MEMORANDUM

TO: ESPC

FROM: D. Reed Freeman

Adam Fleisher

DATE: November 3, 2014 FILE: 68223-0000001

RE: ***Guthy-Renker* case holding that email sender identity information does *not* need to be in email header**

Last week a California state court of appeals handed down an important decision relating to the state's anti-spam law, Ca. Bus. and Prof. Code § 17529.5. The case, *Rosolowski et al. v. Guthy-Renker LLC* (October 29, 2014) holds that:

(1) the identity of the sender of an email does *not* need to be ascertainable from the email header if identifying information is readily ascertainable in the body of the email; and

(2) the content of an email subject line—for purposes of determining whether it is misleading—must be examined in conjunction with the contents of the email itself.

The key finding of *Guthy-Renker*, therefore, is that emails are to be examined in their entirety for purposes of compliance with § 17529.5. The bottom line, therefore, is that email senders now have greater certainty about the scope of California's anti-spam law. Nevertheless, as discussed further below, *Guthy-Renker* must be read in conjunction with two previous cases interpreting California's anti-spam law—*Trancos* and *Kleffman*—for its full significance to be understood.

The California Anti-Spam Law Trilogy

We now have three noteworthy cases on what constitutes a violation of California's anti-spam law. Each decision is fact specific—thus analyzing them together is necessary to understand the scope of permitted activity and the risk profile of activity not clearly covered by the cases. The cases primarily focus on § 17529.5(a)(2), which makes it unlawful for an email to contain or be accompanied by falsified, misrepresented, or forged header information. In other words, the question addressed by each of these cases is:

- ***What information must be (or must not be) in an email header and body for it to avoid violating § 17529.5(a)(2)?***

The answer appears to be that while the ***header*** need not identify the actual sender of the email, at the very least the email itself ***must identify the actual sender of the email***.

Previous Cases: *Kleffman* and *Trancos*

In *Kleffman v. Vonage Holdings Corp.*, 49 Cal.4th 334 (Ca. 2010), the California Supreme Court held that the use of multiple domain names to bypass spam filters does not in its own right violate § 17529.5(a)(2). Vonage sent emails from multiple domain names, but each one could be traded to a single physical address (of a marketing agent, not Vonage itself). These domain names actually existed and were technically accurate—the question was whether the domain names were misrepresentations because the emails, collectively, gave the impression they were from different entities when they were in fact from Vonage, via its marketing agent. The court reasoned that since the domain names in the header information actually existed, were technically accurate, and were traceable to the sender of the emails, they were not misleading in violation of § 17529.5(a)(2).

Balsam v. Trancos, 203 Cal. App. 4th 1083 (Cal. Ct. App 2012) builds on *Kleffman* but reaches a different result. In this case, the emails were sent from domains that were privately registered and thus not traceable to the ultimate sender. The key holding of this case appears to be that "header information in a commercial e-mail is falsified or misrepresented for purposes of § 17529.5(a)(2) when it uses a sender domain name that neither identifies the actual sender on its face nor is readily traceable to the sender using a publicly available online database such as WHOIS." *Id.* at 1101. Nevertheless, the court hedged, and made clear that it was expressing no judgment about whether "the presence of other information identifying the sender in the body of the e-mail could affect liability under the statute." *Id.*

As such, *Trancos* left open the possibility that an email that could not be traced to the sender by the domain name or header information could nonetheless *not* be a "falsified" or "misrepresented" header. *Trancos* left the distinction ambiguous at best, especially because the email sender in *Trancos* provided multiple ways to unsubscribe in each email as well as domain names with working emails that made it possible to *contact* the sender (even though the identity of the sender was hidden).

Guthy-Renker

This most recent case appears to affirm the dicta in *Trancos*. Here, like in *Trancos*, the identity of the sender of the emails could not be ascertained through the use of a publicly available database such as WHOIS or from the name in the "from" line. That is, the domain names ("Proactiv Special Offer," "Wen Hair Care," etc.) were *not traceable* to the sender (Guthy-Renker).

