# I Didn't Want That! An Experiment on Interventions for Deceptive Post-Transaction Marketing

Alan Nochenson
*The Pennsylvania State University, USA*

Jens Grossklags
*Technical University Munich, Germany*

***Abstract*—Post-transaction marketing offers are presented to consumers after they have successfully concluded a primary purchase. While, in principle, they could represent desirable marketing offers to the consumer, in many instances consumers consider them unwanted, and potentially even deceptive and misleading. However, marketers use a variety of tactics to lure consumers into purchasing these types of offers including exploiting consumers' cognitive biases and leveraging relationships with legitimate businesses to subversively use customer information without genuine consent.**

**In this paper, we conduct a large-scale human subjects experiment with different treatment conditions to test whether imposing a requirement on first-party merchants to include active or passive warning messages affects the likelihood that consumers fall for undesirable post-transaction marketing offers. We find that an active intervention mechanism significantly impacts the rate at which consumers fall for post-transaction marketing scams. In contrast, passive interventions fail to significantly improve upon a baseline treatment without warnings.**

## 1. Introduction

Post-transaction marketing offers are presented to customers on e-commerce sites after they have made a primary purchase. First-party merchants will automatically redirect consumers to the marketer's site and frequently share customers' personal information (including payment credentials) to increase the likelihood of purchase of the post-transaction marketing offer. While, in principle, such piggybacking of offers could potentially be of benefit to the consumer, if the goods are related and of desirable quality, these post-transaction marketing offers are typically of little or no value at all for consumers [1]. Therefore, marketers often rely on consumers' misunderstandings of the situation. In particular, offers are crafted in a way so that without careful scrutiny, consumers frequently believe that the primary transaction has not concluded, yet. Further, disclosures on the marketer's site are phrased and presented to limit consumers' awareness of the context change, and to lead customers to bypass such disclosures as quickly as possible [2]. Offers are professionally arranged and designed in such a way as to make an unnoticed purchase the choice with the least friction. In short, these offers are effective because they prey on customers by exploiting basic weaknesses of cognitive psychology.

In the European Union, post-transaction marketing is typically treated as a part of the broader phenomenon of so-called "subscription traps." These fraudulent activities do not necessarily have to follow a primary purchase, but can also be associated with other primary online activities such as information seeking, gaming, quizzes, or surveys. Additionally, as the name implies the consequence of a subscription trap is commonly a continued membership or automatically repeated purchase. In the United States, the technical term most closely matching the concept of subscription traps would be "negative options" marketing.

A government report has shown the prevalence of these practices in the United States [1]. Likewise, European Union consumers have been severely affected by these practices. For example, a representative consumer survey concluded that 5.6 million Germans were victims of online subscription traps in the two year period leading up to 2014 [3].

In response, intervention mechanisms have been put in place in different markets. In the United States, legal and enforcement interventions have concretely focused on the notice and disclosure practices of the post-transaction marketers, and aimed to outlaw behind-the-scenes information transfers of payment credentials [4]. In the European Union, the EU Consumer Rights Directive which addresses almost all online commerce (except, for example, healthcare by regulated professionals) has led to specific laws by European Union member states [5]. A particularly interesting example is the German "button law" which amongst other requirements includes the stipulation for particular wordings on the button concluding an online transaction [6]. The conceptual idea behind these laws is that additional affirmative steps with a clear notice of purchase terms will prevent consumers from falling for online scams including post-transaction marketing fraud. However, in Germany the number of victims of subscription fraud has further increased since the enactment of the button law indicating an overall growth of fraudulent activities, but also the partial ineffectiveness of the law as an intervention approach [3].

In our work, we explore a complementary intervention approach. We are particularly interested whether interventions focused on the first-party merchant (or more broadly

*Corresponding Author: For questions and comments please contact Jens Grossklags at jens.grossklags@in.tum.de.*

speaking, the originator of the redirection), and the flow between the primary transaction and the post-transaction marketing offer can be effective in ameliorating consumers' misunderstandings about the unfolding context switch.

We take an experimental approach. Based on actual cases [2], we developed an online shopping environment that combines a primary purchasing episode with a redirection to a misleading post-transaction marketing offer. In our case, the primary merchant offers digital music files, while the post-transaction offer resells to the consumer the same music for an additional amount of money. As such, the post-transaction offer can be considered to be of no particular value to the consumer. For this scenario, we studied in our previous work how many individuals fell for the post-transaction marketing offer given different ways in which this offer is presented to the consumer [7].

For the current study, we take as the *baseline treatment* the offer presentation from our previous work which resulted in the lowest transaction rate for the post-transaction marketing offer [7]. We now compare this baseline treatment with four interventions that are placed at the redirection point between the primary purchase confirmation and the post-transaction marketing offer. The interventions vary the intrusiveness of notice (i.e., an enforced delay before redirection) and the effort required to bypass the notice (i.e., an affirmative action from the consumer). All interventions aim to highlight to the consumer that they are being redirected to a third party, and that the primary shopping episode is concluded. We study whether these interventions are effective in reducing the number of purchases of the post-transaction offer compared to the baseline treatment.

