Research Data Reports

FEDERAL RESERVE BANK OF BOSTON™

No. 16-1

Did the Target Data Breach Change Consumer Assessments of Payment Card Security?

Claire Greene and Joanna Stavins

Abstract:
Previous research has found that perceptions of payment security affect consumers' use of payment instruments. We test whether the Target data breach in 2013 was associated with a change in consumers' perceptions of the security of credit cards and debit cards and with subsequent changes in consumers' use of payment cards. Using data from the Survey of Consumer Payment Choice (SCPC), we find that, controlling for possible confounding effects of demographic differences between the two groups, ratings by consumers who assessed the security of personal information of debit cards shortly after the breach were lower than ratings by consumers who responded before the breach was reported. On average, the rating on the security of personal information of debit cards relative to the rating on the security of other payment instruments was 11.3 percent lower shortly after the Target breach. Based on prior research on the impact of security assessments on payment instrument use, we would expect a small (economically insignificant) decline in debit card use from this lower rating. However, we find no statistically or economically significant change in debit card use from 2013 to 2014. For credit cards, there was no difference in the ratings given by consumers who responded to the survey before the breach was reported and the ratings of those who responded after the breach was reported.

Keywords: data breach, payment card security, Survey of Consumer Payment Choice, Target, debit card, credit card

JEL Classifications: D14, D18

Claire Greene and Joanna Stavins are members of the Consumer Payments Research Center in the research department of the Federal Reserve Bank of Boston. Claire Greene is a payments analyst. Joanna Stavins is a senior economist and policy advisor. Their e-mail addresses are claire.m.greene@bos.frb.org and joanna.stavins@bos.frb.org. The authors thank Allison Cole, Kevin Foster, Huijia Wu, and David Zhang for excellent analytical assistance. This paper, which may be revised, is available on the web site of the Federal Reserve Bank of Boston at http://www.bostonfed.org/economic/rdr/index.htm.

Scott Schuh and Suzanne Lorant provided helpful comments. The authors are responsible for any errors.

This version: August 2016

CPRC CONSUMER PAYMENTS Research Center

I. Introduction

On December 19, 2013, Target Corporation announced that hackers may have gained access to payment card data for 40 million credit and debit card accounts used in its stores in the 19 days between November 27 and December 15, 2013. The breach was widely reported, beginning on the evening of December 18.[1] The announcement of the Target breach in late 2013 provides an opportunity to test whether news about payment security breaches changes the way consumers assess and use payment instruments.

Security of payments has long been identified as an important aspect of the consumer payment experience and is receiving renewed attention in the wake of highly publicized cybercrimes. On January 26, 2015, following an intensive, 18-month research effort, the Federal Reserve released a plan entitled, "Strategies for Improving the U.S. Payment System," identifying security improvements as one of its top initiatives.[2] In identifying factors that could affect the end-to-end implementation of security processes, tools, and technologies, the plan notes that "[d]ifferent end-users may balance differently the tradeoff of security against cost and convenience of the payment experience, resulting in inconsistent adoption of security standards and technology." One aspect of this tradeoff involves consumers' perceptions of the security of payment instruments. In almost every annual Survey of Consumer Payment Choice to date, consumers have selected security as the most important aspect of payments, above cost, convenience, and other attributes.

Perceptions have been found to affect payment behavior. Using an econometric model of consumers' adoption and use of payment instruments, Schuh and Stavins (2015b) have found that enhanced security of payment cards is likely to increase the use of credit and debit cards,

[1] For example, http://money.cnn.com/2013/12/18/news/companies/target-credit-card/. A Lexis/Nexis search of print media on the term "Target" within the same paragraph as "data breach" resulted in one article on December 17, 2013, six articles on December 18, 2013, 118 articles on December 19, 2013, 141 articles on December 20, 2013, and 41 articles on December 21, 2013.

[2] https://fedpaymentsimprovement.org/

although the effect is small.[3] Similarly, if consumers' assessment of payment card security were to decrease dramatically, one might expect the use of credit and debit cards to decrease. Of course, these assessments, reflecting consumers' perceptions of security—or of other attributes of payment instruments—can shift even without any underlying changes in the real probability of fraud or theft. Notable external events, such as a widely publicized data breach, could shift consumers' perceptions. To gain insight into whether an event of this type could cause a dramatic shift in perceptions, it is important to understand the strength of the impact of a data breach on consumers' assessment and use of payment instruments. Understanding consumers' short-term response to the 2013 Target breach may be a first step toward understanding the longer-term effects of security breaches on consumers' perceptions of the security of various payment instruments.

At the time the Target data breach was announced, the Consumer Payments Research Center (CPRC) at the Federal Reserve Bank of Boston was surveying U.S. consumers about which aspects of payment instrument security were most important to them and how they rated those aspects for different payment instruments. This survey, conducted as a supplement to the 2013 Survey of Consumer Payment Choice (SCPC), was in the field when the breach was announced, so some respondents answered questions about payment instrument security before the breach was public knowledge, and other respondents answered shortly after the breach was widely known and was receiving extensive attention in the media. This created a natural experiment that made it possible to ask questions that may shed light on the short-term effect of news about data breaches on consumers' perceptions. (The supplementary survey did not ask whether or not respondents had been directly affected by the breach or even whether they knew about it.)

This Research Data Report addresses the following questions:

[3] Schuh and Stavins (2010, 2013) and Koulayev et al. (2016) also find that consumers' perceptions of the security of payment instruments affect their payment use.

- In the short term, did consumers who answered after the breach was announced (Group 2) rate payment instrument security differently from consumers who answered before the breach (Group 1)?
- In prior responses on earlier surveys, did respondents who later constituted Group 1 rate the security of payment instruments differently from those who later constituted Group 2?
- Are there demographic differences between the two groups that could be correlated with their ratings of payment instrument security?
- In the longer run, did consumers' ratings and use of payment instruments change between the fall of 2013 (before the breach) and the fall of 2014?

