Prepared Statement of Benjamin Edelman

presented to the

United States Senate
Committee on Commerce, Science, and Transportation

Benjamin Edelman
Assistant Professor
Harvard Business School

Baker Library 445
1 Soldier's Field Rd
Boston, MA 02163

Chairman Rockefeller, Ranking Member Hutchison, Members of the Committee:

My name is Benjamin Edelman. I am an assistant professor at the Harvard Business School, where my research focuses on the design of electronic marketplaces, including designing online marketplaces to assure safety, reliability, and efficiency. My full biography and publication list are at http://www.benedelman.org/bio and http://www.benedelman.org/publications . Relevant disclosures appear on the final page of my testimony.

Today the committee considers important questions of consumer protection in the context of certain online marketing offers with a special tendency to deceive. I apologize for my absence (the result of prior commitments), but I applaud the committee's efforts. My bottom line:

- Post-transaction marketing offers systematically reach consumers in a time when consumers are particularly vulnerable. Post-transaction offers feature deceptive designs that invite consumers to conclude, mistakenly, that the offers comes from the companies the consumers have chosen to frequent, and that the offers are a required part of the checkout process.

- The automatic transfer of consumers' payment information from a merchant to a post-transaction marketer runs contrary to consumer expectations, and creates a heightened risk that consumers will "accept" financial obligations they did not intend to incur.

- Disclosures fail to cure the deception created by post-transaction offers, their timing and formatting, and their automatic transfer of consumers' payment information.

- Straightforward remedies could protect consumers who have suffered unwanted charges, and could prevent further consumers from incurring similar charges.

Post-Transaction Marketing Generally

It is all too easy for a consumer to stumble into a post-transaction marketing offer. Typically, a user requests a merchant site to browse products and perform a purchase. Having added items to an electronic shopping cart, the user presses a button to check out, then completes a series of forms to provide a shipping address, billing address, payment method, shipping speed, and more. At the conclusion of that process, the user expects to receive a page confirming that the order has been accepted and will be processed. Instead, the user receives a "post-transaction offer" from an unrelated third party. If the user responds to that offer, the user comes to be enrolled in the third party's program. Typically, such programs entail recurring fees of $10 or more per month – charges that continue unless and until the user takes action to insist that the charges cease.

An ordinary web search for the names of top post-transaction marketers reveals thousands of dissatisfied users. Post-transaction marketers have earned unsatisfactory ratings from the Better Business Bureau, and their practices have been subject to consumer class actions. In the following sections, I analyze specific practices that have led to consumers becoming enrolled in post-transaction recurring-billing schemes without meaningful knowledge or consent.

The Timing, Placement, and Format of the Post-Transaction Offers Deceptively Suggest that the Offers are Part of the Checkout Process

Users in an online checkout process have a reasonable expectation, well-grounded in standard practice at most web sites, that checkout will consist of a series of steps, each with a button (usually in the bottom-right corner) required to proceed to the next step. Users rightly expect that a checkout process will end in a page that prominently reports that the transaction was successful. Post-transaction marketing flies in the face of these expectations.

Checkout sequence. Post-transaction marketing challenges norms for checkout sequencing. A post-transaction offer generally appears as a screen that a reasonable consumer might mistake for an intermediary step towards the completion of the requested purchase. The post-transaction offer's color scheme, layout, and overall design are typically consistent with the prior screens in the checkout sequence, and there is usually no large and prominent report that the requested transaction has been completed. Committed to finishing the desired purchase, and burdened by a lengthy checkout process, a user is especially likely to press a button with an affirmative label without reading the details and without learning that the button actually accepts an unrelated offer. Haste is reasonable in this context: The many steps in an online checkout processes leave users unusually vulnerable to unrelated offers that, through their timing, appear to be a necessary part of the checkout sequence.

Size and shape. The unusual shape and size of post-transaction offers further hinder consumers' efforts to recognize the offers as advertisements. From experience around the web, consumers recognize that most online ads conform to certain standard shapes and sizes. But post-transaction offers appear in unusual sizes – making them less readily recognizable as advertisements.