Our study is based on a controlled experimental design with over 450 individuals who completed the study. Further, our scenario involves monetary incentives. Individuals are endowed with a budget, and they are instructed they can keep any unspent money, which presumably incentivizes them not to be wasteful. We, therefore, follow the literature that investigates privacy, security, and marketing practices under experimental conditions that have actual consequences to individuals (see, for example, [8], [9]).

The paper is structured as follows. Section 2 provides a comprehensive discussion on post-transaction marketing; in particular with a focus on consumer protection in the United States. Section 3 describes the experimental design. Section 4 presents the results of the study, and Section 5 discusses and summarizes the results.

## 2. Background on Post-Transaction Marketing

Potentially misleading and deceptive post-transaction marketing offers have a long history [10]. While the exact strategies of implementing these offers vary in how long they bind customers as well as how they are designed along many facets, all of these offers leverage a just concluded primary transaction between a customer and a merchant. Particularly aggressive variations that facilitate a hidden exchange of payment credentials from the first-party merchant to the post transaction marketer (i.e., a so-called data pass) have attracted the attention of payment processors [11] and the United States government [1].

The topic of misleading and deceptive marketing is also becoming increasingly relevant to social media business practices. For example, advertisements on Facebook are frequently used to redirect users to subscription traps (see, for example [12]). Likewise, seemingly newsworthy or otherwise appealing social media content is used to attract and then redirect individuals to deceptive websites (see, for example [13]). More generally, social media content is attractive from the perspective of a fraudster since it triggers a desire for immediate gratification and puts less of an emphasis on delayed costs which are common with subscription traps (see discussion by [14]).

"The main argument for allowing [these post-transaction offers] ... holds that these policies make commerce more efficient and flexible for the seller and buyer [15]." However, in practice, these offers are lucrative for all parties involved, except for consumers. Primary merchants experience increased revenue due to deals with marketers. Deceptive post-transaction marketers typically face very little cost since the products they sell have very little value and consumers are often unaware of having purchased them. Further, since customers are automatically redirected to their marketing sites upon completion of a primary purchase, marketers do not need to invest in advertising or other traditional marketing channels. In contrast, consumers are left standing with a product or subscription they did not want to purchase, and do not need or use.

The transactions are completed because the offers are carefully crafted to exploit weaknesses in the notice and consent process; they exploit behavioral biases and limits of human cognition. Post-transaction offers mimic consistency of appearance with the primary merchant site, which induces a flow-state [2]. Flow is the state when people "lose themselves" in a task and are more likely to not pay sufficient attention due to the speed at which they are processing the current task [16]. Customers are led to use their instinctive system-I cognitive processes, instead of more deliberate and reasoned system-II thinking [17].

Further, two prominent human decision-making biases that are exploited are optimism bias and conditioned-response bias [2]. Optimism bias suggests that consumers are likely to initially believe that they can recognize and address most problematic scenarios. However, since customers are not constantly on the lookout for scams, marketers are able to exploit existing trust by fashioning the visual appeal of their offers after trustworthy examples (in particular, the primary merchant site). Conditioned response biases describe how people react to what they expect to be presented with, not to what is actually shown. I.e., in our scenario, consumers expect that shopping follows an expected process, and that the purchasing session initiated on a trusted first-parted merchant site can be completed in an efficient and problem-free manner.

The Federal Trade Commission (FTC) has been the prime enforcer in the United States against these types of practices. In a 15-year period, there have been about

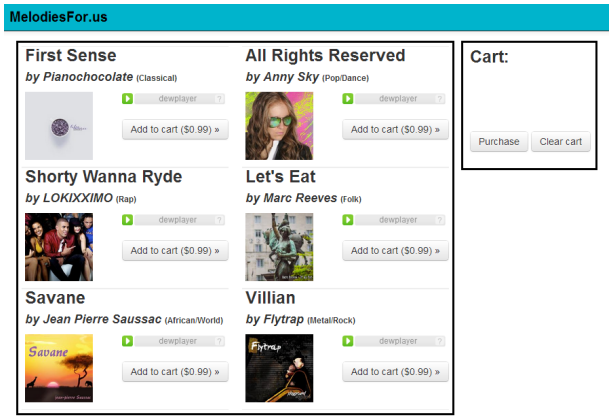


Figure 1. Shopping page.

50 cases brought by the FTC against over 300 entities [18]. Further, since the early 1980's, the FTC has released policy statements on deceptive marketing practices [19]. It has mainly been concerned with material practices that are "likely to mislead the customer ... from the perspective of the reasonable consumer [19]". This concern, specifically with post-transaction marketing tactics on the Internet, has led to comprehensive investigations such as a U.S. Senate report in 2009 [1] documenting that nearly 4 million consumers were faced with reoccurring payments as a result of post-transaction offers and over 35 million consumers fell victim to such offers since 1999. The report showed that over 99% of the purchasers never used the product and were also not satisfied with their purchase.

