



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, 10 PVLR 411, 3/14/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### **‘Payment Card Data Pass’ Rules Gain Some Teeth: An Update on the Legal Landscape**



By **ALYSA Z. HUTNIK, JOSEPH D. WILSON AND  
JEFFREY A. KAUFFMAN**

**O**ur May 31, 2010 article for BNA’s *Privacy & Security Law Report*, entitled “*Scrutiny on Payment Card Data Pass: Raising the Profile of Personal Information Sharing Among Marketers*” (“*Scrutiny ar-*

*Alysa Z. Hutnik is a partner, Joseph D. Wilson is an associate, and Jeffrey A. Kauffman is special counsel in Kelley Drye & Warren’s Washington office. Hutnik and Kauffman focus on FTC, state, and private investigations and litigation involving advertising, privacy, and consumer protection claims. Hutnik is also the chair of the American Bar Association’s Privacy and Information Security Committee (within the Section of Antitrust). Wilson’s practice focuses on business litigation in the federal and state courts.*

tle”),<sup>1</sup> summarized then-recent legislation introduced in Congress regarding an online marketing practice commonly known as “payment card data pass.” As described more fully in the *Scrutiny* article, payment card data pass occurs when a consumer’s credit or debit card information is passed on to a third-party merchant following a sale. Frequently, the third-party merchant uses the billing information to enroll the consumer in various negative option subscription programs, wherein the consumer’s silence, or failure to take action to cancel the agreement, is interpreted by the seller as the consumer’s ongoing acceptance to continue to receive and pay for the goods or services offered by the third party merchant. In many instances, consumers, regulators, and plaintiffs in class action suits have alleged that consumers are unaware that their billing information has

<sup>1</sup> Alysa Z. Hutnik and Joseph D. Wilson, *Scrutiny on Payment Card Data Pass: Raising the Profile of Personal Information Sharing Among Marketers*, 10 *PRIVACY & SECURITY LAW REPORT* 810 (2010) (9 PVLR 810, 5/31/10).

been passed to the third party and that they have been enrolled in a negative option program.

Over the past year, Congress, state and federal regulators, and the private bar, have taken steps to ensure that rigorous consumer protections are in place when data pass offers are made. These protections affect not only the companies who receive the financial information from other companies, but also the merchants who are sharing the information with third parties. This article provides an update on several of the developments that have occurred since the publication of the *Scrutiny* article and discusses practical considerations for businesses engaged in online marketing in light of these recent developments.

## I. New Federal Law Restricts – But Does Not Prohibit – Data Pass

Senate Commerce Committee Chairman, Jay Rockefeller (D-W.Va.), proposed legislation May 19, 2010, entitled “The Restore Online Shoppers Confidence Act,” (ROSCA), S.B. 3386, which, among other things, would impose restrictions on the payment card data pass. Both houses of Congress subsequently approved ROSCA and Dec. 29, 2010, President Obama signed it into law.<sup>2</sup>

### A. ROSCA’s Substantive Restrictions on Payment Card Data Pass

ROSCA restricts certain practices with respect to payment card data pass, both on the front end (“initial merchant”) and on the back end (“post-transaction third-party seller”).<sup>3</sup>

The front-end merchant is prohibited by ROSCA, § 3(a), from “disclos[ing] [a payment card, etc.] account number, or [] disclos[ing] other billing information that is used to charge a customer of the initial merchant, to any post-transaction third-party seller [i.e., the back-end merchant] for use in an Internet-based sale of any goods or services from that post-transaction third-party seller.”

Under ROSCA, § 3(a), it is also unlawful for the back-end merchant “to charge or attempt to charge any consumers [payment card or financial account] for any good or service sold in a transaction effected on the Internet, unless—

- (1) **before** obtaining the consumer’s billing information, the post-transaction third party seller has clearly and conspicuously disclosed to the consumer all material terms of the transaction, including—(A) a description of the goods or services being offered; (B) the fact that the post-transaction third party seller is not affiliated with the initial merchant . . . ; and (C) the cost of such goods or services; and

- (2) the post-transaction third party seller has received **the express informed consent for the charge from the consumer** whose [payment card, etc.] will be charged by—(A) obtaining from the consumer—(i) the full account number of the account to be charged; and (ii) the consumer’s name and address and a means to contact the consumer; and (B) **requiring the consumer to perform an additional affirmative action**, such as clicking on a confirmation button or checking a box that indicates the consumer’s consent to be charged the amount disclosed.<sup>4</sup> (emphasis added)