However, the court reasoned that the body of the emails was sufficient to enable the recipient to identify Guthy as the sender. The court noted the following key facts: (1) The emails were advertisements for Guthy's various consumer brands; (2) they provided a hyperlink to Guthy's website; (3) they provided an unsubscribe notice; and (4) they provided a physical address in Palm Desert, California. In short, the court concluded that "Irrespective of the

allegedly untraceable domain names herein, ***the identity of the sender was readily ascertainable from the body of the emails.***"

In other words, *Guthy-Renker* suggests that a header line in a commercial email advertisement does not misrepresent the identity of the sender if:

- It does not identify the official name of the entity which sent the email, or
- It does not identify an entity whose domain name is traceable from an online database

If the sender's identity is readily ascertainable from the body of the email.

What Must an Email Have to Comply with § 17529.5(a)(2)?

Based on this trilogy, we know the following with regard to what constitutes a misrepresentation or a falsified header under § 17529.5(a)(2):

- The domain name can be "gibberish" or nonsensical so long as it is accurate and traceable, even if only by using WHOIS (*Kleffman*);
- The domain name can be untraceable *only* if the sender can be readily identified from the body of the email (*Guthy-Renker*)
- The domain name *cannot* be untraceable *even if* the email otherwise provides the ability to *contact* the sender, but fails to provide the *identity* of the sender (*Trancos*).

***Guthy-Renker* also holds that an unqualified offer in a subject line does not violate § 17529.5(a)(3)**

Section 17529.5(a)(3) makes it unlawful for an email to have a subject line "that a person knows would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message." The subject lines at issue included statements offering, for example, a free gift, but did not (in the subject line) qualify that the gift was contingent on a purchase.

The court's analysis with regard to whether the subject line was misleading as to a material fact about the message relied on the same basic analysis as the question of the identity of the sender. That is, the key is that the emails "*in their entirety*" were not misleading because the body of the emails makes clear that the free gifts (for example) were contingent on a purchase. The court reasoned that the subject lines were unlikely to mislead a recipient acting reasonably under the circumstances because the advertisements in the email body "plainly and conspicuously stated the conditional nature of the offer." Furthermore, the court noted, "no email is so simple as to merely offer a 'Free Gift' with nothing further said." In other words, no recipient, acting reasonably under the circumstances, reads an email subject line as the entire contents of the missive.

Three Notes of Caution

First, *Hypertouch, Inc. v. Valueclick, Inc.* 192 Cal.App.4th 805 (2011), treated the subject line of an email separately from the body of the email, thus holding that "If a subject line creates the impression that the content of the e-mail will allow the recipient to obtain a free gift by doing one act (such as opening the e-mail or participating in a single survey), and the content of the e-mail reveals that the 'gift' can only be obtained by undertaking more onerous tasks (such as paying money for the gift or agreeing to partake in other offers), the subject line is misleading about the contents of the e-mail." *Id.* at 192. The *Guthy-Renker* court simply stated that it disagreed, but since *Hypertouch* was also decided by a state appeals court, the case is still, at least in theory, good law.

Second, *Guthy-Renker* did not reach the issue of whether the California anti-spam law is preempted by the federal CAN-SPAM Act. *Trancos*, along with *Hypertouch*, both reasoned that because the California law prohibits material falsity in a commercial email message, CAN-SPAM does not preempt it. Thus it still appears that email senders cannot rely on CAN-SPAM preemption for claims arising under § 17529.5(a).

Third, while under *Guthy-Renker* the California anti-spam law does not make it unlawful to send an email with a subject line making an unqualified promise, the substance of such advertising is still subject to the FTC Act, which bars unfair and deceptive acts and practices, as well as state "little FTC Acts" barring the same. The general principle, which applies to email offers as well as any other offers, is that any limitations or qualifications relating to a claim (e.g., "free gift") must be clearly and conspicuously disclosed to the consumer as close as possible to the claim itself.