annual Nutrition Business Journal Summit
Topic: "NBJ State of the Industry"
Speaker: Ivan Wasserman
Dana Point, CA
For more information

Awards

"cramming" unauthorized "enhanced service" charges onto consumers' phone bills over a four-year period, consisting of voicemail, streaming video, identity-theft protection, directory assistance, and job skills training, which consumers neither authorized nor knew about. In its motion, the FTC argues that BSG billed consumers for these fraudulent services "on behalf of a serial phone bill crammer amid a flood of complaints, while utterly failing to investigate either the highly deceptive marketing for these services or whether consumers actually used them."

The FTC further alleges that "in the face of stark evidence of ongoing fraud, BSG continued to bill month after month for these services, even approving billing for new services pitched by the same crammer. In fact, BSG continued to bill and collect for these services after major telephone companies refused to do so." According to the Commission, BSG placed the fraudulent charges on approximately 1.2 million telephone lines and ceased the fraudulent billing practices only after the FBI executed a search warrant on the third-party crammer.

The Commission claims that BSG's conduct violated "core provisions" of the permanent injunction, "which prohibits unauthorized billing, misrepresentations to consumers, and billing for vendors who fail to clearly disclose the terms of their services." The more than $52.6 million the FTC seeks represents the amount BSG fraudulently billed consumers but failed to refund.

The Commission successfully filed three previous actions against BSG in connection with its cramming activities. In addition to the permanent injunction issued in September 1999, the FTC previously obtained two other cramming orders against the company, one of which resulted in a $34.5 million judgment.

To read the FTC's motion for a civil contempt order, click here.

Why it matters: The FTC actively polices the marketplace and will hit previous bad actors for violating permanent injunctions. Billing aggregators are reminded that they cannot pass on fraudulent charges and claim ignorance as a defense. As noted by David Vladeck, Director of the FTC's Bureau of Consumer Protection, "under previous federal court orders, BSG cannot profit from the fraud of others and then deny responsibility for the harm they made possible." The FTC's motion against BSG also serves as a critical reminder that consumer-centric businesses must ensure their billing practices are lawful, and that they take immediate steps if they see any signs of potentially fraudulent charges.

back to top

Stay Denied: Federal Court Gives Green Light to Text-Spam Lawsuit Against Google

A federal court in Oakland, California, denied Google's motion to stay a class action lawsuit filed against it by named plaintiffs Nicole Pimental and Jessica Franklin.

Plaintiffs allege that Google's social apps company, Slide, Inc., violated

the Telephone Consumer Protection Act (TCPA) by using automated dialing devices to send text messages to consumers without their consent.

Google had asked the court to stay the action pending a ruling by the Federal Communications Commission interpreting the TCPA. The court denied that motion.

Google acquired Slide, the creator of the Disco app that allows people to send text messages to as many as 99 people at one time. Plaintiffs allege, in a single cause of action, that Google and Slide sent text messages to consumers' cell phones without their prior express consent in violation of the TCPA. Specifically, plaintiffs allege that Google and Slide "made unsolicited text message calls . . . using equipment that . . . had the capacity to store or produce telephone numbers to be called, using a random or sequential number generator," i.e., an automatic telephone dialing system (ATDS) under federal law. An ATDS is defined as "equipment which has the capacity . . . to store or produce telephone numbers to be called, using a random or sequential number generator [and] to dial such numbers."

Google and Slide denied liability and raised the following affirmative defenses: (1) they obtained the required "prior express consent" because individuals who received text messages knowingly released their telephone numbers to Disco—either directly when signing up for the service and agreeing to the Disco terms of use, or indirectly through the group creators, and (2) the technology used to operate the Disco service did not constitute an "automatic telephone dialing system." They further contend that their technology does not have the "capacity" to store or produce telephone numbers that could be dialed using a random or sequential number generator.

The TCPA regulates telemarketers selling goods and services to prevent any telephone-based abusive or deceptive activity. Under the TCPA, a consumer's "prior express consent" is required before anyone may send the consumer an advertisement via text message to the consumer's telephone.

