BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

The authors discuss new restrictions on certain payment card transactions among online marketers, and the areas of risk going forward for companies that continue to engage in the same or similar personal data sharing practices with third parties for marketing purposes when the practice is not clearly disclosed and agreed to by consumers.

Scrutiny on Payment Card Data Pass: Raising the Profile of Personal Information Sharing Among Marketers

BY ALYSA Z. HUTNIK AND JOSEPH D. WILSON

Until now, this situation was fairly common: a consumer shops online, visiting an online marketing company's website. The consumer decides to purchase, say, virus protection software from that website and provides her credit card information for that transaction. Before the transaction is complete, the website conveys one or more additional offers. Perhaps one of those offers includes a ''free'' trial component. The consumer agrees to the offer, thinking it is from the same company, and the transaction for the virus protection software is completed. The next month, the consumer sees a charge on her credit card statement for the virus protection software, but she also sees charges for subscription services from one or more other companies from whom she does not recall making a purchase.

Here's what happened: The online marketing company partnered with one or more other companies. After the consumer entered her payment card information to make a transaction with the online marketing company, but before that transaction was complete, the online marketing company shared her payment card information with one or more third party companies. The consumer was presented with offers by one or more of

 ISSN 1538-3423

these other third party companies via a pop-up screen or a prompt on the main webpage. Neither prompt asked the consumer to re-enter her payment card information in exchange for agreeing to these additional offers. The consumer agrees to one or more of these offers, thinking the offer is from the original online marketing company and/or that there was no charge associated with such offers. The sale for the original transaction is completed with online marketing company, as well as additional membership purchases to third party companies. The consumer is later surprised with a payment card bill that shows charges to multiple companies, all dating back to that one purchase experience.

This experience reflects what is referred to as ''data pass'' among online marketers, and it is getting considerable scrutiny. On April 27, Visa announced a new rule to expressly restrict online marketers from sharing cardholder information to other companies without the consumer's knowledge or active consent. And on May 19, Senate Commerce Committee Chairman, Jay Rockefeller (D-W.Va.), proposed legislation (S. 3386), entitled '' The Restore Online Shoppers' Confidence Act ,'' which would prohibit companies from enrolling consumers in paid-subscription programs unless the consumers separately provided full payment card numbers to each company presenting an offer and affirmatively agreed to each offer.

This article discusses the new restrictions on payment card data pass, and the areas of risk going forward for companies that continue to engage in the same or similar personal data sharing practices with third parties for marketing purposes when the practice is not clearly disclosed and agreed to by consumers.

I. Payment Card Data Pass—New Express Restrictions

Before April 27, Visa's rules had already prohibited merchants from sharing a cardholder's account number and other Visa transaction information with any entity that is not directly involved in completing the transaction, preventing fraud, or as required by law. That rule, however, did not expressly restrict merchants from partnering with other companies offering products if they are offered sometime during the transaction process. The new rule, announced April 27, now requires merchants to prompt consumers to re-enter their card information to accept a subsequent offer from a third-party merchant. This additional disclosure and affirmative consent is intended to make more clear to consumers that a second purchase is being initiated and obtain their affirmative consent to complete that sale and know with whom the purchase is made.[1] As of the date of this article's publication, the authors are not aware of similar express requirements by other card brands on data pass.

Chairman Rockefeller's bill would affirm the restrictions announced by Visa, and add a few additional ones. The bill, which is cosponsored by Sens. Mark Pryor (D-Ark.), Bill Nelson (D-Fla.), Amy Klobuchar (D-Minn.), Claire McCaskill (D-Mo.) and George LeMieux (R-Fla.), would (1) prohibit companies from using misleading post-transaction advertisements by requiring them to clearly disclose the terms of the offers to consumers, and to obtain consumers' billing information, including full credit or debit card numbers, directly from the consumers; (2) prohibit online marketers and other commercial websites from sharing a consumer's billing information, including credit and debit card numbers, to post-transaction third party sellers, and (3) require companies that use ''negative options'' on the internet to meet certain minimum disclosure and enrollment requirements to ensure that consumers' purchases are made on an informed basis.[2] The bill was referred to the Senate Committee on Commerce, Science, and Transportation where its fate remains to be seen.

II. FTC Scrutiny of Personal Data Sharing

A. FTC Enforcement Examples

While only time will tell whether the new Visa rule and threat of enacted legislation will curb data pass of payment card information among online marketers, what *is* clear is the overall scrutiny that online marketers face with respect to the sharing of sensitive personal information for marketing purposes depending on how its done, and the potential exposure if their business practices trigger a red flag. The Federal Trade Commission (FTC) is the most active regulator to enforce potentially ''deceptive'' or ''unfair'' business practices involving the sharing of personal information under Section 5 of the FTC Act, 15 U.S.C. § 45(a). Deceptive practices are those that involve a material representation, omission, or practice that is likely to mislead a reasonable consumer.[3] ''Unfair'' practices are those that ''cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition'' *Id.* § 45(n).