In order to combat this type of behavior by marketers, the Restore Online Shoppers' Confidence Act (ROSCA) was passed in the United States [4]. ROSCA is a direct response to the U.S. Senate report's finding that deceptive practices online "undermined consumer confidence" [1]. ROSCA prescribes that marketers who use these types of offers clearly disclose the associated terms and require an "additional affirmative action" to complete a sale (therefore somewhat combating the practice of data-pass) [4].

In the European Union, the Consumer Rights Directive has led to specific laws by European Union member states [5]. The conceptual idea behind these laws is that additional affirmative steps with a clear notice of purchase terms will prevent consumers from falling for online scams including post-transaction marketing.

In this study, the baseline treatment captures a scenario which conceptually matches the interventions placed on post-transaction marketers by ROSCA and the EU Consumer Rights Directive. We are then interested to evaluate complementary approaches to further reduce the harm of deceptive post-transaction offers.

# 3. Methods

## 3.1. Experimental Design

**3.1.1. Setup and Consent Practices.** Our experiment was run on the Amazon Mechanical Turk service (see Section 3.3.2). Participants could discover the task by utilizing the service's search results page, where they could preview the task. This preview informed potential participants that they would be participating in a research study on music purchasing behavior. Further, the instructions included that they would be put in a simulated purchasing environment, and would be paid based on their actions in the environment. Once participants agreed to participate in the task through the Mechanical Turk interface, they were presented with a link to enter the study.

After entering the experiment, participants were immediately shown a consent form. This consent form detailed the way they were to be paid, and the contact information for the researchers running the experiment. The consent form also informed them that they were able to leave the task at any time if they felt uncomfortable or did not wish to continue for any reason (however, they would not be paid for a partial effort). The consent form did not detail the exact structure of the experiment. Revealing the post-transaction offer in advance would have compromised the study, i.e., it would have significantly biased the conversion rate and effectiveness of interventions. From an ecological validity point, we are less interested in studying post-transaction offers that consumers are already aware of, e.g., because they have been warned by friends, or previously have made a bad experience on the same site.

**3.1.2. Experimental Framework.** After participants consented to the terms of the experiment, they were redirected to a music store entitled MelodiesFor.Us. They were shown detailed instructions. Further, the instructions informed them that they would be asked to fill out a post-experimental survey, and that completion of the survey would be the last requirement for being paid, and would also mark the end of the experiment. This information was important to set a common expectation about the end point of the experiment.

An essential part of the instructions was the description of the experimental budget and payment conditions: "For this study, we have given to you (in addition to the participation reward) a starting budget of $1.50. Using this budget, you have to purchase exactly one song in the music store. Any transaction in the shopping environment reduces your starting budget as described in the shopping environment. At the end of the study, you will receive any remaining money as a bonus payment." That is, we clearly stated the budget available, but did not describe in detail which specific actions could lead to a reduction of the budget during the experiment. Further, we set incentives for participants to minimize expenditures since they were able to keep any remaining funds.

Once participants read the instructions and began the task, they were redirected to the "shopping" page of

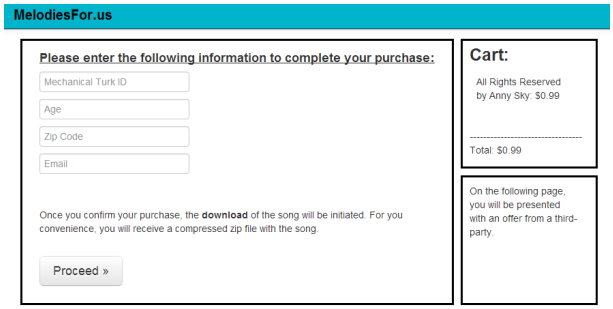


Figure 2. Checkout page. (Box at the bottom right was only present in treatment T1.)

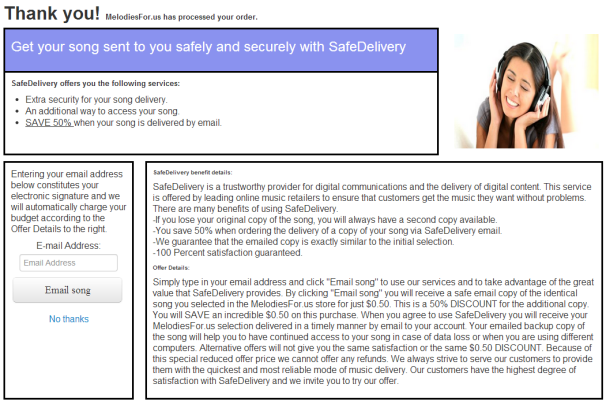


Figure 3. Post-transaction offer page.

MelodiesFor.Us (see Figure 1). This page displayed 6 songs which participants were able to sample and then add to their cart. All songs were taken from the site Jamendo.com and are released under a Creative Commons license. We selected songs of different genres to increase the likelihood of all participants finding at least one song they liked. Participants were required (and informed in the instructions) that they had to purchase exactly one song. All songs cost $0.99.