In March of this year a separate entity, GroupMe, petitioned the FCC for "clarification" regarding its duty to obtain prior express consent from consumers and to determine whether its equipment falls under the statutory definition of an ATDS. Specifically, GroupMe sought clarification of the meaning of "prior express consent," which is not defined by the TCPA. In addition, GroupMe inquired as to whether the term "capacity" as used in the definition of an ATDS meant "a theoretical, potential capacity to auto-dial, albeit only after a significant re-design of the software, or rather the actual, existing capacity of the equipment at the time of use, could, in fact, have employed the functionalities described in the TCPA."

Based on the pending petition, Google moved to stay the suit stating that the FCC had primary jurisdiction over the matters and that its ruling, if any, could shed light on the court's ultimate analysis with respect to plaintiffs' claims. Under the doctrine, primary jurisdiction applies only "if a claim requires resolution of an issue of first impression, or of a particularly complicated issue that Congress has committed to a regulatory agency, and if protection of the integrity of a

regulatory scheme dictates preliminary resort to the agency which administers the scheme." The court found that the doctrine did not apply because the lawsuit did not raise technical or policy considerations solely within the FCC's expertise and the issues were not particularly within the FCC's discretion since Congress did not explicitly delegate those issues solely for FCC consideration.

The court found that a delay was not appropriate: "The court is not convinced that the FCC has agreed to issue a ruling, let alone issue a ruling on an expedited basis." Moreover, even if the FCC were poised to issue a ruling immediately, inconsistent rulings by the FCC and the court are not likely since the parties' deadline for hearing motions for summary judgment is October 30, 2012, and trial is set for February 19, 2013. As the court noted, "the parties need to conduct discovery to obtain the facts and expert opinions necessary, so that once these issues are decided by the FCC or the Court, the Court can apply the undisputed facts to the law on motion for summary judgment, or a jury can find those facts at a trial on the merits. A stay will not permit the parties to obtain the discovery necessary to resolve the factual disputes Defendants raise in their Answer and Affirmative Defenses."

To read the court's order denying Google's stay, click here.

Why it matters: Businesses cannot rely on the doctrine of primary jurisdiction to shield potential class action litigation solely because an inquiry pending before a federal agency touches upon the issues raised in the litigation. The court's decision also makes clear that defenses to fend off class claims should be prepared in the event refuge under the primary jurisdiction doctrine proves fruitless.

back to top

Federal Court Certifies Class Action Against IKEA

A federal court in California is allowing a class action lawsuit to proceed against popular furniture maker IKEA.

In their lawsuit, named plaintiffs Reid Yeoman and Rita Medellin allege that IKEA violated California's Song-Beverly Credit Card Act (the "Act") by unlawfully asking for and storing consumers' ZIP codes during credit card sales transactions.

The Act prohibits retailers from capturing personal identification information as a condition for payment via credit card. Plaintiff Medellin alleges that IKEA's cashier asked for her ZIP code when she made a credit card purchase, and that she gave it to the cashier because she thought it was required to complete the transaction.

The Act protects consumers by prohibiting retailers from capturing personal identification information during a credit card sale if the captured information is not required to complete the transaction. Even simple information like a ZIP code is prohibited because retailers may either use the information to locate the consumers' full addresses to send marketing materials or sell their information to other retailers or marketers. Plaintiffs allege that "IKEA systematically and intentionally violates the Credit Card Act by uniformly requesting that cardholders provide personal identification information, including their ZIP codes,

during credit card transactions, and then recording that information in electronic database systems. There is no legitimate need for IKEA to collect a credit card customer's personal identification information in order to complete the credit card transaction." Plaintiffs claim that IKEA uses the "unlawfully collected" data "for business-related purposes." Plaintiff Medellin filed a motion for class certification on behalf of all IKEA customers who were asked to provide personal identification information during a credit card sale.