Format and design elements. The format of post-transaction offers compounds deception. On many sites I have examined, post-transaction offers mimic the color scheme, fonts, and other design characteristics of the sites in which they appear. Post-transaction offers even present design elements thematically linked to the surrounding merchant's site. (For example, a post-transaction offer on a florist's web site often shows flowers as part of its pitch.) These design elements further blur the boundary between the requested site and the post-transaction offer.

Buttons versus links. Post-transaction offers often use a button for a positive option (e.g. to accept the offer), while a negative option is a bare hyperlink. From experience around the web, users naturally expect that buttons, not mere hyperlinks, advance from page to page in an online checkout process. By presenting the affirmative choice in a button but the negative option in a hyperlink, post-transaction offers make the affirmative choice that much more appealing – closer to what users expect to need in order to proceed through checkout.

Automatic Transfer of Consumers' Payment Information Removes a Key Warning that Users Are Incurring a Financial Obligation

A distinctive characteristic of post-transaction marketing is the automatic transfer of users' payment information from a merchant web site to the post-transaction marketer. As a result, a

user can end up facing recurring credit card charges from a post-transaction marketing program *without the consumer ever typing a credit card number into any site or form* operated by the post-transaction marketer.

To most users, automatic transfer of payment information is quite unexpected. For one, it violates widespread norms about how online advertising works. Clicking an ad on a newspaper's web site does not give the advertiser the user's credit card number, even if the user is a paying subscriber of the newspaper. But, remarkably, clicking a similar post-transaction offer can indeed transfer a credit card number – eliminating a key warning that would otherwise alert consumers to the impending financial obligation.

Consumers rely on the process of providing a credit card number as a barrier to unexpected charges. Users rightly expect that by clicking from site to site, button to button, they do not incur financial obligations. This expectation is part of what makes the web fun, flexible, and low-risk: Users believe they cannot incur financial obligations except by typing their credit card numbers, and users expect to be able to cancel an unwanted transaction if a site requests a credit card number that a user does not care to provide. Here too, post-transaction marketing defies settled norms. By obtaining a user's credit card number directly from an affiliated merchant, a post-transaction marketer can charge a consumer who has not performed the evaluation that consumer would naturally impose before knowingly entering into a paid relationship.

Credit card network rules confirm the impropriety of automatic transfer of users' payment information. Visa's Rules for Merchants[1] say charges may occur after a "cardholder provides the merchant with the account number, expiration date, billing address, and CVV2" (page 12). Visa's requirement is clear: the "cardholder" must provide the information; Visa does not indicate that any designee (such an independent web site) may provide this information to a partner who will later charge the consumer for separate and unrelated services.

In a summer 2009 change, one post-transaction marketer began to require that a user retype the last four digits of a credit card number before becoming enrolled in that company's service. Although this requirement may reduce some accidental enrollments, it does not address the core deception that yields unrequested signups. In no other context site can typing just four digits begin a recurring billing relationship; consumers rightly and reasonably expect that entering a paid relationship requires typing an *entire* card number. Indeed, Visa's Rules for Merchants require that the consumer provide "the account number" – the *entire* account number, not a small portion thereof. To a typical consumer, a request to reenter a portion of a card number looks more like a verification process than authorization: Thanks to Verified By Visa, nonretention of customers' CVV codes, and other efforts to reauthenticate online purchases, consumers expect these extra requests in their online purchases. But typing four digits does not indicate that a consumer authorizes credit card charges from a company with which the consumer otherwise has no relationship.

[1] http://usa.visa.com/download/merchants/rules_for_visa_merchants.pdf

Disclosures Fail to Cure the Deception of Post-Transaction Marketing Practices

Post-transaction marketers typically argue that their disclosures tell consumers what they're signing up for – suggesting that any consumer who signs up must in fact want the service. I disagree. Although post-transaction marketers typically do mention pricing and selected product details, the substance and format of these disclosures fail to cure the deception created by the substance and context of the offer.

For one, post-transaction disclosures are typically positioned where they are easily overlooked. For example, consumers naturally begin their inspection of a web page at the top-left corner (where key information usually appears), and consumers naturally proceed diagonally towards the bottom-right (which, especially in a checkout page, typically contains the button to proceed to the next step). Following this standard pattern, a disclosure in the bottom-left corner is naturally overlooked. Yet the bottom-left corner is exactly where many post-transaction offers present key details of their service.