After adding a song to their cart and hitting the "Purchase" button, participants were redirected to the "Checkout" page (see Figure 2). This page required them to fill in a small amount of personal information to complete their purchase. If the treatment called for it (i.e., treatment T1, see Section 3.2), a small box was displayed with an intervention in the bottom right-hand corner.

Once participants entered their personal information, they were (depending on the treatment) redirected to an interstitial page (i.e., for treatments T2-T4; see Section 3.2), that displayed the matching intervention. After passing by the interstitial page or if no such intervention was present (i.e., treatments T0, and T1), participants were shown the post-transaction marketing offer page (see Figure 3). This offer page was identical for all treatments. The layout of the offer page was specifically designed to look similar but not identical (in terms of coloring and other features) to the main shopping site of MelodiesFor.Us. This tactic is commonly used on real sites, and presumably contributes to the ambiguity of the acceptability of these practices. From a consumer's perspective it likely adds to the impression that the primary shopping site and the post-transaction marketing offer are related, which may partly lead to a transfer of trust.

The post-transaction marketing offer page includes a mix of disclosures, with the most concrete explanation given at the bottom right. It offers a "50% discount" on a second copy of the song, i.e., for an additional expenditure of $0.50, participants would receive a second copy of the song they just purchased in the primary transaction and that they had already received at this point. Following examples in practice [2], the offer disclosures require a careful reading to fully comprehend the terms. We expected that this offer had essentially no value to the participants.

After either accepting the offer or not, participants were redirected to the post-experimental survey. This survey asked for basic demographic information, information about the experience and participants reflections on the experience, and included questions from suitable instruments meant to measure factors that may be significant in explaining behaviors expressed by participants in this experiment.

After completing the post-experimental survey, participants were redirected to a page that indicated their successful completion of the experiment. Participants could now indicate completion of the task on Mechanical Turk, and would subsequently receive payment.

## 3.2. Interventions

On the first glance, the most effective interventions that are likely to reduce the number of consumers that purchase deceptive post-transaction marketing offers are likely to be implemented on the side of post-transaction marketers. However, these marketers have little incentive to vigorously comply with the intent of regulations. Further, regulations such as ROSCA leave a lot of flexibility for implementations as given in our experiment [4]. In contrast, while first-party merchants benefit (at least in the short term) from their affiliation with dubious marketers, they have more to lose, and are more likely to follow the intent of regulations which explicitly target them. In addition, a critical element for the success of interventions is that they should aim to disrupt any psychological flow-state that consumers have entered once they engage in a shopping task. For example, an early privacy experiment by Spiekermann et al. demonstrated quite powerfully how interactions in a shopping environment (which would likely also include the sampling of songs) increase the susceptibility to willingly give up privacy [9].

**3.2.1. Intervention Types.** The concept of using interventions to reduce unwanted or insecure behaviors has found consideration in the usable security and privacy literature. As discussed above, our primary objective is to identify interventions that disrupt the flow-state associated with a shopping experience and are likely to raise awareness that a redirection to a third party is taking place.

To address this goal, we chose to use interstitial (full page) interventions for selected treatments (i.e., treatments T2-T4). Previous studies, in particular, Egelman et al. showed that interstitial warnings can lead to safer online behaviors or more privacy-conscious actions [20]. To contrast and compare the impact of the interstitial warnings, we also conducted a baseline treatment without warnings (T0), and a treatment that merely displayed a warning on the bottom right of the check-out page (T1; see Figure 2).

Within the treatments that present an intervention message on an interstitial screen, we used both passive (timer-based) and active (click-based) interventions. The passive interventions showed participants a message on an interstitial screen which closed after a certain period of time. We chose to use timer-based intervention messages partially due to the results of Good et al. [21]. In the context of installation decisions for software with spyware functionalities, they showed that subjects who acted slower during the experiment were less likely to install particularly harmful software [21]. Further, by presenting short notices on a separate screen before installation, they were able to reduce the number of potentially harmful installations, which shares similarities with all our interstitial interventions.

Additionally, we decided to experimentally test a treatment where participants needed to click a button to continue after reading the interstitial message. Besides the results by Good et al., this decision was motivated by requirements given by the Restore Online Shoppers' Confidence Act, which states that during post-transaction marketing scenarios consumers have "to perform an additional affirmative action, such as clicking on a confirmation button" [4].

## 3.3. Details about Experimental Process

**3.3.1. Detailed Description of Experimental Treatments.** In this study, the treatments differed only in their presentation of an intervention (see Table 1 for an overview). All of these interventions warned participants about a marketing offer from a third party that they were about to encounter. All other parts of the experiment were identical across treatments.