In the context of businesses sharing personal data for marketing purposes, the FTC has clearly taken a stand when such sharing of personal information is inconsistent with the representations made in the privacy policy present at the time the consumer shared his or her personal information. There are a number of cases where the FTC has outlined this theory, including in cases brought against *Geocities* and *Microsoft*.[4] Notably, as relevant to the data pass scenario, the FTC's enforcement examples also include cases where the FTC has held companies responsible for promises *made by their business partners* about how the personal information will be used.

The key case in point is the FTC's case against an internet company, *CartManager*, that provided shopping

[1] *See* Tyler Metzger, *Visa tackles deceptive online 'data pass' marketing* (Apr. 27, 2010), available at http://www.creditcards.com/credit-card-news/visa-data-pass-deceptive-marketing-1282.php.

[2] For further information on this legislation, see http://www.adlawaccess.com/.

[3] *See* FTC Policy Statement on Deception, *appended to Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984), available at http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[4] *See, e.g.*, Decision and Order, *Geocities*, No. C-3850 (FTC Feb. 5, 1999) (privacy policy stated that the company would only disclose consumer information to third parties if it obtained customer consent; Geocities later sold and rented customer data without consent); Decision and Order, *Microsoft Corp.*, No. C-4069 (FTC Dec. 20, 2002) (company represented that it provided a certain level of security of its Passport system, which the FTC asserted were not supported) [FTC approved consent order proposed Aug. 8, 2002 (1 PVLR 962, 8/12/02)].

  PVLR ISSN 1538-3423

cart software to online merchants. The FTC charged that the company rented personal information about merchants' customers to marketers, knowing that such disclosure conflicted with the merchant's privacy policies (4 PVLR 311, 3/14/05).[5] In that case, when consumers were ready to make a purchase, they entered information on ''shopping cart'' and ''check out'' pages that asked for their name, address, phone number, e-mail address, credit card number, and merchandise. The web pages were designed to look like the other pages on the merchants' sites, and typically displayed the merchants' names and logos, but were actually located on the third party CartManager's web site.[6]

According to the FTC, some of the merchants who used CartManager's shopping cart and check-out software stated in their privacy policies that they did not sell, trade, or lend personal information provided by consumers to third parties. CartManager, however, *did* collect and rent the personal information of consumers who shopped at the merchant websites. Thus, the business partner's (CartManager's) practices regarding use of personal information conflicted with the merchant's practices and privacy policy representations about the use of personal information. The FTC charged that CartManager did not adequately inform consumers or merchants that it would collect and rent this information and that it acted knowing that renting the information was contrary to many merchants' privacy policies. The FTC charged that CartManager's business practices were unfair and violated Section 5 of the FTC Act.

CartManager settled the charges with the FTC, and the settlement (a) bars CartManager from using the personal data already collected and bars future misrepresentations about the collection, use, or disclosure of personally identifiable information, (b) requires the company to ensure that consumers receive a clear and conspicuous notice before their personal information is disclosed to other companies for marketing purposes, and (c) required the company to give up the fees it made renting the consumer information.[7]

The FTC's *CartManager* and other privacy cases underscore that the FTC will continue to scrutinize both potentially deceptive representations or omissions about how online marketers use and disclose personal information collected in a transaction with third parties for marketing purposes, and the extent to which business practices are consistent with such privacy policies (or omissions about how personal information will be used). It is also notable that the FTC's scrutiny and privacy enforcement is not necessarily limited to payment card data, but rather may focus on the sharing of *any* consumer personal information if such sharing is contrary to the privacy representations made to the consumer at the time of the data collection, and/or involves a practice that the FTC views as unfair.

B. Best Practices to Avoid FTC Enforcement

The FTC's privacy case examples provide several clear guidelines:

- First, make sure that your business practices regarding the handling of personal information are consistent with what you promise consumers in your privacy policy.
- Second, if your website will involve transactions with third party companies, confirm that the privacy practices of the business partners (at least with respect to any personal data they collect on your website) are consistent with your business's privacy policy, and that the disclosure flow and identity of each such merchant on the website is clear and understandable to the purchaser.
- Third, if you decide to change your privacy policy in a way that materially affects what you promised to consumers in the prior iteration of your privacy policy, work closely with your legal counsel to take necessary steps before you apply the new privacy policy retroactively to personal data collected under the original privacy policy.
- Fourth, before you share personal information with third parties for their marketing purposes, exercise due diligence and vet the parties to ensure that their handling of personal data does not raise red flags.
  - For example, how does the Better Business Bureau rate the company?
  - Has the company been subject to consumer protection-related lawsuits or publicly-known regulatory investigations, and for what reasons?
  - How does the company address consumer complaints regarding their advertising or business practices?