Post-transaction offers also often bury mention of key terms – for example, the monthly charge and the fact that charges recur each month – within long paragraphs. In the example disclosure that post-transaction marketer Webloyalty provided to CNET News.com in July 2009,[2] the first mention of Webloyalty's "$12 per month" charge appears six lines into the second paragraph of text – a location easily overlooked by a consumer skimming the text. Furthermore, that mention appears under headings labeled "Thank you…" and "Sign up to claim your rewards!" – headings giving no suggestion that the paragraph actually discloses a charge.

In the context of unprecedented automatic transfer of credit card numbers from one company to another, disclosures must be exceptionally effective to overcome consumers' longstanding expectation that only typing a credit card number can create a financial obligation. I suspect consumers' confusion is so fundamental that no disclosure can cure the problem. The confusion certainly is not cured by ordinary plain-type text presented within extended boilerplate below an irrelevant header.

Credit Card Network Rules Disallow Key Post-Transaction Marketing Practices

Credit card networks rules specifically disallow important post-transaction marketing practices. For one, as detailed above, Visa's Rules for Merchants require that the "cardholder" – not any intermediary or merchant – provides the card number to the company seeking to charge the consumer's card. To the extent that post-transaction marketers obtain customers' card numbers in other ways, e.g. from other merchants that already hold consumers' card numbers, credit card networks should disallow such charges.

Post-transaction marketers also appear to violate credit card network rules about recurring payments. Visa's Rules for Merchants state that "Cardholders should be routinely notified of regular recurring payments … at least 10 days in advance" of each such charge (page 57). Most recurring billing merchants comply with this rule; for example, I receive monthly notifications

[2] http://bto.cnet.com/i/bto/20090723/WEBLOYALTY.jpg

from my mobile phone carrier and my broadband provider. However, I understand that post-transaction marketers do not provide such notifications. Visa's rules are clear, and post-transaction marketers should comply with Visa's requirements.

Low Service Usage Rates Support an Inference of Deception

When consumers pay for a service but systematically fail to use that service, there is ample basis to conclude that consumers did not intend to buy the service and that the service's marketing is deceptive. See *FTC v Cyberspace.com, LLC*, 453 F.3d 1196, 1201 (9th Cir. 2006), drawing an inference that solicitation was deceptive from the fact that less than 1% of consumers ever used an internet service they allegedly accepted by cashing or depositing a solicitation check.

The FTC's reasoning is directly on point in the context of post-transaction marketing. A Webloyalty press release from August 2009 claims "over 2 million memberships."[3] Yet traffic analysis service Alexa.com reports that neither Webloyalty.com nor any of its product sites (Reservationrewards.com, Shopperdiscountsandrewards.com, Travelvaluesplus.com, Walletshield.com, and Completesavings.com) appear within Alexa's top 100,000 sites. The difference is readily explained: Blogs, new stories, litigation allegations, and other sources all report systematic user complaints that they did not know they were enrolled in a Webloyalty program and that they certainly never used any Webloyalty services. As in *Cyberspace.com*, this gap between signups and users confirms that Webloyalty's marketing failed to obtain meaningful consent from the users who purportedly "accepted" Webloyalty's offer.

Ordinary Market Mechanisms Do Not Hold Post-Transaction Marketers Accountable

The structure of post-transaction marketing impedes users' efforts to determine which merchants passed their payment information to a post-transaction marketer – preventing users from complaining to those merchants. As a result, the merchants that provide users' credit card numbers to post-transaction marketers generally escape criticism for supporting these practices.

Meanwhile, users sometimes blame companies that in fact had no role in post-transaction marketing. For example, I have read complaints blaming Amazon, AOL, eBay, and Paypal for subscribing users to Webloyalty, when in fact not one of these companies has ever promoted Webloyalty.

Competition between firms further hinders accountability. When a sector includes some sites that promote post-transaction offers and some sites that refuse to include such offers, the former group enjoys a revenue advantage that the latter lacks. As a result, the former can tout lower prices – knowing that some portion of users will see a post-transaction offer, respond, and incur charges that make up for the lower up-front price. Users appreciate the low posted prices but cannot readily assess the costs of post-transaction marketing. As a result, sites that

[3] "Webloyalty Announces Relationship with Clipper Magazine." August 19, 2009.

participate in post-transaction offers appear to offer lower prices and a better value, when in fact their revenue advantage is, for many users, illusory and in any event, ill-gotten.