Each treatment was assigned a number ranging from 0 to 4, with 0 being the least obtrusive and 4 being the most obtrusive, and the others being on a scale between them. The "no intervention" treatment T0 is the baseline. Treatments T0 and T1 did not show participants any interstitial screen. Participants in those treatments purchased a song and were redirected immediately to the post-transaction offer page without any interstitial. In treatments T2, T3, and T4, participants were interrupted between these two parts of the shopping experience by an interstitial page which warned them about the third-party marketing offer page to follow. In treatments T2 and T3, the interstitial page was dismissed automatically after a set period of time (5 seconds for the "short" intervention, and 10 seconds for the "long" one). In T4, participants were required to hit a button labeled "Okay" to progress from the interstitial to the offer page. The message that we displayed to participants varied only in the last sentence of the intervention message. The generic intervention message displayed in treatments T1 through T4 was: "*On the following page, you will be presented with an offer from a third-party.*"

| Treatment | Intervention | Description |
|---|---|---|
| T0 | None | Baseline treatment. No intervention was present. |
| T1 | Checkout | A small box on the checkout page alerted participants that the next page was a marketing offer. |
| T2 | Timer short | An interstitial screen indicated the next page is a marketing offer. Participant was redirected after 5 seconds. |
| T3 | Timer long | An interstitial screen indicated the next page is a marketing offer. Participant was redirected after 10 seconds. |
| T4 | Button | An interstitial screen indicated the next page is a marketing offer. Participant was redirected after she clicked a button. |

TABLE 1. EXPERIMENTAL TREATMENTS OVERVIEW.

This message was not displayed in the baseline treatment T0. In T1, this was the entire message and it was displayed in the lower right-hand corner of the "checkout" page (see Figure 2). In the "Timer" treatments T2 and T3, this was followed by the phrase (with X being replaced with either 5 or 10, depending on the treatment): "*You will be redirected in X seconds.*"

In the active, click-based intervention of treatment T4, the first message was followed by the text (as well as a button): "*Please click the button below to continue.*"

These additional message explanations were always presented on a separate line from the main intervention message. The complete message was presented in a box that was constant size, regardless of the message enclosed.

**3.3.2. Experimenting on Amazon Mechanical Turk.** Our study was run on Amazon Mechanical Turk which allows "Requesters" to outsource Human Intelligence Tasks (HITs) to workers (Turkers). The service can be used for a variety of tasks, and has been used by many researchers including us for privacy and security studies with surveys (e.g., [22], [23]) and behavioral experiments (e.g., [24], [25]).

Mechanical Turk is a useful tool for conducting research. First, the payment/quality ratio per subject is significantly lower compared to traditional laboratory studies. This means that researchers are able to obtain a large sample at a relatively small cost (and generally in a short amount of time). Second, the demographic mix of participants is likely more diverse than university student convenience samples [26]. The demographic structure of Amazon Mechanical Turk is a topic that has been investigated by a number of authors in the last few years (e.g., [27], [28], [29]). Researchers have reported that slightly over half of the worker population is female, and the median age of Turkers is around 30 years [28]. These studies have shown that the country-of-origin for Turkers is in nearly half of the cases the United States with the other half being based in India, with small representations from other countries. In our study, we restricted participants to those that are U.S.-based

in order to ensure language comprehension and contextual understanding.

A number of authors have conducted experimental economics experiments on Mechanical Turk in recent years. For example, Horton used Mechanical Turk to replicate three experiments that have been extensively studied in economic laboratories [30]. One of the replicated experiments involved participants playing a one-shot prisoner's dilemma game (with payments one-tenth the size online as in a physical lab). The authors found no significant differences in behavior between the traditional and online versions of the study. Each replication that was conducted was completed in fewer than 48 hours and cost less than $1 per subject on average. Despite the low stakes and relative anonymity of Mechanical Turk subjects, the subjects' behaviors were consistent with findings from the standard laboratory [30].

**3.3.3. Ethical Considerations.** The study has been approved by our university's Institutional Review Board. However, by design, the subject matter of the experiment lends itself to being perceived as misleading and deceptive. The study aimed at reproducing somewhat unscrupulous (but real) tactics that are seen on e-commerce sites. Further, while many usability of privacy and security studies are being conducted on Mechanical Turk, our study is expected to impact individuals due to its immediate payment consequences. We presented potential participants with a consent form before the task which detailed that participants were under no obligation to complete the task and that they were able to leave the task at any time, if it made them feel uncomfortable.

## 4. Results

**Who completed the experiment?** As in a typical electronic commerce situation, we expected that many participants would not complete our purchasing study due to attrition [31]. For example, on the "checkout" page participants had to enter their email address, zip code, age, and Mechanical Turk ID; which could have led individuals to abort the shopping episode. However, we also expected attrition (to a lesser degree) on the consent form, instructions page, and music shop page, and on the post-transaction marketing site.

There were 651 people that began the experiment. Of this group, 476 (72%) finished the entire experiment including the post-experimental survey (see Table 2). On the screens that required input of some personal information (i.e., on the checkout page and the post-experimental survey page), attrition rates were 12% and 4% respectively (of the total number of participants in the experiment).