With respect to this fourth point, if your business's brand is going to be associated with such partners, it's wise to know beforehand these relevant facts – and before a lawsuit or investigation pairs your business with theirs. Keeping a pulse on consumer complaints associated with a business practice and addressing the practice outlined in the consumer complaints before they attract a regulator's attention are also good ways to avoid an FTC investigation.

III. Private Litigants Scrutinize Personal Data Sharing

Understanding the FTC's privacy enforcement is critical both to avoid being the subject of an FTC investigation but also to avoid lawsuits brought by private litigants. While the FTC Act does not allow for private citizens to bring actions to redress violations of the FTC Act, *e.g., Holloway v. Bristol Myers Corp.*, 485 F.2d 986, 1002 (D.C. Cir. 1973), most states have passed various forms of consumer protection acts (CPAs) that, in varying terms, protect consumers from unfair or deceptive trade acts or practices. Many CPAs are modeled after Section 5 of the FTC Act, but, unlike the FTC Act, the CPAs *do* permit private individuals to bring lawsuits to redress unfair or deceptive business practices or acts in violation of the particular CPA, in most instances. And unlike the FTC Act, CPAs also frequently permit plaintiffs to recover compensatory damages from a defendant, as well as other forms of relief, including injunctions, punitive damages, statutory penalties and attorney's fees and other costs incurred by the plaintiff in prosecuting the lawsuit, depending on the particular CPA.

Two recently filed cases, *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 Tassell v. United Marketing Group Inc.*, 1:10-cv-2675 (N.D. Ill.),

[5] *See* Complaint and Decision and Order in, *Vision I Props.*, No. C4135 (FTC Apr. 19, 2005), available at http://www.ftc.gov/opa/2005/03/cartmanager.shtm

[6] *Id.*

[7] *Id.*

provide examples of putative class action cases brought on behalf of broad classes of consumers contending that the defendant-merchants passing of credit card data to other merchants violate a state CPA.

A. Ferrington

In *Ferrington*, two named plaintiffs filed a complaint in federal court in California against computer security giant McAfee, Inc. alleging, among other things, that McAfee violated 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 ''CLRA''). According to the plaintiffs, McAfee's website deceived consumers who purchased McAfee software products from the website into clicking on a ''Try It Now'' pop-up ad during the portion of the transaction in which the purchaser's software is downloaded. According to the complaint, the pop-up allegedly deceives consumers because it appears to the consumer that he or she must click on it to continue the download process. Clicking on the ''Try It Now'' ad, the plaintiffs allege, transports the consumer, unbeknownst to him or her, to the website of a McAfee partner, Arpu, Inc., and consummates a purchase by the consumer of a subscription service from Arpu.

The complaint further alleges that, unbeknownst to the consumer, McAfee passed the consumer's credit card and other billing information that the consumer entered on the McAfee site to Arpu. The Arpu subscription purchased by the consumer in the transaction is a negative option subscription, the charges for which are billed to the consumer's credit card each month. The monthly charge is small ($4.95), and it appears on the consumer's credit card statement in such a way that the vendor name is not readily recognizable to the consumer.

Subject to certification by the court, the class of plaintiffs in *Ferrington* consists of ''[a]ll persons in the United States who purchased products or services from McAfee . . . and were subsequently charged by a third party for unused and unclaimed products and services after McAfee transferred their credit/debit card and other billing information to the third-party.'' Among the relief that the plaintiffs seek in the case is ''an order from the Court requiring [McAfee] to disgorge all ill-gotten gains and provide full restitution of all monies they wrongfully obtained from Plaintiffs and the Class through [this] scheme;'' compensatory, statutory and punitive damages; and their attorney's fees incurred in litigating the case.