We find evidence that, in the short run, ratings of the security of debit cards in safeguarding personal information[4] (PI) by consumers who responded immediately after announcement of the Target breach were significantly worse than such ratings by consumers who responded before the breach was widely known. On average, the rating of the security of personal information when using debit cards relative to the rating of the security of personal information when using other payment instruments was 11.3 percent lower after the breach was announced. However, there is no direct evidence that the decline was caused by announcement of the breach or that the different ratings were later reflected in long-lasting differences in payment card use. We found no statistically significant change in the adoption or shares of payment instrument use of debit cards in the long run, from 2013 to 2014.

The remainder of this report is organized as follows: Section II describes the data used in the analysis. Section III reports consumers' absolute and relative ratings[5] of the security of personal information of three payment instruments in the short run, conditional on whether the consumers responded before or after the announcement of the Target breach. Section IV reports absolute and relative ratings for overall security in the 2013 SCPC to examine whether there were any differences between the two groups' ratings even before the breach was announced,

[4] Personal information includes name, address, telephone number, Social Security number, date and place of birth, mother's maiden name, etc.

[5] Relative ratings are consumers' ratings of an instrument based on one or more criteria relative to consumers' ratings of all the other payment instruments on the same criterion or criteria.

for example, possible unobserved differences in attitudes that could be an element of the pre- and post-announcement results. Section V compares the demographic characteristics of Groups 1 and 2 to examine whether or not these characteristics might be related to differences in the ratings. Section VI uses 2013 and 2014 survey data to test whether there were any longer-term changes in payment choice after the Target breach announcement. Section VII concludes.

II. Data

This analysis uses data from three iterations of the Survey of Consumer Payment Choice (SCPC), a representative sample of U.S. consumers, age 18 years and older. The SCPC is developed by the CPRC and was administered annually from 2008 to 2014 through the RAND Corporation's American Life Panel (ALP) to a sample of the adult U.S. population. The survey includes individual-level data on payment choice in the United States, including data on adoption and use of nine common payment instruments, adoption and use of several types of deposit and payment accounts (checking, savings, PayPal, etc.), assessment of payment characteristics, and payment history (credit rating, revolving on credit, overdraft, foreclosure, and bankruptcy). A detailed description of the data and survey methodology, together with a summary of aggregate changes in U.S. payments by consumers, is available in Foster et al. (2009, 2011), Foster, Schuh, and Zhang (2013), and Schuh and Stavins (2014, 2015a).

The first iteration of the SCPC used in this report, the 2013 SCPC, is the sixth in a series of annual surveys fielded primarily in October of each year. In the fall of 2013, a sample of U.S. adults answered questions about their assessment, ownership, and use of nine payment instruments as part of the 2013 SCPC. All respondents to the 2013 SCPC completed the survey before the announcement of the Target data breach. The 1,908 respondents to the 2013 SCPC were asked to rate overall payment instrument security from "very risky" to "very secure" on a scale of 1-to-5, where 1 is "very risky."[6] In general, a lower rating of a particular payment method means that a consumer considered that payment method to be inferior with respect to overall security. This overall security question, encompassing both "permanent financial loss"

[6] Omitted from this report are an additional 181 SCPC respondents who answered later or did not respond to the supplementary survey.

and "unwanted disclosure of personal information," incorporates many concepts of security. These concepts include the idea that a consumer does not want to lose money or have it stolen, that a consumer needs to have protection of personal information, such as a Social Security number, and that passwords and account information should be kept safe.

The second iteration used in this report is a supplementary survey to the SCPC that was in the field from early November 2013 through March 2014—coincidentally, at the time of the announcement of the Target data breach. The same 1,908 U.S. adults who had completed the 2013 SCPC were asked to report in more detail their assessments of specific aspects of payment instrument security. Most respondents to the supplementary survey provided their security assessments before the breach had become public knowledge (1,808 respondents). We refer to them as Group 1. One hundred of the respondents, however, provided assessments after the breach was public knowledge (Figure A.1). We refer to these respondents as Group 2. This divided sample created a natural experiment for investigating whether or not the group of consumers who responded before announcement of the breach assessed payment instrument security differently from the group who responded after.[7]

The supplementary SCPC was designed to gain insight into various aspects of security in order to contribute to the Federal Reserve's financial services payment system improvement project. In the supplementary survey, the concept of security is divided into three components, with a focus on separating financial security from privacy. The former concept involves a risk of losing money, while the latter involves the risk of having one's personal information obtained by others without one's consent. The supplementary SCPC also asked about confidentiality of information about the transaction itself.

Figure A.1 in Appendix A matches the timeline of data collection to the news announcement of the Target breach, using Google searches on the term "Target data breach" as

[7] If, instead of making use of a natural experiment, one were designing an experiment along these lines, it would be optimal to split the sample 50/50. But with this natural experiment resulting in lopsided sample sizes, the confidence intervals for group differences are larger than they would be with a balanced sample.

a proxy for consumer awareness of the breach.[8] Table A.1, also in Appendix A, summarizes the survey questions.

The third iteration used in this report is the 2014 SCPC, in the field 10 months after the Target breach was reported. In the fall of 2014, U.S. consumers again answered questions about overall payment instrument security and their adoption and use of nine payment instruments. Some consumers responded to all three iterations. Forty-nine (49) members of Group 2 and 1,339 members of Group 1 completed the 2014 SCPC. With so few Group 2 respondents completing all three iterations, all analysis of the 2014 SCPC reported here relies on the sample of 1,388 respondents who completed all three surveys.

