wiley

NEWSLETTER

Have You Adjusted to ROSCA's New Billing Restrictions for Online Transactions?

September 2011

Late last year, Congress enacted the "Restore Online Shoppers' Confidence Act" (ROSCA) to address certain aggressive online sales tactics that had run up millions of dollars on consumers' cards. Websites today should review their current treatment of credit and debit card data to ensure that they are operating in compliance with the law.

ROSCA's Target Conduct

ROSCA was enacted to battle the practice of "post-transaction data pass." In a typical example of this practice, a website engaged in e-commerce would partner with a third-party company. After a consumer entered payment card data for a purchase, but before the transaction was completed, the website would pass the payment data along to the third-party company. That third-party company would then present the consumer with offers (such as to join a membership club) via a prompt or a pop-up screen. This normally occurred in such a way that the consumer was unaware that he or she was dealing with a third party. The consumer might agree to one or more of these offers, thinking them part of the original transaction. Importantly, the consumer would not be asked to enter payment data a second time because the payment card data had already been passed to the third party. Many consumers were surprised to find a charge for the additional offers on the credit card bill later on. These offers typically took the form of a "negative option" in which the user's account would continue to be charged on a monthly basis unless the user acted to stop it.

A Senate investigation found that hundreds of legitimate websites had shared their customers' billing information through this "data pass" process with other companies. These post-transaction third-party sellers then enrolled online consumers in their membership programs more than 35 million times, charging them over $1.4 billion for benefits and services they were often unaware they had purchased.

What ROSCA Requires

ROSCA took aim at this practice in several ways. First, it forbids any such "post-transaction third-party seller" from charging a consumer's payment card for an e-commerce transaction unless, before obtaining the payment information, it "clearly and conspicuously discloses" all of the material terms, **including that the third party is not affiliated with the website** on which the consumer made the original purchases. Also, the third-

party merchant must receive the consumer's "express informed consent for the charge" by obtaining **from the consumer** the "full account number" and billing contact information.

Second, ROSCA also prohibits the initial website from disclosing payment card data used for the initial transaction to any post-transaction third-party seller for use in a post-transaction Internet-based sale. This does not affect a website's ability to pass payment data to a company that operates the website's own e-commerce pages.

Third, ROSCA prohibits charging a consumer for a transaction effected on the Internet through a negative option feature unless three conditions are met. First, the seller must clearly and conspicuously disclose all material terms of the transaction before obtaining the user's billing data. Second, the seller must obtain the user's "express informed consent" before charging the user's payment account. Third, the seller must provide "simple mechanisms" by which the consumer may stop recurring charges.

Violations of ROSCA are treated as unfair or deceptive acts or practices under the Federal Trade Commission (FTC) Act. The FTC and state Attorneys General have authority to bring actions to enforce ROSCA.

What Should Websites Do?

So what does this mean for an e-commerce site? First, the site should review its arrangements with its business partners to make sure that it is not engaging in any impermissible "data pass" activities. It may want to review with care how any business partners conduct any third-party post-transaction sales.

Second, a website should review its own actual practices regarding the transfer of payment information. Credit card networks also impose some restrictions on transfers of payment information that may apply to a website.

Third, a website should review whether it engages in any practice that might fall within the scope of "negative option billing" under ROSCA. It is particularly important for websites that assess a periodic charge to ensure that they are making the necessary disclosures and have provided a simple mechanism by which users can stop the recurring charges.