IKEA opposed the motion, claiming that the class was overbroad since customers often voluntarily provided their personal information while filling out promotional forms in the store or so that they could participate in IKEA's rewards program, sign up for catalogs, or receive marketing materials via e-mail. IKEA also argued that the Act focuses on a single privacy concern: "To prevent corporations from needlessly storing consumer information for use in direct-mail marketing campaigns or selling the information to other marketers for an identical purpose . . . [and] . . . that allowing persons who have volunteered personal identification information to thereafter assert a claim for a violation of the Act, predicated on that person's privacy interests, is in direct contravention to the purpose of the Act and would be entirely illogical."

The court rejected IKEA's arguments and certified a class, thereby allowing plaintiffs to proceed with their action. In this regard, the court noted, "The Song-Beverly Credit Card Act does not provide an exception allowing a retailer to request or require the cardholder to provide personal identification information as a condition of accepting a credit card payment when the individual has previously or subsequently provided any personal information to the retailer. Such an exception would contravene one of the purposes of the Song-Beverly Credit Card Act which is to prevent store clerks from obtaining customers' personal identification information." Thus the court found no hurdle to class certification simply because the class may include consumers who voluntarily provided their personal information to IKEA.

The court also found that IKEA had "a uniform policy and practice of requesting personal identification information from customers during credit card transactions . . . [and] that common questions of law and fact predominate over other issues . . . on the grounds that IKEA's uniform policy and practice of requesting personal identification information from customers during credit card transactions can be evaluated to determine if the [Act] was violated."

Ultimately, the court concluded that the questions of law or fact common to class members predominate over any questions affecting only individual members. The certified class consists of "all persons from whom IKEA requested and recorded a ZIP Code in conjunction with a credit card transaction in California from February 16, 2010 through the date of trial in" the action. Excluded from the class are any consumers who provided personal information under special circumstances incidental to the sales transaction, such as for shipping and delivery purposes.

To read the court's order certifying the class, click here.

Why it matters: The IKEA decision illustrates that collecting personal

information at the point of sale involving a credit card is very risky business. According to the court decision, asking for such minimal personal information violates the Song-Beverly Credit Card Act and makes it virtually impossible in California for retailers to obtain personal information during credit card sales unless they avoid any impression that personal information was collected as a condition to the credit card sale. Retailers should find other methods that encourage consumers to voluntarily provide their information in situations separate from credit card sales.

back to top

Class Action Lawsuit Filed Against MyCashNow Over Text Spam

Plaintiff Flemming Kristensen filed a class action lawsuit against payday lender MyCashNow (currently Credit Payment Services, Inc.) alleging it sent massive unsolicited text messages to consumers without their consent in violation of the Telephone Consumer Protection Act (TCPA).

Plaintiff filed the lawsuit "on behalf of all persons in the U.S. and its Territories who received one or more unauthorized text message advertisements from Credit Payment Services or MyCashNow."

Plaintiff alleges that MyCashNow markets its payday loan services via unlawful text messages to consumers' cell phones nationwide that "has caused consumers actual harm, not only because consumers were subjected to the aggravation that necessarily accompanies wireless spam, but also because consumers frequently have to pay their cell phone service providers for the receipt of such wireless spam." Plaintiff claims that he received the following text spam advertisement on or around December 6, 2011: "DO YOU NEED UP TO $5000 TODAY? EASY QUICK AND ALL ONLINE AT: WWW.LEND5K.COM 24 MONTH REPAY, ALL CREDIT OK. REPLY STOP 2 END." He, along with thousands of consumers who received similar text spam advertisements, did not consent to receive such messages.

According to the TCPA, companies must have consent in order to send text message advertisements to consumers using an automated telephone dialing system, which is defined as equipment with the capacity to store or produce telephone numbers to be called by using a random or sequential number generator. Plaintiff seeks injunctive relief requiring MyCashNow to stop sending wireless spam, as well as statutory damages (up to $500 per violation), reasonable attorneys' fees and costs.

To read plaintiff's complaint, click here.