III. Do Ratings of the Before and After Groups Differ in the Short Term?

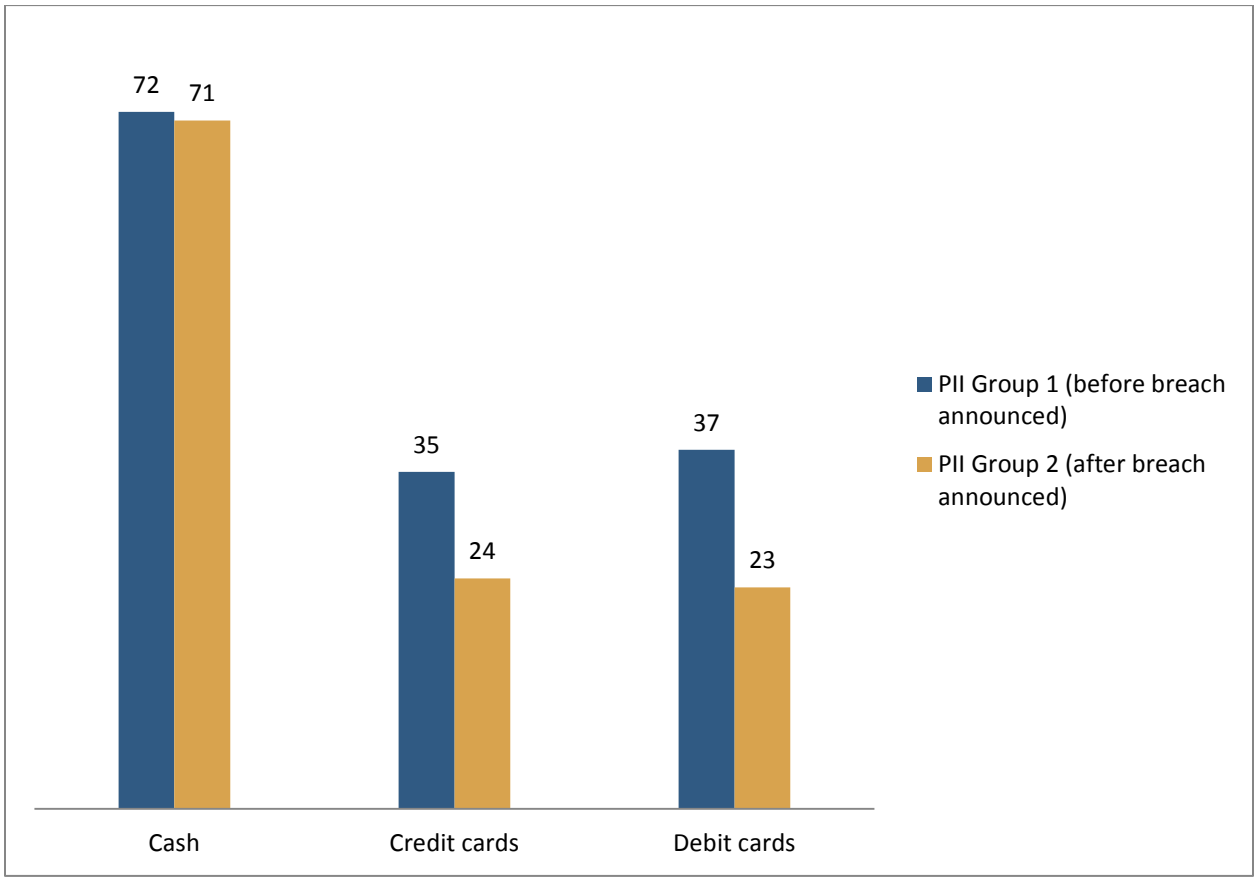
Absolute ratings

Did Group 2, responding to the survey supplement after the breach, rate payment cards more poorly than Group 1, responding to the supplement before the breach? We use cash as a control against which to examine consumers' ratings of cards, because the Target breach should not have affected consumers' perceived security of using cash. Almost three-quarters of each group rated cash as secure or very secure for security of personal information (Figure 1). Before and after the breach announcement, ratings of the security of cash were about the same.

Group 1 (responding before the breach announcement) rated credit card security for personal information higher than Group 2 (responding after) did. Thirty-five percent of Group 1 and 24 percent of Group 2 rated personal information as secure or very secure with credit cards.[9] Ratings of debit card security for personal information by consumers in Group 1 also were more favorable than those by consumers in Group 2 (responding after the breach).[10] Thirty-seven (37 percent) of consumer in Group 1 said personal information was secure or very

[8] The Google search intensity measure is an index, based on the number of searches at various points in time. "100" indicates the maximum number of searches in a particular time period. The source is *Google Trends*. In this case, the searches were for "Target data breach."
[9] Statistically significant at the 10 percent level.
[10] Statistically significant at the 5 percent level.

secure with debit cards, compared with just 23 percent of consumers in Group 2. Fewer than 40 percent of consumers in Group 1 said personal information was at risk ("risky") or very much at risk ("very risky") with debit cards, compared with almost 50 percent of consumers in Group 2 (Appendix B).



Source: 2013 SCPC, Federal Reserve Bank of Boston.

Figure 1: Percentage of consumers rating security of personal information "secure" or "very secure."

There was no statistically significant difference between the two groups' ratings of other aspects of payment instrument security, that is, security of financial wealth and the confidentiality of the transaction. See Appendix B for the percentage of respondents reporting positive (secure or very secure) and negative (risky or very risky) ratings for each of the three aspects of security studied (personal information, financial wealth, confidentiality).