### B. Government Enforcement of ROSCA

Section 5 of ROSCA provides that violations of the act or any regulation promulgated pursuant to it are deemed to be violations of “a rule under section 18 of the Federal Trade Commission Act regarding unfair or deceptive acts or practices” and that the Federal Trade Commission is to enforce ROSCA “in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the [FTC] Act” were part of ROSCA. Accordingly, those who violate ROSCA could be subject to civil penalties of up to \$16,000 per violation in FTC enforcement actions. In calculating the amount of civil penalties, the FTC typically views the term “per violation” broadly, which may range from each individual transaction or each sales campaign that the FTC alleges violated the act, or even each day the FTC asserts the entity violated the act. Clearly the numbers can quickly add up under any of these scenarios, in light of the starting figure for civil penalties and how they may be calculated.

Because the legislation was recently enacted, there are no public FTC-led ROSCA enforcement actions to date. However, FTC investigations, until and if they resolve in a settlement or litigation, are typically non-public in nature, so companies should not take comfort in the lack of public actions thus far. Moreover, the FTC has been highly active in enforcing against businesses with practices involving the sharing of consumers’ sensitive personal information with third parties, in which the issue of data pass falls squarely.<sup>5</sup>

Under certain conditions, ROSCA also allows a state attorney general to bring an action in federal court on behalf of the citizens of the attorney general’s state in order to enjoin an act that is prohibited by ROSCA or a regulation promulgated under it.<sup>6</sup> While there appear to be no publicly-known state ROSCA enforcement actions yet, some states, including New York and Iowa, have litigated and settled investigations involving data pass issues under their respective consumer protection statutes prior to ROSCA’s enactment.

<sup>2</sup> See Pub. L. No. 111-345, 124 Stat. 3618.

<sup>3</sup> ROSCA, § 3(d), defines the “initial merchant” as “a person that has obtained a consumer’s billing information directly from the consumer through an Internet transaction initiated by the consumer,” and the “post-transaction third party seller” as “a person that — (A) sells, or offers for sale, any good or service on the Internet; (B) solicits the purchase of such goods or services on the Internet through an initial merchant after the consumer has initiated a transaction with the initial merchant; and (C) is not — (i) the initial merchant; (ii) a subsidiary or corporate affiliate of the initial merchant; or (iii) a successor of an entity described in clause (i) or (ii).”

<sup>4</sup> ROSCA § 3(a).

<sup>5</sup> See, e.g., FTC website listing privacy and data security enforcement cases, available at <http://business.ftc.gov/legal-resources/8/35>

<sup>6</sup> See ROSCA § 6.

<sup>7</sup> See, e.g., *Press Release, Cuomo Investigating 22 Popular Online Retailers For Linking Consumers To Discount Clubs That Charge Hidden Fees*, NY Att’y Gen. Office (Jan. 27, 2010), available at [http://www.ag.ny.gov/media\\_center/2010/jan/jan27a\\_10.html](http://www.ag.ny.gov/media_center/2010/jan/jan27a_10.html); *Press Release, Court: Vertrue Violated Iowa Consumer Fraud Laws in “Sales” to 497,000 Iowans*, IA Att’y

## II. The Risk of Civil Liability in Private Actions

ROSCA, like the FTC Act, is silent on whether it provides private citizens a private right of action. Given ROSCA's various terms indicating that violations of it are to be treated in the same manner as violations of the FTC Act, it is likely that ROSCA will be treated akin to the FTC Act when it comes to this issue, with an eventual court holding that there is no private right of action under ROSCA.

A holding that ROSCA does not provide for a private right of action by private citizens, however, may not have any practical effect in curtailing lawsuits by consumers invoking ROSCA. As the *Scrutiny* article alluded to, various state consumer protections acts ("CPAs") provide consumers with private rights of actions for damages, statutory penalties, and other relief. Moreover, various state CPAs make violations of federal statutes, such as the FTC Act, an actionable basis for a private right of action. Thus, ROSCA-styled class action complaints recently have been and are likely to continue to be filed against merchants, pursuant to various state CPAs.