Suggested Remedies

I suggest seven specific remedies for deceptive post-transaction marketing practices:

- *End automatic credit card transfer.* Merchants should cease providing, and post-transaction marketers should cease receiving, consumers' credit card numbers. If a consumer is to sign up for a post-transaction offer, the consumer should retype her credit card number – just as is required for all other online purchases. This additional step will help the consumer understand that the post-transaction offer is separate from, and additional to, the transaction the user had initially requested.

- *Improved disclosures*. Under a clear heading ("monthly fee"), separate and apart from other text, a post-transaction disclosure should present the essence of the consumer's obligation. Language should be clear and direct – concise declarative sentences, without unnecessary complication or excess detail. Formatting should be designed to draw attention to these key disclosures, separating this material from marketing copy.

- *Monthly reminders of impending charges*. Consistent with credit card network rules, post-transaction marketers should notify each consumer before each monthly charge.

- *Disclosure of consumer signup sources*. In monthly emails to consumers, in an online account management interface, in call center scripts, and/or in credit card charge details, post-transaction marketers should remind consumers how they signed up.[4] No consumer should be left wondering which web site presented a post-transaction offer.

- *Easy reversal of unauthorized charges*. Pursuant to a class action settlement, Webloyalty currently agrees to refund historic charges if a user completes and mails a four-page affidavit. But Webloyalty was happy to enroll users with just a few clicks, and cancellation of charges should be equally easily – not requiring a lengthy form, signature, certification, and more. Nothing in the settlement prohibits Webloyalty from granting refunds more easily than the settlement requires. Nor should these refunds become unavailable when the settlement claims period comes to a close.

- *Notification and easy refunds for current non-users*. For current subscribers of post-transaction services who have not used such services recently (or at all), there is good reason to doubt the efficacy of prior "consent" for associated charges. Such users should receive individual email and postal notification of the programs in which they have been enrolled, the duration of enrollment, and the charges they have incurred. Withdrawal and refund should be as easy as possible – a single hyperlink or a return

[4] At the suggestion of the Center for Democracy and Technology, similar accountability was added to certain adware popups – telling consumers what software caused them to receive the bundled adware that later showed popups. Such accountability helped put an end to deceptive adware bundles.

postcard. All charges should be refunded to the consumer's original form of payment or by check, without requiring an extended refund procedure or affidavit .

- *Ongoing cross-check of usage rate*. If a paid service has an unusually low usage rate, that is prima facie evidence that users may be enrolling in the service without understanding what they're getting. The FTC, state attorneys general, or this committee could monitor usage rates at large post-transaction marketers to confirm that large numbers of consumers are not tricked into paying for services they are not using.

Last month FBI Director Robert Mueller admitted that he nearly succumbed to a phishing scheme. In response, Mueller's wife banned him from further online banking. That's a troubling outcome – in part for the public's ongoing losses to phishing, but also for the costs and inefficiencies that will result if others follow Mueller's lead and abandon online banking.

Through its current work, this committee can protect the balance of online commerce from the deterioration of trust currently tainting online banking. I seek an Internet that is safe for commerce – safe not just for the savvy shopper and tech expert, but also for regular users, including users who are busy, hurried, distracted, or even naïve. Conversely, the Internet cannot achieve its full potential if convoluted schemes trick consumers into incurring charges for services they did not request and did not fairly accept. Trusted Internet commerce has no place for credit card numbers copied from merchant to merchant, for obfuscated disclosures, or for tricky charges disguised as "savings." Ongoing oversight by this committee can help put an end to these important problems.

Disclosures

I appear on my own behalf, not on behalf of Harvard Business School or anyone else.

I serve as a consultant to a variety of companies on subjects unrelated to those issue here, though often generally on the subjects of online advertising and fair treatment of consumers. My biography, http://www.benedelman.org/bio , details those of my clients for which I have had occasion to make public disclosure.