B. Van Tassell

The plaintiffs in *Van Tassell* instituted their class action in Illinois state court, alleging, among other things, that the defendants in the case violated an Illinois CPA, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILL. COMP. STAT. 505 (the Illinois CFA). The defendants then removed the case from state court to federal court pursuant to their right to do so provided by the federal Class Action Fairness Act of 2005 (CAFA), Pub.L. 109-2, Feb. 18, 2005, 119 Stat. [Notice of removal to federal court 4/30/10]. The *Van Tassell* complaint alleges that, when consumers submit their credit or debit card information to make a purchase via the websites operated by the merchant group of defendants in the case, those defendants then pass that information, unbeknownst to the consumer and without his or her authorization, to another defendant, United Marketing Group (''UMG''). UMG then enrolls the consumer in a negative option subscription service, and UMG bills the consumer's credit or debit card a relatively small fee (about $10-$20) for that subscription on a recurring monthly basis. UMG shares some of the revenues that it receives from those transactions with the merchant-defendant whose website the consumer first contacted. The plaintiffs have demanded relief similar to that demanded by the plaintiffs in *Ferrington*. The federal court May 4 dismissed the complaint without prejudice so that the plaintiffs may re-file the case in conformance with federal court pleading standards.

Like Section 5(a) of the FTC Act's restriction against ''unfair or deceptive acts or practices in or affecting commerce,'' the Illinois CFA provides in pertinent part ''that unfair or deceptive acts or practices . . . in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.'' Ill. CFA § 505/2. Similarly, California's UCL prohibits entities from engaging in, among other things, any ''unfair or fraudulent business act or practice [.]'' UCL § 17200. Under the UCL, the meaning of ''fraudulent'' is synonymous with ''deceptive'' in that an act or practice is fraudulent under the UCL if it is *likely* to deceive members of the public; no one actually has to have been deceived or damaged by an act or practice for it to be fraudulent under the UCL.[8] A private litigant may obtain injunctive relief and restitution on a UCL claim, but the UCL does not provide for the recovery of damages or attorney's fees on claims by private litigants.[9] In comparison to the scope of the UCL, the CLRA proscribes only certain, enumerated acts and practices.[10] The remedies available under the CLRA, however, are more expansive than those available under the UCL. Private litigants can obtain actual and punitive damages, restitution and injunctions, and the court must award a prevailing plaintiff its court costs and attorney's fees in litigation filed under the CLRA.[11]

C. FTC Interpretations Likely Used as Authority in These and Similar Cases

The standards set by the FTC in its privacy enforcement are likely to bear on these types of private lawsuits because courts often refer to the FTC's interpretation as well as federal court decisions concerning what is considered unfair or deceptive under Section 5(a) of the FTC Act as persuasive authority in construing whether an act or practice violates the Illinois CFA or the UCL.[12] CPAs in several other states afford similar

---

[8] *See, e.g., Committee on Children's Television Corp. v. General Foods Corp.*, 35 Cal.3d 197, 211 (1983).

[9] UCL §§ 17003-04; *Cel-Tech Communications v. Los Angeles Cellular Telephone Co.*, 20 Cal.4th 163, 179 (1992).

[10] CLRA § 1761.

[11] CLRA § 1780.

[12] *See* 815 ILL. COMP. STAT. 505/2. (stating that ''consideration shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5 (a) of the Federal Trade Commission Act'' in construing the Illinois CFDPA. *See also Cel-Tech Communications v. Los Angeles Cellular Telephone Co.*, 20 Cal.4th 163, 185-86 & n.11 (1992) (relying on FTC authority in construing UCL); *People ex rel. Mosk v. National Research Co. of Cal.*, 201 Cal.App.2d 765, 773 (Cal. Dist. Ct. App. 1962) (same). *But see Overstock.com,*

  PVLR ISSN 1538-3423

treatment to federal court decisions and FTC's interpretations of Section 5(a) in construing their CPAs.[13] Conversely, these standards may be important to companies that are defending private lawsuits brought under state CPAs because the company potentially can use such standards as support for establishing that their internet marketing acts and practices do not run afoul of what is considered unfair or deceptive under Section 5(a) of the Act and, by extension, should not be seen as unfair or deceptive under the state CPA in question.

Ferrington presents a ready example of a plaintiff that has relied on an FTC standard in an effort to establish that a defendant's acts or practices were deceptive or unfair under a state CPA. As noted above, the plaintiffs in *Ferrington* contend that McAfee's sharing of credit card information with another online retailer, Arpu, via the interconnection of their websites was deceptive and unfair. In support of that allegation, the Complaint states that the FTC ''has found that the passing of billing information from one vendor to another . . . is at odds with consumer expectations and thus unfair.'' The Complaint refers to the FTC's Telemarketing Sales Rule, 68 Fed. Reg. 4579, 4619 (Jan. 29, 2003), to support that proposition. While it is questionable whether *telemarketing* standards set by the FTC have any relevance or should be afforded any persuasive weight in a case involving internet marketing practices, that is probably not the last we have heard from the *Ferrington* plaintiffs with regard to the FTC standards they will rely upon in an effort prove their claims under the UCL and CLRA. Should *Van Tassell* be re-filed, we similarly expect that the plaintiffs there will invoke in some way analysis under Section 5(a) regarding what is unlawful conduct in this area of internet marketing in an effort to establish that the acts of the defendants violated the Illinois CFDPA.