For example, we highlighted two representative cases that were filed prior to ROSCA's enactment in our *Scrutiny* article: *Ferrington v. McAfee Inc.*, 5:10-cv-1455 (N.D. Cal.) [complaint filed 4/6/10, first amended complaint filed 5/13/10], and *Van Tassel v. United Mktg. Group Inc.*, 1:10-cv-2675 (N.D. Ill.). Each case was brought in the name of broad classes of consumers and sought to recover significant monetary damages, statutory penalties, and other monetary relief from the defendant-merchants. The plaintiffs in each case sought to obtain these and other remedies on the theory that the alleged payment card data pass practices were deceptive and violated California and Illinois CPAs.

The facts alleged by the plaintiffs in *Ferrington* and in *Van Tassel* are substantially the same (at least on a general level). The plaintiffs in each case allege that when consumers submit payment card information to make a purchase via the websites operated by a front-end merchant, this merchant then passes that information, unbeknownst to the consumer and without his or her authorization, to the website of a back-end merchant. This latter merchant then enrolls the consumer, who thinks that he or she is still engaged in a transaction with the front-end merchant, in a subscription service, and the back-end merchant bills the consumer's credit or debit card a relatively small fee (\$4.95 in *Ferrington* and between \$10-\$20 in *Van Tassel*) for that subscription on a recurring monthly basis.<sup>8</sup>

Gen. Office (March 23, 2010), available at [http://www.state.ia.us/government/ag/latest\\_news/releases/mar\\_2010/Vertrue.html](http://www.state.ia.us/government/ag/latest_news/releases/mar_2010/Vertrue.html). In March 2011, Iowa obtained judgment for more than \$30 million against Vertrue for violations of Iowa's Buying Club Memberships Law and Consumer Fraud Act. *Press Release, Judge Orders Vertrue to Pay Nearly \$33 Million* (March 8, 2011), available at [http://www.state.ia.us/government/ag/latest\\_news/releases/mar\\_2011/Vertrue.html](http://www.state.ia.us/government/ag/latest_news/releases/mar_2011/Vertrue.html).

<sup>8</sup> Some of the plaintiffs' claims in *Ferrington* are brought under two California CPAs, the Unfair Competition Law, CAL. BUS. & PROF. CODE §§ 17200-17210 (the "UCL") and the Consumer Legal Remedies Act, CAL. CIV. CODE §§ 1750-1784. The plaintiffs in *Van Tassel* assert that the payment card data pass practice at issue there violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. 505.

## A. Recent Developments in *Ferrington*

At the time the *Scrutiny* article was published, the *Ferrington* case was at the pleading stage. Since then, the defendant, McAfee, Inc., who is a front-end merchant under the allegations of the amended complaint, filed a motion to dismiss the amended complaint for failure to state a claim. The plaintiffs opposed that motion. On Oct. 5, 2010, the court issued an opinion granting that motion in part and denying it in part ("Order"). One of the more noteworthy aspects of the Order for online marketers is its holding denying the motion to dismiss insofar as it asserted that the plaintiffs did not have standing to bring claim against McAfee under California's Unfair Competition Law ("UCL").<sup>9</sup>

Defendant McAfee had argued that the plaintiffs lacked standing to bring their UCL claim because the claim sought recovery of fees which the plaintiffs had paid directly to the back-end merchant, Arpu, Inc. for the subscription service and not to McAfee. According to McAfee, the UCL claim, therefore, sought restitution that was not allowed under the UCL, which is limited to restitution of what a plaintiff loses directly to a defendant. In rejecting this argument, the court explained, as threshold matters, that the UCL "creates a cause of action for business practices that are 1) unlawful, 2) unfair, or 3) fraudulent," and that the scope of the UCL's coverage is "sweeping" and that its standard for what constitutes wrongful business conduct is "intentionally broad" but that "its remedies are limited." As to the available remedies, the *Ferrington* court explained that those "are generally limited to injunctive relief and restitution; damages and non-restitutionary disgorgement are not available."