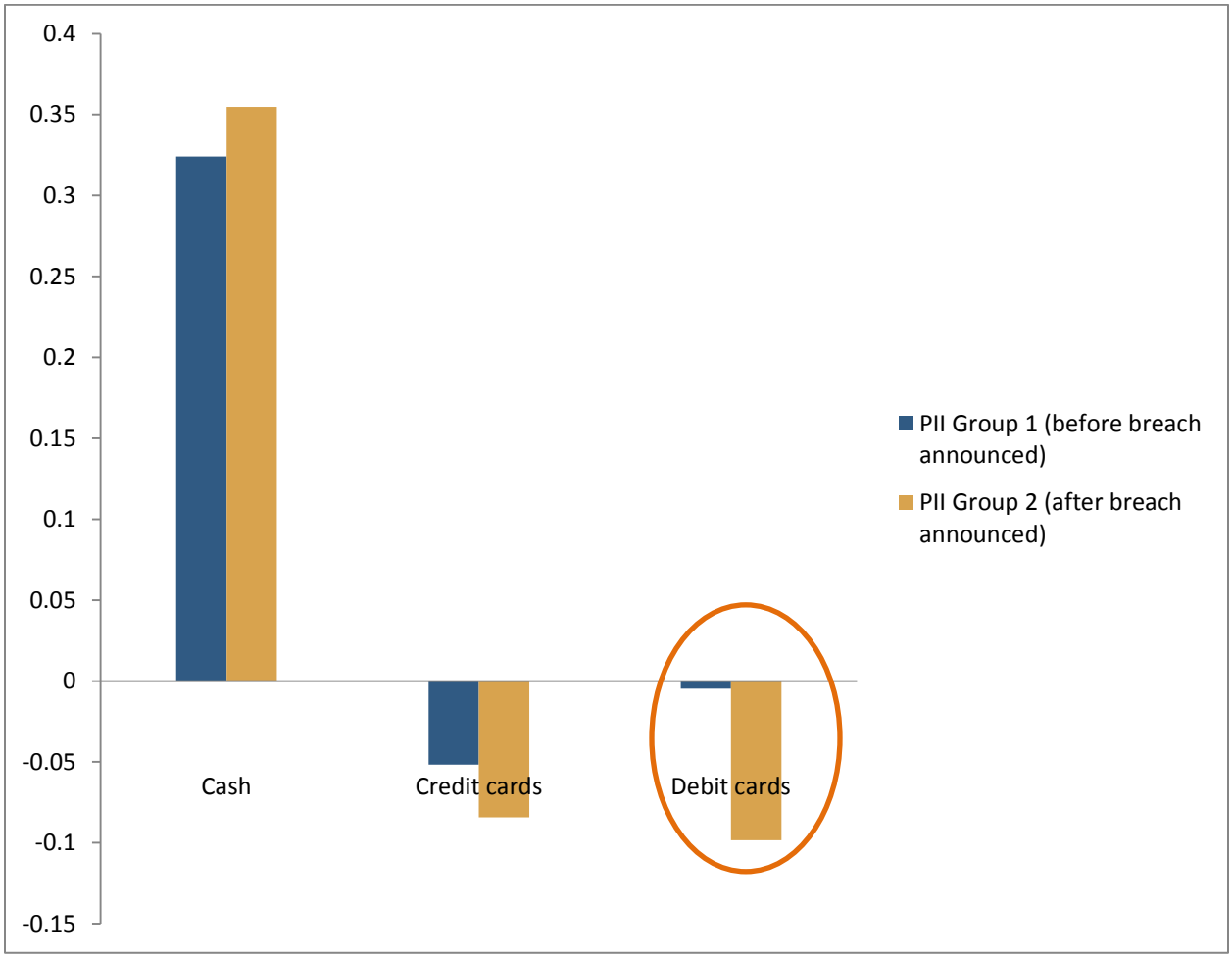
Relative ratings

Relative ratings of payment instruments (in the sense of ratings of a payment instrument relative to the ratings of other payment instruments) have been shown to be important for payment instrument adoption and use. Schuh and Stavins (2010, 2013) and Koulayev et al. (2016) have found that consumer payment behavior is strongly correlated with relative characteristics, that is, a consumer's average rating of a given payment method relative to his or her ratings of all the other payment methods.[11] Using relative ratings makes it possible to correct for each individual's assessment. For example, two respondents might rate debit cards as somewhat insecure, or "2." But that rating has a different meaning if one of those respondents rates security of cash and credit cards as "4" and the other respondent rates the security of cash and credit cards as "1." The first respondent considers debit cards to be less secure than other payment methods, while the second respondent considers debit cards to be more secure than other payment methods. We expect that consumers' behavior is more likely to be correlated with such relative assessments than with the absolute assessments.

Figure 2 shows ratings of Group 1 and Group 2 of particular payment instruments relative to these groups' ratings of all the other payment instruments. Note that the relative rating can be positive (if the payment method is considered superior to other payments) or negative (if the payment method is considered inferior to other payments). A rating at the baseline in Figure 2 means that—on average—respondents to the supplementary survey rate the payment instrument the same as the other instruments (in each case, six of seven payment

[11] Appendix C shows how the relative characteristic ratings were constructed. In addition to security, other characteristics in the 2013 SCPC were acceptance, setup, convenience, cost, and record keeping.

instruments[12] were used to construct the average). Bars below the baseline indicate that consumers rate the instrument as less secure than other payment instruments. Bars above the baseline indicate that respondents rate the instrument more positively than other payment instruments. For example, the first set of bars on the left in Figure 2 shows that both Group 1 and Group 2 rated cash as highly secure for safety of personal information compared with check, debit, credit, prepaid, OBBP, and BANP.[13]



Source: 2013 SCPC, Federal Reserve Bank of Boston, and authors' analysis.
Note: Relative ratings are the average of the natural logarithmic ratios of each payment method versus other payment methods. The values can range from approximately -1.6 to +1.6.

Figure 2: Ratings of security of personal information, relative to rating of other payment instruments.

[12] The seven payment instruments are cash; check; debit, credit, and prepaid cards; online banking bill pay (OBBP); and bank account number payment (BANP).
[13] Relative ratings are the average of the natural logarithmic ratios of each payment method versus the other payment methods. The values can range from approximately -1.6 to +1.6.

Relative to other payment instruments, Group 1 (before the breach announcement) and Group 2 (after the breach announcement) both rated the security of personal information with credit cards as inferior to average of the ratings for personal information security of all the other payment instruments studied. This seems odd intuitively because one might expect that consumers whose awareness of card hacking had been heightened by news of the breach would rate the security of both credits and debit cards as relatively worse than other consumers would. However, the difference between Group 1 and Group 2 in the relative ratings of credit cards' personal information security is not statistically significant, and the explanation for the failure of the announcement to significantly affect these ratings may well be that even before the announcement consumers took a dim view of the security of personal information with credit cards.

In contrast, the ratings by the pre-announcement group (Group 1) and the post-announcement group (Group 2) of the security of their personal information with debit cards relative to the security of their personal information with other payment instruments diverged significantly [circled bars in Figure 2]. For debit cards, consumers in Group 1 had a neutral view. Consumers in Group 2 had a significantly more negative view of the security of personal information with debit cards compared with consumers in Group 1. Knowledge of differences in consumer liability may have been a factor in the differences in the credit card and debit card ratings. It is possible that consumers with increased awareness of hacking also had increased awareness of the consumer protections mandated for credit cards.[14]

IV. Might Differences in Ratings Be Related to Prior Differences between the Groups?

Because this is a natural experiment, it is possible that differences between the two groups—either demographic differences or attitudinal differences or some other difference(s)

[14] Under the Fair Credit Billing Act (FCBA), a consumer's liability for unauthorized use of a credit card is limited to $50 in most instances. The Electronic Funds Transfer Act (EFTA) limits liability for fraudulent charges or transfers. https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards. To limit their liability for debit cards to $50, consumers must report unauthorized transactions within two business days. After two days, liability increases to $500; after 60 days liability is unlimited.