We also expected attrition on the post-transaction offer page and we observed that 7% of participants left the study on this page. This figure can perhaps be considered as a direct measure of the number of individuals who recognized that another transaction was taking place, but who were unable to figure out the implications of taking a particular action on the site. However, investigating the precise reasons for dropping out is the subject for future work; for example, it would be possible to send a separate paid survey to those Mechanical Turk users.

| Last page | Count | Percentage |
|---|---|---|
| Consent form | 10 | 2% |
| Instructions | 0 | 0% |
| Music Shopping | 24 | 4% |
| Checkout song | 79 | 12% |
| Post transaction offer | 46 | 7% |
| Post survey | 25 | 4% |
| Completed experiment | 476 | 72% |

TABLE 2. DROP-OUT RATES PER SCREEN, AND EXPERIMENT COMPLETION RATE.

| Education level | Count | Percentage |
|---|---|---|
| Graduate or professional degree | 59 | 13% |
| Four year college degree | 135 | 29% |
| Two year college degree | 51 | 11% |
| Some college | 174 | 37% |
| High school degree | 46 | 10% |
| Some high school | 2 | 0.4% |

TABLE 3. SELF-REPORTED EDUCATION LEVELS OF PARTICIPANTS.

From this point forward, all analyses will be conducted on only those participants who completed all parts of the experiment. From the post-experimental survey, we gathered the following demographic information. The mean age of participants was 31 years ($\sigma = 10$ years). As expected by our participation requirement, 98% of participants reported their country-of-origin as the United States. Participants in this study were 55% male (256 participants). Most participants had completed some college or more (409 participants; 90%; see Table 3). This demographic mix of participants was consistent with previously-completed surveys on the demographics of participants on Mechanical Turk [27], [30].

**How effective were the interventions?** As the main effect under investigation, we are interested whether the interventions inserted from the vantage point of the primary merchant lowered the relative amount of purchasers of the post-transaction offer. See Table 4 for the detailed results.

Overall, the conversion rate seems to be a pseudo-linear function of the inverse degree of the obtrusiveness of the intervention. That is, the lower-numbered treatments (which are less obtrusive) have higher conversion rates, while the higher-numbered and more obtrusive treatments have lower conversion rates, respectively. This is consistent with our expectations. However, these differences are not necessarily significant.

Treatment T0, the baseline treatment, did not include any type of intervention, and, as expected, had the highest conversion rate. Treatment T4, which presented participants with an active, click-based intervention, had the lowest conversion rate. This difference is statistically significant ($\chi^2 = 3.8$, $p = .05$). While the conversion rates for the remaining treatments are marginally lower compared to the baseline treatment, these differences are not significant. We consider this finding somewhat surprising. In particular, we did not expect the timer-based treatments T2 & T3 to differ that much from the click-based, active intervention, T4. From our point of view, a delay of 5-10 seconds seemed

| Treatment | Intervention | % Conversion (# convert/# total) |
|---|---|---|
| T0 | None | 18.7% (17/91) |
| T1 | Checkout | 18.1% (15/83) |
| T2 | Timer short | 16.5% (16/97) |
| T3 | Timer long | 17.7% (17/96) |
| T4 | Button | 9.0% (9/100) |

TABLE 4. EXPERIMENTAL TREATMENTS AND CONVERSION RATES.

| Rating | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Count | 237 | 88 | 73 | 42 | 27 |
| % | 51% | 19% | 16% | 9% | 6% |

TABLE 5. RATINGS OF POST-TRANSACTION OFFER.

like a sufficiently long time for participants to notice the switch of context.

**What did people think of the post-transaction offer?** Post-transaction offers sometimes have value, in practice. However, we argued that the offer in our experiment has no value (since participants would receive the same song a second time, but at an additional cost). Nevertheless, it may be the case that some individuals would perceive some value in the SafeDelivery service in our study; perhaps because they did not fully understand the details of the offer.

We found that over 50% of participants rated the offer's value at the lowest possible value and only 6% of the participants chose the highest value (see Table 5). That is, the majority understood the useless premise of the service, but a small group of participants was likely entirely misled by the offer's presentation style and disclosures. There is a significant relationship ($R^2 = 0.77$, $p < .05$) between the rating that participants gave to the service and the likelihood of having purchased the offer. The mean rating from purchasers of the offer is 3.6 ($\sigma = 1.3$) whereas the mean rating for the remaining participants is 1.7 ($\sigma = 1$).

## 5. Discussion and Concluding Remarks

Reducing the number of individuals who fall for post-transaction offers that are not valuable, and potentially misleading and deceptive is challenging. We aimed to break the flow induced by a shopping experience and impose interventions on the redirection behavior of primary merchants. We observe that nevertheless a substantial number of individuals purchase the post-transaction marketing offer; presumably because they do not recognize that they are now outside the primary shopping experience, or they do not invest enough effort to understand the offer. Only the most obtrusive intervention mechanism in our study that required a user action in the form of a click on a button had a significant effect on the conversion rate; in our case, reducing conversion by about 50%. One might interpret this reduction as a great success, and call for regulations that mimic this intervention. However, even in this quite obtrusive treatment condition 9% of the participants purchased a product that did not offer them any additional utility. Further, these individuals gave away almost their entire potential bonus payment from participating in the task (i.e., \$1.50 budget - \$0.99 for the mandatory song purchase - \$0.50 for the post-transaction purchase). As a result, those that purchased the post-transaction offer were only able to keep a bonus of \$0.01. On Mechanical Turk, a bonus payment of \$0.50 is a typical payment level, and participants certainly would have liked to receive this payment.