In reaching its holding on the standing issue, the *Ferrington* court relied substantially on *Troyk v. Farmers Group, Inc.*,<sup>10</sup> which the court described as "suggest[ing] more generally that the UCL permits restitution from a defendant whose unfair business practices caused the plaintiff to pay money to a third party, as long as it is reasonable to infer that the defendant indirectly received that money from the third party." The court further opined that "[t]he distinction that California courts have drawn between restitutionary disgorgement and non-restitutionary disgorgement does not turn on whether Plaintiffs paid money directly to the defendant. It turns, rather, on whether the profits sought to be disgorged would merely 'restore the status quo by returning to the plaintiff funds in which she has an ownership interest' or would achieve something broader."<sup>11</sup> Applying this proposition and its reading of *Troyk*, the *Ferrington* court concluded that "[h]ere, Plaintiffs allege that McAfee receives a fee from Arpu for each customer whose billing information is transferred to Arpu via the pop-up ad;" "[t]aking this allegation as true, the Court finds that Plaintiffs may be able to show that the fees paid by Arpu to McAfee come from the monies Plaintiffs paid (and lost) to Arpu because of McAfee's business practices;" and "[t]hus, Plaintiffs have alleged an injury in fact and lost money that may be recoverable under the UCL."

For online marketers, particularly those engaged in business in California, the practical importance of the

<sup>9</sup> CAL. BUS. & PROF. CODE §§ 17200-17210.

<sup>10</sup> 171 Cal. App. 4th 1305, 1338, 90 Cal. Rptr. 3d 589 (2009).

<sup>11</sup> Order at 12 (quoting *In re First Alliance Mortg. Co.*, 471 F.3d 977, 996 (9th Cir. 2006)).

*Ferrington* order is to be cautious—liability may extend under the UCL even if the business does not collect payment from the consumer for the second online transaction involved in a payment card data pass.

Two additional aspects are worth noting in the *Ferrington* order for online marketers:

- **Plaintiffs’ Pleading of Deception Was Sufficient:** The court found that the plaintiffs had alleged sufficient facts with respect to the pop-up ad and the process by which the plaintiffs were allegedly deceived into purchasing the subscription service from the second merchant, such that their claim for a fraudulent practice under the UCL could proceed. The court, however, showed some skepticism of the plaintiffs’ theory, noting that “their case as pleaded is not air-tight” and that there were “visual clues in the pop-up that undermine Plaintiffs’ claims[.]”<sup>12</sup>
- **Software Not Covered by California’s CLRA:** The court dismissed the plaintiffs’ claim under California’s Consumer Legal Remedies Act (the “CLRA”), which “prohibits certain ‘unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer.’” (citing Cal. Civ. Code § 1770(a)). McAfee had argued the plaintiffs had failed to state a cognizable claim under the CLRA because software, or a license for its use of software, cannot be considered a “good” or a “service” under the CLRA. While “find[ing] that this issue presents a very close call, the *Ferrington* court agreed with McAfee by following various authorities providing that software was akin to intangible chattels, which are not covered under the CLRA.”<sup>13</sup>

Because the Order permits some of the plaintiffs’ claims to go forward, the next substantial activity will likely involve plaintiffs’ effort to have their putative class of allegedly wronged consumers certified, and McAfee’s challenge to the certification of that class.

## B. Recent Developments in *Van Tassel*

*Van Tassel* was originally filed in state court, and removed to federal court by the defendants. On May 4, 2010, the court dismissed the case without prejudice to the filing of a timely motion to remand or the filing of a proper amended federal complaint. Subsequent to the publication of the *Scrutiny* article, the plaintiffs in *Van Tassel* took the court up on its invitation and filed an amended complaint Oct. 28, 2010.

On Dec. 13, 2010, defendant UMG, Inc., the back-end merchant providing the subscription service, along with another defendant (collectively “UMG”) filed a motion to dismiss. Their supporting arguments included that the case should be sent to arbitration because the plaintiffs agreed to submit any dispute to arbitration when they enrolled in UMG’s subscription service. Notably, the arbitration provision in dispute contained a term providing that “[a]ny such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of another party.” The plaintiffs’ opposition argues, in part, that UMG has not established that the

plaintiffs agreed to arbitrate the case. The plaintiffs assert that even if they technically enrolled in a UMG subscription service providing for arbitration in the event of a dispute, they did not enroll willingly, and, in any event, the arbitration provision is an unconscionable, unenforceable term because of its term waiving the right to bring a class-wide arbitration. We note the resolution of whether such a waiver may be enforceable under state contract law is pending before the Supreme Court, based on the appeal of the Ninth Circuit’s ruling in *AT&T Mobility v. Concepcion*, 584 F.3d 849 (9th Cir. 2009), cert. granted, 130 S. Ct. 3322 (May 24, 2010).