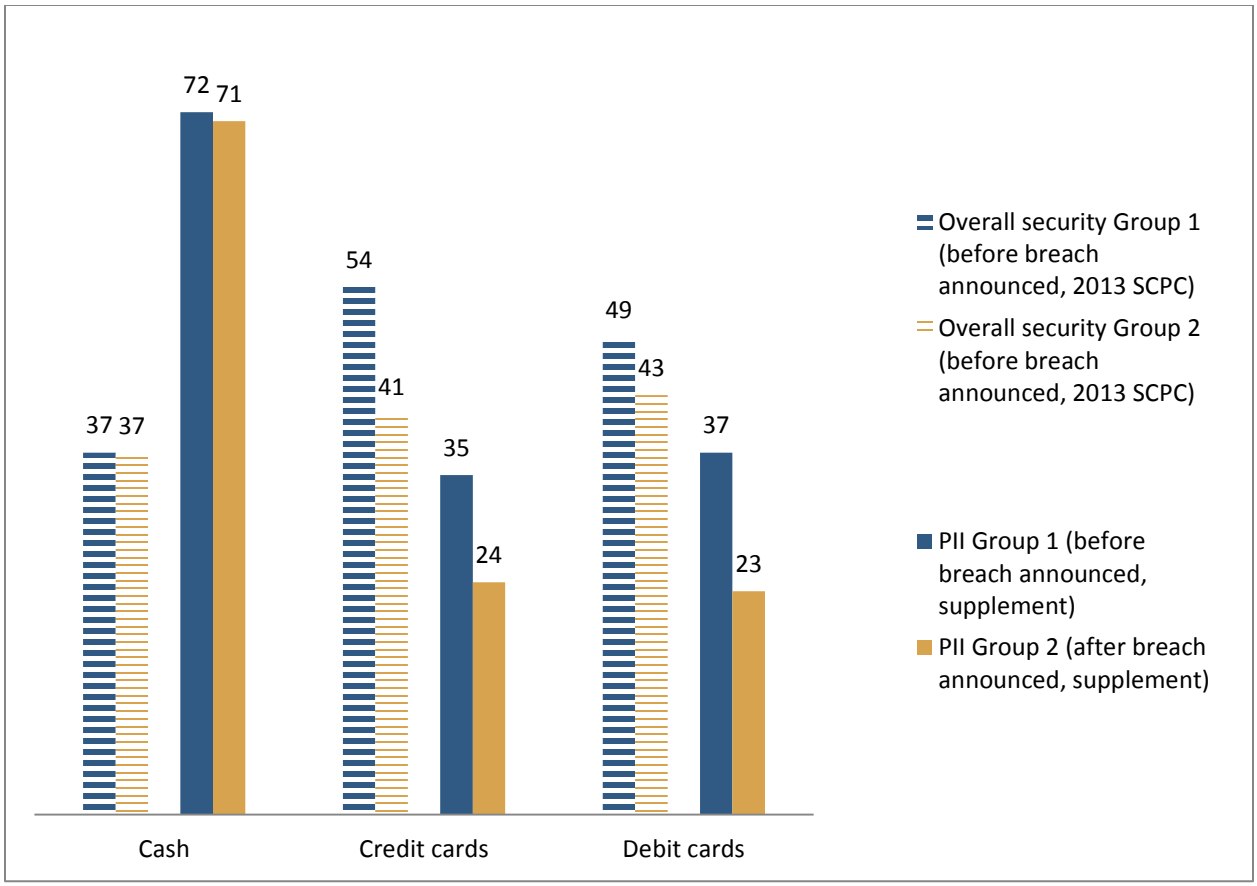
that we cannot measure—underlie their ratings. Therefore, we cannot look only at the responses of Group 1 and Group 2 to the supplementary security survey. In addition, we need to compare the responses of the members of Group 1 and Group 2 to the 2013 SCPC, to see whether any differences in assessments could be due to the fact that the two groups had already rated payment instruments differently prior to announcement of the Target breach. Members of both Group 1 and Group 2 took the 2013 SCPC (but not the supplementary survey in the case of Group 2) before the Target breach was announced. We use ratings by both groups before the announcement as a control to examine whether or not the post-breach differences are somehow related to the prior opinions of their members. (We explore demographic differences later.)

Absolute ratings

Again, we use cash as a control to examine ratings of payment cards. In the 2013 SCPC, respondents who later constituted Group 1 rated cash the same as respondents did who later constituted Group 2: thirty-seven percent rated cash as secure or very secure. As noted above, the two groups also rated cash as about the same for security of personal information in the supplementary SCPC as in the 2013 SCPC (Figure 3). As far as cash ratings are concerned, these two groups responded the same way.

With regard to credit cards, even before the breach was announced, Group 1 rated the overall security of credit cards higher than Group 2 did, as Figure 3 shows: 54 percent of Group 1 rated the overall security of credit cards as secure or very secure compared with 41 percent of Group 2.[15] In the supplementary SCPC, Group 1 rated credit card security for personal information more secure than Group 2 did. Thirty-five percent of Group 1 and 24 percent of Group 2 rated personal information as secure or very secure.[16] Given that differences in ratings between the two groups were already present in the SCPC, there is no evidence that the Target breach affected ratings of the security of personal information of credit cards.

[15] Statistically significant at the 5 percent level.
[16] Statistically significant at the 10 percent level.



Source: 2013 SCPC, Federal Reserve Bank of Boston, and 2013 SCPC Supplementary Survey.

Figure 3: Percentage of consumers rating security of personal information "secure" or "very secure" compared with prior ratings of overall security.