IV. Considerations If Your Company Faces a Class Action For Sharing Personal Data

If your company finds itself facing a consumer class action brought pursuant to a state CPA and alleging only state law claims, like the *Ferrington* and *Van Tassell* cases, the matters for your company to consider in planning its defense are too numerous to summarize in this article. That said, one critical step to consider early—especially in a consumer protection oriented case—is whether to keep the case in the forum in which the plaintiffs filed the lawsuit. Thus, if the plaintiffs filed the case in state court, your company may wish to consider whether it is more advantageous to litigate the case in federal court, and if so, then to remove the case to federal court if your company can establish that the federal court has jurisdiction over the subject matter of the case. Conversely, if the plaintiffs filed the case in federal court originally, your company may be able to get the case dismissed if it can show that the federal court does not have subject matter jurisdiction, such that the plaintiffs would have to re-file the case in state court if they want to proceed with it.[14]

If your company has a choice between state and federal court in defending a consumer class action, it should assess the potential benefits and drawbacks that litigating in each court may present. In making this assessment, keep in mind the following considerations:

- *the pleading standards applicable in each forum*. The standards as to what a complaint filed in federal court must include for it to state a claim for relief on its face recently became stricter. The federal standard may be stricter than what applies in the state court that could hear your class action. The stricter this standard, the better chance your company has getting the case dismissed at the outset because the complaint fails to state a claim for which relief can be granted.
- *the settlement approval procedures in each forum*. Typically, both federal and state courts must approve settlements of class actions. CAFA requires that federal courts scrutinize certain class action settlements more closely than those courts had to do in the past, notably settlements awarding coupons to the plaintiff class. Generally speaking, state courts are not as strict. Thus, a state court might give your company a greater range of options in crafting a settlement.[15]
- *the discovery rules applicable in each forum*. Discovery can be expensive and, in consumer class actions, the defendant typically produces most of the discovery. Thus, your company will want to evaluate and weigh the limits each forum places on discovery requests and how receptive each forum will be to your company's request to shift to the plaintiffs its costs of responding to their discovery requests.

Conclusion

The legal standards for online merchants in collecting and sharing consumer data with other merchants for marketing purposes are rapidly evolving. Keeping abreast of changes regarding those standards by tracking industry developments, pending legislation, regulatory enforcement, and in cases brought by private litigants, such as the samples of each described in this article, can help identify the practices that are likely to

Inc. v. Gradient Analytics, Inc., 151 Cal. App. 4th 688, 715 (2007).

[13] *See* John E. Villafranco & August T. Horvath (eds.), Consumer Protection Law Developments 377-78 (ABA 2009).

[14] Until the federal Class Action Fairness Act of 2005 (CAFA), Pub. L. 109-2, Feb., 18, 2005, 119 Stat. 14 [28 U.S.C. Sections 1332(d), 1453, and 1711-1715], was enacted, federal courts typically could not hear consumer class actions alleging only state law claims. The prerequisites to federal court diversity jurisdiction typically could not be met before CAFA because the claims of each named plaintiff had to exceed the jurisdictional minimum of $75,000—which typically was not the case since each plaintiff's claim would only be about the value of its own transaction with the defendant—or because one of the named plaintiffs and one of defendants were residents of the same state. CAFA was enacted to allow more of those kinds of class actions into federal court by liberalizing the diversity jurisdiction prerequisites. *See id.* § 2. CAFA permits diversity jurisdiction in class actions if: (a) at least one member of the class and one defendant are citizens of different states, (b) the amount in controversy under the claims of all class members, when aggregated, exceeds $5,000,000 and (c) the number of members in the proposed plaintiff class is 100 or more.

[15] See Donna L. Wilson, John W. McGuinness and Veronica D. Gray, Settling Class Actions: Alternatives to Coupon Settlements After CAFA and Considerations for Corporate Defendants, ANDREWS LITIG. RPTR., Feb. 2009, at 1-5. For other interesting information on CAFA and class action settlements, see postings at http://www.consumerfinancelawblog.com/articles/class-action/.

trigger unwanted scrutiny and proactive steps your business can take to avoid such scrutiny (and potential investigations and lawsuits).

  PVLR ISSN 1538-3423