The two other grounds asserted by UMG for dismissal were actually addressed somewhat in *Ferrington*. First, UMG argues that the complaint should be dismissed because it refunded to the plaintiffs all of the subscription service fees which they had been charged and, therefore, the case is moot. The plaintiffs oppose, arguing that the refund of their fees did not moot the case because that refund does not cover their “entire demand” in the case, which also includes interest on those fees, statutory penalties, and their attorney’s fees. In *Ferrington*, McAfee made the same argument as UMG makes in *Van Tassel*. The court in *Ferrington* rejected that argument, reasoning that it was “satisfied that the interest still owed Plaintiff Schmidt [on the subscription fees] is sufficient to establish standing.”<sup>14</sup>

UMG also argues that, as a matter of law, their website was not deceptive, and they include various screenshots to support this position. In opposition, the *Van Tassel* plaintiffs argue that, at the motion to dismiss stage, it is not proper for the court to consider the screenshots, which UMG asked the court to take judicial notice of, and, if those are not considered, the court must reject UMG’s argument on deception. Again, *Ferrington* speaks to this issue. In *Ferrington*, the court there was asked by McAfee to take judicial notice of screenshots of McAfee and Arpu’s websites. The court noted that “judicial notice of facts not subject to reasonable dispute that are ‘capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned,’” and, following that standard, it declined to accept McAfee’s invitation for almost all of its screenshots because the plaintiffs had demonstrated that those were subject to dispute.<sup>15</sup>

All told, it will be interesting to see how the court in *Van Tassel* rules on the motion to dismiss. That order will provide further guidance to online marketers with respect to risk associated with payment card data pass practices, and arguments that may have some traction in court if facing similar litigation.

## Conclusion

Given the fast changing legal landscape on payment card data pass, we conclude with a few recommendations of practical steps that online marketers can consider to reduce their risk profile:

- **Understand your business.** Regularly audit (i.e., review and evaluate) your company’s business practices to understand if you are engaging in

<sup>12</sup> Order at 14-15.

<sup>13</sup> Order at 25-27.

<sup>14</sup> Order at 5 n.3 (citing *Tavernor v. Illinois Fed’n of Teachers*, 226 F.3d 842, 849 (7th Cir. 2000, stating “a person is fully compensated for the temporary deprivation of money if the repayment is made with a market rate of interest”).

<sup>15</sup> Order at 4-5 (citations omitted).

data pass or negative option marketing. In some instances, the business may not even realize that a particular practice falls within the scope of ROSCA or related laws—or that part of their sales force is engaging in such activity. If you determine that you do engage in these practices, it is critical to review the entirety of the offer and practice in light of current law and enforcement/litigation risk, and make any necessary changes promptly.

- **Be vigilant with your third-party marketers.** Be sure to understand your third-party affiliate marketers—who they are (and with whom they in turn work), as well as their business practices. Simple steps, such as investigating affiliates' online complaints, Better Business Bureau ratings, and regulatory and litigation history can shed light on an affiliate's compliance programs and procedures, and if they are often the target of complaints (which in turn usually begs regulator scrutiny). Also consider including express contract terms in agreements with affiliates to confirm compliance with ROSCA and other state and federal consumer protection laws. Lastly, regularly monitor at least a general sample of third-party affiliate offers to ensure on-going compliance.
- **Ensure consumers understand the offer.** Consumers need to be provided adequate disclosures

regarding the material terms of the offer provided, and they need to be provided the terms in a proximate, clear, and conspicuous manner. In other words, have you provided the disclosure in a manner that would actually be noticed and read by the consumer who is reviewing the marketing offer. ROSCA provides some guidance on how certain terms should be presented to consumers, but it does not cover all aspects of how to explain terms to consumers to ensure effective (and legally compliant) disclosures. Close legal review of offers will help to ensure compliance with federal and state consumer protection laws.

- **Track complaints and react quickly and meaningfully.** If your company markets data pass or negative option offers—and even if you don't—it is critically important to listen and respond to your customers in a meaningful way. Customer complaints are a rich source of information about areas of your business that may need more focus and attention. Ignoring or not rapidly or adequately responding to consumer complaints is one of the quickest ways to attract regulatory scrutiny and consumer lawsuits.

These proactive measures collectively can significantly reduce the company's risk exposure going forward.