In the 2013 SCPC, the two groups rated overall security of debit cards about the same (Figure 3). You can see in Figure 3 that the two groups' 2013 SCPC ratings of debit cards differ less than their 2013 SCPC ratings of credit cards. The difference in the debit card ratings in the 2013 SCPC (49 percent secure or very secure by Group 1 and 43 percent by Group 2) is not statistically significant. As noted above, in the supplementary SCPC, ratings of debit card security for personal information by consumers in Group 2 (responding after the announcement of the breach) were less favorable than those by consumers in Group 1.[17] Thirty-seven percent of consumers in Group 1 said that personal information was secure or very secure with debit

[17] Statistically significant at the 5 percent level.

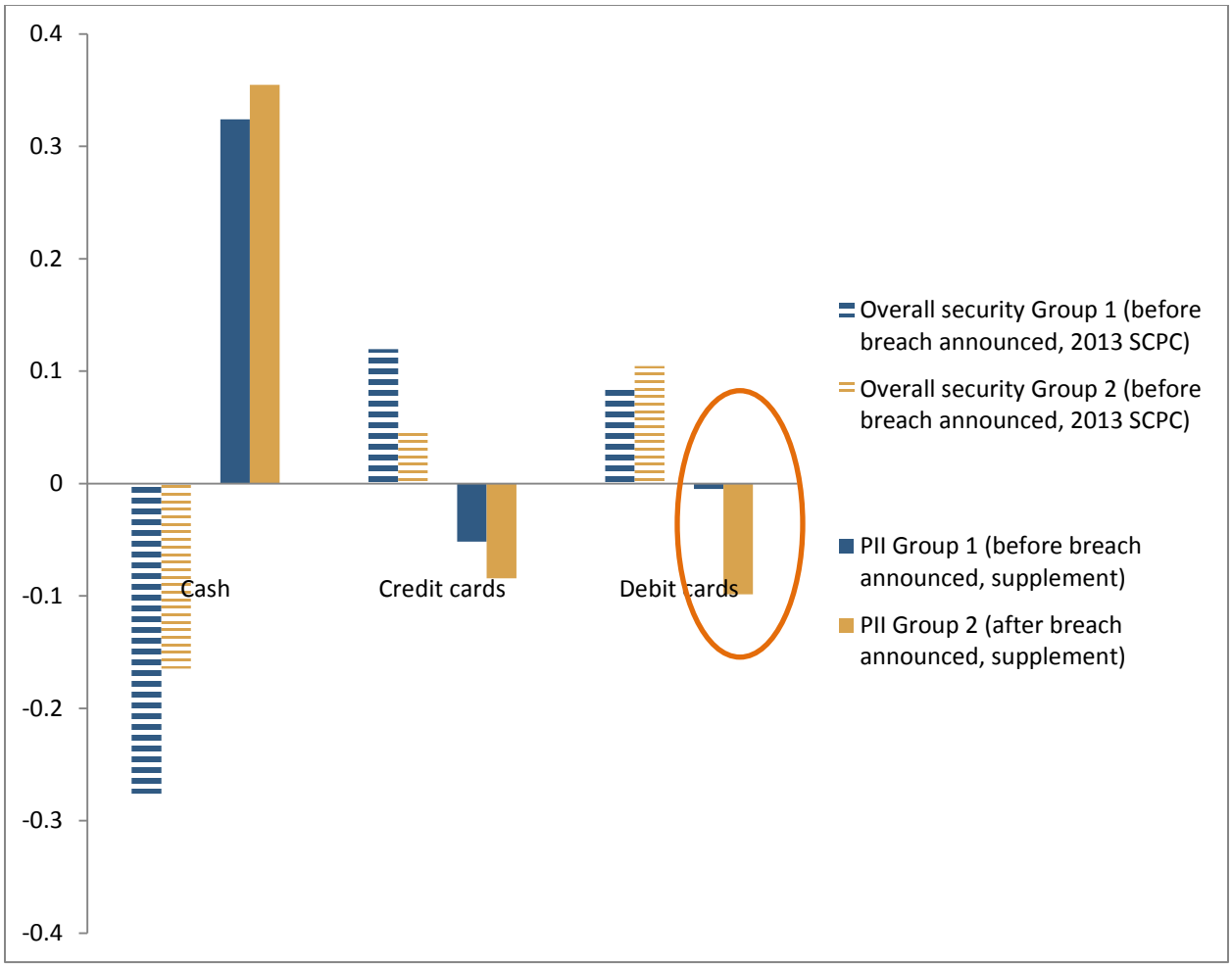
cards. Just 23 percent of consumers in Group 2 said that personal information was secure or very secure with debit cards. These differences are statistically significant.

Relative Ratings

The relative ratings shown in Figure 4 indicate that Group 2 ratings of the overall security of credit cards were worse than the ratings of Group 1.[18] These overall ratings were provided before the Target breach was announced. This agrees with the finding that consumers in Group 2 were significantly less likely to rate overall security of credit cards as secure or very secure than consumers in Group 1. Regarding the security of personal information aspect of overall security, both Group 1 (before the breach announcement) and Group 2 (after the announcement) rated the security of personal information with credit cards as inferior to the alternatives.[19]

Consumers in the two groups (both responding before the breach became public) rated the relative overall security of debit cards about the same in the main 2013 SCPC. However, there is a significant divergence between ratings of the pre-announcement group (Group 1) and the post-announcement group (Group 2) of the security of their personal information with debit cards relative to the security of their personal information with other payment instruments [circled bars in Figure 4]. This finding suggests that for debit cards, the differences between the two groups in their ratings of the security of personal information for debit cards may have been related to the Target breach announcement.

[18] Statistically significant at the 10 percent level. These ratings are from the 2013 SCPC, not the supplementary survey. Note that the groups were defined later, based on when respondents replied to the supplementary survey.
[19] These ratings are from the supplementary survey.



Source: 2013 SCPC, Federal Reserve Bank of Boston, authors' analysis.
Note: Relative ratings are the average of the natural logarithmic ratios of each payment method versus other payment methods. The values can range from approximately -1.6 to +1.6.

Figure 4: Relative ratings of security of personal information vs. prior relative ratings of overall security.