Why it matters: The class action lawsuit illustrates some of the dangers of using modern technology when marketing to consumers in today's growing age of cell phones and social media. Before embarking on any advertising campaign that includes advertisements sent to consumers' cell phones, retailers must first obtain the consumer's express prior consent.

back to top

Plaintiffs Permitted to Move Forward in Apple's

Tracking Class Action

Northern California District Judge Lucy Koh rejected Apple's claim that class action plaintiffs failed to sufficiently allege that they suffered any economic injury as a result of Apple's actions.

As a result, the company must now defend against plaintiffs' allegations that it secretly tracks iPhone and iPad users without their permission.

In preparation for the September 16, 2012, trial, the court lifted the stay of discovery and ordered Apple to turn documents over to the plaintiffs by May 17, without any "game play." Vikram Ajjampur of Florida and William Devito of New York filed suit against Apple last year after researchers discovered that iPhones collect and store users' location information in an unencrypted file, even when location services are switched off in the phone's settings. According to the lawsuit, "Apple collects the location information covertly, surreptitiously, and in violation of law," and puts its users at risk of stalking and invasion of privacy by failing to adequately and securely store consumer location information. Furthermore, plaintiffs argue that "the accessibility of the unencrypted information collected by Apple places users at serious risk of privacy invasions, including stalking."

On April 27, 2011, Apple posted a "Q & A on Location Data" on its Web site in which it denied all claims that it was tracking the location of customers' phones through applications. According to Apple, "The iPhone is not logging your location. Rather, it's maintaining a database of Wi-Fi hotspots and cell towers around your current location, some of which may be located more than one hundred miles away from your iPhone, to help your iPhone rapidly and accurately calculate its location when requested." In response to consumer claims that the iPhone sometimes continues to update "its Wi-Fi and cell tower data from Apple's crowd-sourced database" even when location services is turned off, Apple stated that such activity is being caused by a bug. Soon after Apple released software to correct the problem.

In its recent motion to dismiss, Apple tried to end the lawsuit on the grounds that there was not a "single, concrete injury inflicted on any one of the plaintiffs here, much less one that is traceable [to Apple]." In response, plaintiffs argued they suffered economic injury by paying top dollar for an iPad or iPhone, a cost they claim they would not have incurred had they known their location information would be so easily collected and transmitted. In addition, plaintiffs claim they suffered damages when their device's battery power, storage and bandwidth were compromised by the transmission of their personal and location data. The court ultimately rejected Apple's arguments and held that plaintiffs' allegations of economic injury were sufficient. Judge Koh did, however, streamline the lawsuit by dismissing some of the plaintiffs' allegations. Apple has not released a comment on the ruling.

The Apple location-tracking class action lawsuit was brought on behalf of all persons in the United States who purchased, owned or carried around an iPhone with the iOS 4 operating system or a 3G iPad between the release of those products for sale by Apple and the present date. Plaintiffs are seeking an unspecified amount of damages for violating the Computer Fraud and Abuse Act and other privacy laws. In addition, plaintiffs are asking for an injunction requiring Apple to disable

such tracking in its next released operating system for iPhones and 3G iPads.

To read the complaint in *Ajjampur et al. v. Apple, Inc.*, click here.

To read Apple's Q & A on Location Data, click here.

Why it matters: In a very short period of time the Internet, cell phones and smart phone technology have revolutionized the way people do everything from making calls to paying bills to buying movie or concert tickets. As consumers are increasingly reliant on their phones, they tend to use them to store personal and important information. Occasionally, however, such information is tracked or recorded by malware or seemingly innocent software. Android phones, for example, recently came under fire after malware capable of recording phone calls was discovered on several phones.

In an effort to protect cell phone users, federal regulators, consumer advocates and government officials are closely watching companies that are responsible for protecting their customers' privacy. The instant case serves as a reminder that similarly situated companies must use caution when dealing with software and/or applications that track the location of cellular phones and related items. If it is necessary to collect a customer's location information, companies should impose encryption requirements to ensure it is not accessible by other apps/software.

back to top