From the Puget Sound Business Journal
:http://www.bizjournals.com/seattle/blog/techflash/2011/01/creating-a-safety-net-for-online.html

Jan 14, 2011, 7:06am PST

GUEST POST

A safety net for online shoppers

Rob McKenna

Rob McKenna: Businesses and consumers agree that saying "no" means "no." But does *not* saying "no" – or simply remaining silent – qualify as a "yes?" Some marketers seem to think so. They've increasingly used deceptive tactics to charge consumers for products and services they never intended to buy and to collect consumers' personal information, resulting in increased solicitations.

At the Attorney General's Office, we've fought hard to stop companies from fleecing online shoppers through tactics known as "post-transaction marketing" and "negative-option billing."

We investigated and sued some of the worst offenders, including Washington state-based Intelius. The suit persuaded Intelius to clean up its act. We proposed state legislation to protect consumers, and when our bill died in committee, we took our case to the federal government.

Thankfully, Congress shared our concerns and yours. A federal bill imposing new restrictions on online retailers will help protect consumers from abusive business practices. Known as the Restore Online Shoppers' Confidence Act (S 3386), the bill was signed by the President on Dec. 29. The U.S. Senate Committee on Commerce, Science and Transportation deserves applause for crafting this bill, which is expected to save consumers millions of dollars and finally brings consumer protection laws into the digital age.

Post-transaction marketers such as Affinion, Vertrue and Webloyalty make their money by piggybacking their ads on the Web sites of other retailers. They obtain credit card data from consumers who have purchased other products, such as movie tickets or flowers, then insert themselves in the checkout process in such a way that shoppers are often unaware they have agreed to additional purchases, typically enrollment in a club membership.

Our Consumer Protection High-Tech Unit has brought more than a dozen cases involving spyware, malicious pop-ups and deceptive Internet advertising since 2006 – more than any other state. We've taught other states how they can do the same.

In 2009, when the U.S. Senate Commerce, Science and Transportation Committee released its investigative report accusing Web companies of duping consumers, I submitted

testimony. I pointed out that my office's investigations showed that companies engaging in this form of marketing are aware that their marketing and billing practices are deceiving consumers.

With this law, the federal government will achieve on a macro scale what Washington accomplished with our Intelius case in August 2010. The law will prohibit Internet retailers from passing along your credit card information to third-party sellers. Companies like Affinion, Vertrue and Webloyalty will need to disclose the terms of their offers and obtain billing information directly from consumers.

Under the new federal law, negative-option marketers will also need to beef up their disclosures to consumers. And consumers must give their informed consent before being billed.

Remember the old Columbia Records one-cent for 13 albums deal? Still have that old Doobie Brothers 8-track they automatically sent and billed you for when you forgot to mail it back?

In 1973, the Federal Trade Commission adopted a rule known as the Prenotification Negative Option Rule to address music and book clubs that took a consumer's failure to refuse a shipment to mean that merchandise would be automatically sent and the consumer would be billed.

In the online world, marketing tactics have evolved to include free-to-pay conversions, continuity programs and automatic renewals. Some merchants refer to these plans as "advance consent." They should be called "contrived consent." Although groups like the Electronic Retailing Association have established guidelines aimed at preventing abuses through the use of such promotions, serious problems persist.

These tactics are often interwoven with post-transaction sales and pitches for free trials or gifts. In one case brought by office, 13,000 customers who were lured by online offers for freebies ended up paying $14.95 a month on their phone bills for an Internet-related service.

The company behind these pitches, JSE Direct and its subsidiaries, claimed their program would guard customers from "unscrupulous marketers." Ironically, we charged that JSE sold the personal information of thousands of consumers while billing them for a service that only 5 percent ever used. For the record, just one consumer received a free product.

In another case, we alleged that SubscriberBASE misled consumers into believing that they would receive free high-definition televisions, digital cameras and laptops. To qualify, consumers first had to provide personal information which the defendants then leased to other online marketers, then make pricey purchases. And, of course, most never actually received the freebies.

In the not-so-old days, merchants had to sell you a product. But deceptive marketing starts with the assumption that you've already bought it. That's no convenience for the consumer. It's trickery that breeds distrust and favors unethical players over honest retailers. Washington residents and businesses deserve better.

Rob McKenna is Washington state's Attorney General. Opinions expressed in guest posts are those of their authors, and don't necessarily reflect the views of TechFlash or its staff