V. Demographic Characteristics vs. Timing: Effect on Assessments

To enable better estimates of payments assessments and behavior of the entire population of U.S. consumers, SCPC respondents were assigned survey weights designed to align the composition of the SCPC sample with that of the Current Population Survey, to the extent possible.[20] This follows common practice in other social science surveys.[21] The entire

[20] http://www.census.gov/programs-surveys/cps.html
[21] For a detailed discussion of 2013 SCPC post-stratification weighting, see Angrisani, Foster, and Hitczenko (2015, 2016 [forthcoming]).

SCPC sample was used for weighting, not the two subsamples discussed here (Group 1 and Group 2). Therefore, the demographics of Group 1 and Group 2 do not match. Demographic differences between Group 1 and Group 2 may be a factor in their different ratings. Compared with Group 1, respondents in Group 2 are more likely to be younger than 44, nonwhite, Latino, and employed (Table 1).

	Group 1	Group 2	Current Population Survey
Age 25–44	34%	66%	34%
Nonwhite	22%	32%	21%
Latino	16%	23%	15%
Employed	62%	76%	60%

Source: 2013 SCPC, Federal Reserve Bank of Boston.
Note: The entire SCPC sample, not the two subsamples discussed here (Group 1 and Group 2), was used for weighting. Differences between Groups 1 and 2 listed in this table are statistically significant.

Table 1: Comparison of sample, 2013 SCPC Groups 1 and 2 with Current Population Survey.

	Absolute	**Relative**
Credit card ratings		
Entire sample (Groups 1 and 2)	2.87	-.05
Age 25–44	2.88	-.03**
Nonwhite	2.78*	-.05
Latino	2.85	-.08
Employed	2.90	-.04**
Debit card ratings		
Entire sample (Groups 1 and 2)	2.93	-.01
Age 25–44	2.91	.02**
Nonwhite	2.90	.01
Latino	3.00	.01
Employed	2.94	.00*

Source: 2013 SCPC, Federal Reserve Bank of Boston, authors' analysis.
Note: Asterisks indicate that ratings of the identified group are statistically different from ratings of those outside the group. For example, relative ratings of consumers aged 25–44 are different from relative ratings of consumers younger than 25 or older than 44. * $p < 0.10$, ** $p < 0.05$

Table 2: Comparison of ratings of PII security, demographic subgroups versus whole sample, 2013 SCPC.

In some cases, members of these subgroups that are overrepresented in Group 2 rated security of personal information differently than respondents outside these subgroups, and the differences are statistically significant. Looking at relative ratings, respondents aged 25 to 44 rated the security of personal information of both credit cards and debit cards more positively than respondents aged 18 to 24 and 45 and older. People who were employed rated the security of personal information of both credit cards and debit cards as more positive than did those with a different employment status. For absolute ratings, nonwhites rated the personal information security of credit cards significantly worse than whites did (Table 2).

To investigate whether these demographic differences between Group 1 and Group 2 affected the discrepancy in their security ratings, we conducted a regression analysis. For example, we investigated whether being between the ages of 25 and 44 was associated with rating the relative security of personal information of debit cards as inferior. If that were the case, it might mean that the demographic composition of Group 2—and not anything to do with the timing of Group 2's response to the supplementary security survey—was associated with the lower security rating. Demographic variables included in the analysis were age, gender, race, ethnicity, education, marital status, nationality, income, employment, geographic region, financial responsibility, household size, home ownership, and bankruptcy history (Appendix D, part 1).[22]

In fact, however, we found that even after controlling for all the demographic factors, Group 2 members (subjects who responded after the Target breach was announced) rated the security of debit cards significantly lower than Group 1 members did. On average, the relative rating on the security of personal information of debit cards was 11.3 percent lower by Group 2 than the rating by Group 1 (Table 3). There was no statistically significant effect of membership in Group 2 versus membership in Group 1 on overall ratings of debit cards (Table 3), so Group 2 did not hold a generally more negative view of overall debit card security before the breach than Group 1 did. Being a member of Group 2 also had no statistically significant effect on the

[22] Financial responsibility encompasses questions about responsibility for paying monthly bills, shopping, and making decisions about savings and investments. Financial distress includes questions about filing for bankruptcy protection in last 12 months and last seven years.

rating of the security of personal information for credit cards or on the security of financial wealth for credit or debit cards. Although we controlled for the effects of several observed characteristics of individual respondents, other unobserved differences of consumers in Group 2 compared with Group 1 might have influenced their perceptions and relative security ratings.

Percentage effect of Group 2 membership:	**Debit Cards**	**Credit Cards**
Relative rating of overall security	-2.0	-7.1*
Relative rating of the security of personal information	-11.3***	-4.2
Relative rating of the security of financial wealth	1.2	1.7

Source: 2013 SCPC, Federal Reserve Bank of Boston.
Note: Coefficient estimates of the effect of being in Group 2 on relative security ratings (OLS regression). The coefficients are shown in percentage points, indicating the average percentage difference between Group 1 and Group 2 ratings of the corresponding payment instrument relative to other instruments. For example, the number −11.3 means that on average Group 2 rates the security of personal information for debit cards as 11.3 percent lower than Group 1 does (both relative to other payment methods). * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$ *See* Appendix E for full regression results.

Table 3: Regression of Security Assessments on Being a Member of Group 2.

To test the strength of this connection between being a member of Group 2 and the relative rating of security of personal information of debit cards, an ordered probit regression analysis was performed to see whether being a member of Group 2 could predict the absolute security rating (Appendix D, Part 2). Group 2 membership predicts a more negative rating for the absolute security rating of debit card personal information, although the connection is somewhat less statistically significant than for the relative rating. (As noted above, relative ratings have been shown to be important to the choice of which payment instrument to use.) For absolute ratings for the security of financial wealth, there was no statistically significant effect of Group 2 membership on the ratings of credit or debit cards (as was found above for relative ratings).