However, it may be difficult to achieve a much lower conversion rate in practice. As former FTC commissioners summarized, it is challenging to help "the ignorant, the unthinking, and the credulous [32]." On the other hand, it may be reasonable to shift the burden further away from consumers who are exhausted from the multitude of security, privacy and online marketing problems they face online. One potential step forward would be to provide more robust baseline regulation, that outlaws more unwanted practices [33], so that consumers can focus their attention on a smaller sample of potential problems, e.g., genuine cybercrime [34]. While the FTC has not updated any rules relevant for post-transactions marketing recently [35], the enactment of ROSCA is a step in the right direction, by limiting data-pass arrangements in the context of post-transactions marketing [4]. Alternatively, harsher penalties against first-party merchants and/or post-transaction marketers could nudge more of the involved businesses away from overwhelmingly unwanted practices with little consumer value [32].

We consider it surprising that the timer-based treatments did not impact conversion behavior in comparison to the baseline treatment and the weak intervention given by T1. Certainly, a larger participant pool may reveal a significant but small effect (see, for example, research by Böhme and Köpsell [36]); however, such a larger experiment may suffer from overfitting of the data. In contrast, the relative success of the click-based intervention perhaps reveals some wisdom behind the recommendation offered by ROSCA to have an "additional affirmative action" for the purchase of a post-transaction marketing offer. (However, the ROSCA recommendation was not intended as a primary merchant intervention as tested in our experiment.)

Likewise, our investigation is relevant to better understand the impact of the implementations of the European Union Consumer Rights Directive by European Union member states which include, for example, the German "Button Law." The law stipulates the introduction of an order button informing consumers of their obligation to pay for a promoted product or service, and the presentation of prices for goods and services before the button would be pressed. While the law also applies to online marketplaces such as Amazon and eBay, the primary motivation were fraudulent online transactions occurring in scenarios in which consumers do not expect to be engaging in a costly action. Our experiment includes a treatment with an affirmative action before the redirection to a post-transaction offer, and an affirmative action to conclude the purchase of the post-transaction offer, however, several details do not match the specifics of the law (such as the button text). While it would be helpful to design an experiment exactly targeting the "Button Law," our research provides insights into the magnitude of effects that can be achieved with specific user

interface stipulations to avoid consumer fraud.

**Acknowledgments:** We thank Chris J. Hoofnagle, Jim Jansen, Paul Muntean, David Reitter and the anonymous reviewers for their detailed feedback and suggestions for improvements of the manuscript. The research project (including the human subject experiments) has been supported by a Google Faculty Research Award, which we gratefully acknowledge. The research activities of Jens Grossklags are also supported by the German Institute for Trust and Safety on the Internet (DIVSI).

## References

[1] U.S. Senate, "Aggressive Sales Tactics on the Internet and Their Impact on American Consumers," November 2009.

[2] R. Meyer, "Prepared Statement of Robert J. Meyer," *Hearing before the Committee on Commerce, Science, and Transportation (United States Senate)*, Nov. 2009, available at: https://www.gpo.gov/fdsys/pkg/CHRG-111shrg54917/html/CHRG-111shrg54917.htm.

[3] infas Institut für angewandte Sozialwissenschaft GmbH, "Millionendelikt Internetbetrug," 2014.

[4] U.S. House, "Restore Online Shoppers' Confidence Act (ROSCA)," 2010, available at: http://www.ftc.gov/enforcement/statutes/restore-online-shoppers-confidence-act.

[5] European Union, "Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights," 2011.

[6] Bürgerliches Gesetzbuch (BGB), "Paragraph 312j Besondere Pflichten im elektronischen Geschäfts-verkehr gegenüber Verbrauchern," 2011.

[7] A. Nochenson and J. Grossklags, "An online experiment on consumers' susceptibility to fall for post-transaction marketing scams," in *Proceedings of the European Conference on Information Systems (ECIS)*, Tel Aviv, Israel, 2014.

[8] J. Grossklags and A. Acquisti, "When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information," in *Proceedings of the 6th Workshop on the Economics of Information Security (WEIS)*, Pittsburgh, PA, 2007.

[9] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior," in *Proceedings of the ACM Conference on Electronic Commerce (EC)*, Tampa, FL, 2001, pp. 38–47.

[10] J. Licata and C. Von Bergen, "An exploratory study of negative option marketing: Good, bad or ugly?" *International Journal of Bank Marketing*, vol. 25, no. 4, pp. 207–222, 2007.

[11] T. Metzger, "Visa tackles deceptive online "data pass" marketing," *Creditcards.com*, Apr. 2010, available at: http://www.creditcards.com/credit-card-news/visa-data-pass-deceptive-marketing-1282.php.

[12] Watchlist Internet, "Wie man durch Werbung auf Facebook in die Abo-Falle tappt," 2013, https://www.watchlist-internet.at/abo-fallen/wie-man-durch-werbung-auf-facebook-in-die-abo-falle-tappt/.

[13] National Fraud and Cybercrime Reporting Centre, "Watch out for the "new iphone for £1" subscription trap," 2015, http://www.actionfraud.police.uk/news/watch-out-for-the-new-iphone-for-1pound-subscription-trap-sept15.

[14] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security & Privacy*, vol. 3, no. 1, pp. 26–33, Jan.–Feb. 2005.

[15] P. Messinger, Y. Lin, and Y. Yan, "Negative option billing: Current practice and future concerns," *Asia Pacific and Globalization Review*, vol. 1, no. 1, pp. 55–69, Nov. 2011.

[16] M. Csikszentmihalyi, *Beyond Boredom and Anxiety*. San Francisco, CA: Josey-Bass, 1975.

[17] D. Kahneman, J. Knetsch, and R. Thaler, "Anomalies: The endowment effect, loss aversion, and status quo bias," *The Journal of Economic Perspectives*, vol. 5, no. 1, pp. 193–206, Winter 1991.

[18] D. Ballare and C. Von Bergen, "Negative option marketing and ethical theory," in *International Academy of Business and Public Administration Disciplines*, Dallas, TX, 2008, pp. 24–27.

[19] Federal Trade Commission, "FTC Policy Statement on Deception," 1983, available at: http://www.ftc.gov/ftc-policy-statement-on-deception.

[20] S. Egelman, J. Tsai, L. Cranor, and A. Acquisti, "Timing is everything?: The effects of timing and placement of online privacy indicators," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'09)*, Boston, MA, Apr. 2009, pp. 319–328.

[21] N. Good, J. Grossklags, D. Mulligan, and J. Konstan, "Noticing notice: A large-scale experiment on the timing of software license agreements," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'07)*, San Jose, CA, 2007, pp. 607–616.

[22] Y. Pu and J. Grossklags, "Towards a model on the factors influencing social app users' valuation of interdependent privacy," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 2, pp. 61–81, 2016.

[23] J. Weidman, W. Aurite, and J. Grossklags, "Understanding interdependent privacy concerns and likely use factors for genetic testing: A vignette study," in *Proceedings of the 3rd International Workshop Genome Privacy and Security (GenoPri)*, Chicago, IL, 2016.

[24] N. Christin, S. Egelman, T. Vidas, and J. Grossklags, "It's all about the Benjamins: An empirical study on incentivizing users to ignore security advice," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, G. Danezis, Ed. Springer, Berlin Heidelberg, 2012, vol. 7035, pp. 16–30.

[25] J. Grossklags and D. Reitter, "How task familiarity and cognitive predispositions impact behavior in a security game of timing," in *Proceedings of the 27th IEEE Computer Security Foundations Symposium (CSF)*, Vienna, Austria, 2014, pp. 111–122.

[26] C. Kam, J. Wilking, and E. Zechmeister, "Beyond the "narrow data base": Another convenience sample for experimental research," *Political Behavior*, vol. 29, no. 4, pp. 415–440, Dec. 2007.

[27] P. Ipeirotis, "Demographics of Mechanical Turk," Social Science Research Network, Technical Report No. 1585030, Tech. Rep., 2010.

[28] W. Mason and S. Suri, "Conducting behavioral research on Amazon's Mechanical Turk," *Behavior Research Methods*, vol. 44, no. 1, pp. 1–23, Mar. 2012.

[29] J. Ross, L. Irani, M. Silberman, A. Zaldivar, and B. Tomlinson, "Who are the crowdworkers?: Shifting demographics in Mechanical Turk," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'10), Extended Abstracts*, Atlanta, GA, Apr. 2010, pp. 2863–2872.

[30] J. Horton, D. Rand, and R. Zeckhauser, "The online laboratory: Conducting experiments in a real labor market," *Experimental Economics*, vol. 14, no. 3, pp. 399–425, Sep. 2011.

[31] C. Sismeiro and R. Bucklin, "Modeling purchase behavior at an e-commerce web site: A task-completion approach," *Journal of Marketing Research*, vol. 41, no. 3, 2004.

[32] H. Beales, R. Craswell, and S. Salop, "Efficient regulation of consumer information," *Journal of Law & Economics*, vol. 24, no. 3, pp. 491–539, Dec. 1981.

[33] J. Turow, C. Hoofnagle, D. Mulligan, N. Good, and J. Grossklags, "The Federal Trade Commission and consumer privacy in the coming decade," *I/S: A Journal of Law and Policy for the Information Society*, vol. 3, no. 3, pp. 723–749, Winter 2007-2008.

[34] M. Bidgoli and J. Grossklags, "Hello. This is the IRS calling.: A case study on scams, extortion, impersonation, and phone spoofing," in *Proceedings of the Symposium on Electronic Crime Research (eCrime)*, Scottsdale, AZ, 2017.

[35] C. Hoofnagle, *Federal Trade Commission Privacy Law and Policy*. Cambridge University Press, 2016.

[36] R. Böhme and S. Köpsell, "Trained to accept? A field experiment on consent dialogs," in *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, Atlanta, GA, 2010, pp. 2403–2406.