Some Group 2 respondents took the supplementary survey immediately after the Target breach was announced; 30 Group 2 respondents took the survey in the two weeks between December 19, 2013 and January 1, 2014. Others took it weeks after the announcement: 29 within two to four weeks and 41 after more than four weeks. However, controlling for the number of

days elapsed between the breach announcement and the day when the respondents took the survey did not alter our relative ratings results .[23]

VI. Long-Term Responses to Security Breaches

The SCPC is an annual survey, so the next opportunity to measure security assessments of payment instruments and payment instrument use occurred 10 months after the Target breach occurred. Compared with the 2013 full sample, the 2014 full sample (cited results not shown) showed a decline in both the relative and absolute security ratings of debit cards,[24] an increase in the absolute security ratings of cash,[25] and no statistically significant change in the security ratings of credit cards. Also, the 2014 SCPC full sample showed no statistically significant differences in the number of payments by cash, credit card, or debit card or in the shares of use of these payment instruments. Debit cards remained the most popular payment instrument among consumers in 2014, accounting for 30.8 percent of their monthly payments (compared with 31.1 percent in 2013, a statistically insignificant difference).

Looking at respondents who completed both the 2013 SCPC and the 2014 SCPC (some of whom did not complete the supplementary security survey in 2013), there was a statistically significant decline in both their relative and absolute security ratings of debit cards from 2013 to 2014.[26] Absolute ratings declined from 3.14 to 3.02. For comparison, absolute ratings of credit cards declined from 3.31 to 3.27. Relative ratings declined from 0.07 to 0.01. (For comparison, relative ratings of credit cards declined from 0.13 to 0.11 over the same time period.) Also, for

[23] When the number of days was included in the model, it had no significant effect on the security rating, and the effect of being in Group 2 remained unchanged. Both direct and interaction effects were included. We also separated Group 2 respondents who answered the survey within two weeks after the Target breach from those who answered two to four weeks after the breach and those whose who answered later than four weeks after the breach. None of these specifications affected the main result: a significant difference between Group 1 and Group 2 in the relative rating of the security of personal information of debit cards. In addition, if we truncate the entire sample to those who answered the supplementary survey within four weeks of the breach (before and after), we still found a significant difference between Group 1 and 2.

[24] Statistically significant at the 1 percent level for both absolute and relative ratings.

[25] Statistically significant at the 5 percent level.

[26] Statistically significant at the 1 percent level.

this panel, there was no statistically significant change in their shares of use of debit cards, credit cards, or cash from 2013 to 2014.[27]

Schuh and Stavins (2015b) modelled the effect on debit card use of consumers' assessments of the security of personal information. Based on their estimate of the responsiveness of debit card use to a change in the assessment of the security of personal information, a 10 percent increase in rating would result in an increase in debit card share of 0.02 percentage points. So an 11.3 percent decline in rating would result in a decrease in debit card share of 0.022 percentage points. A 0.022 percentage point decline in share from 2013 to 2014 would not be statistically or economically significant. Therefore, it is not surprising that we do not observe a statistically or economically significant change in use from 2013 to 2014.

This lack of long-term behavior change aligns with work by Kosse (2013), which found that while reports of skimming depress debit card use in the Netherlands, "the effect only lasts for one day, with consumers reverting back to their normal payment behavior almost immediately." Also, Mikhed and Vogan (2015) found that, while consumers respond to their own exposure to a breach, exposure to news about data breaches does not correlate with a consumer response.

VII. Conclusion

As demonstrated by a regression controlling for demographic and income differences, ratings of debit cards' relative security of personal information by consumers responding shortly after the Target breach were inferior to such ratings by consumers who responded before the breach. On average, the relative rating of the security of personal information of debit cards was 11.3 percent lower shortly after the Target breach. However, comparing 2014 debit card use with 2013 use, we find no significant change in debit card use from 2013 to 2014. Therefore, while the security ratings and survey completion times (pre- or post-breach) are

[27] Narrowing this group further to only respondents who completed all three iterations of the SCPC analyzed here (2013, supplementary security survey, and 2014), there were no statistically significant changes in the adoption of debit cards and credit cards from 2013 to 2014 by either Group 1 or Group 2. In addition, there were no statistically significant changes in shares of use by members of either Group 1 or Group 2. Only 49 members of Group 2 completed the 2014 SCPC; this small sample size makes statistical analysis difficult.

correlated, we find no evidence that the Target breach announcement caused any long-term effects on changes in payment behavior.

References

Angrisani, Marco, Kevin Foster, and Marcin Hitczenko. 2015. "The 2013 Survey of Consumer Payment Choice: Technical Appendix." Federal Reserve Bank of Boston Research Data Report No. 15-5.

Angrisani, Marco, Kevin Foster, and Marcin Hitczenko. forthcoming. "The 2014 Survey of Consumer Payment Choice: Technical Appendix." Federal Reserve Bank of Boston Research Data Report

Foster, Kevin, Erik Meijer, Scott Schuh, and Michael A. Zabek. 2009. "The 2008 Survey of Consumer Payment Choice." Federal Reserve Bank of Boston Public Policy Discussion Paper 09-10.

Foster, Kevin, Erik Meijer, Scott Schuh, and Michael A. Zabek. 2011. "The 2009 Survey of Consumer Payment Choice." Federal Reserve Bank of Boston Public Policy Discussion Paper 11-1.

Foster, Kevin, Scott Schuh, and Hanbing Zhang. 2013. "The 2010 Survey of Consumer Payment Choice." Federal Reserve Bank of Boston Research Data Report 13-2.

Kosse, Anneke. 2013. "Do Newspaper Articles on Card Fraud Affect Debit Card Usage?" *Journal of Banking and Finance* 37 (12): 5382–5391.

Koulayev, Sergei, Marc Rysman, Scott Schuh, and Joanna Stavins. 2016. "Explaining Adoption and Use of Payment Instruments by U.S. Consumers." *RAND Journal of Economics* 47 (2), Summer: 293–325.

Mikhed, Vyacheslav, and Michael Vogan. 2015. "Out of Sight, Out of Mind: Consumer Reaction to News on Data Breaches and Identity Theft." Federal Reserve Bank of Philadelphia Working Paper 15-42.

Schuh, Scott, and Joanna Stavins. 2010. "Why Are (Some) Consumers (Still) Writing Paper Checks?" *Journal of Banking and Finance* 34(8): 1745–1758.

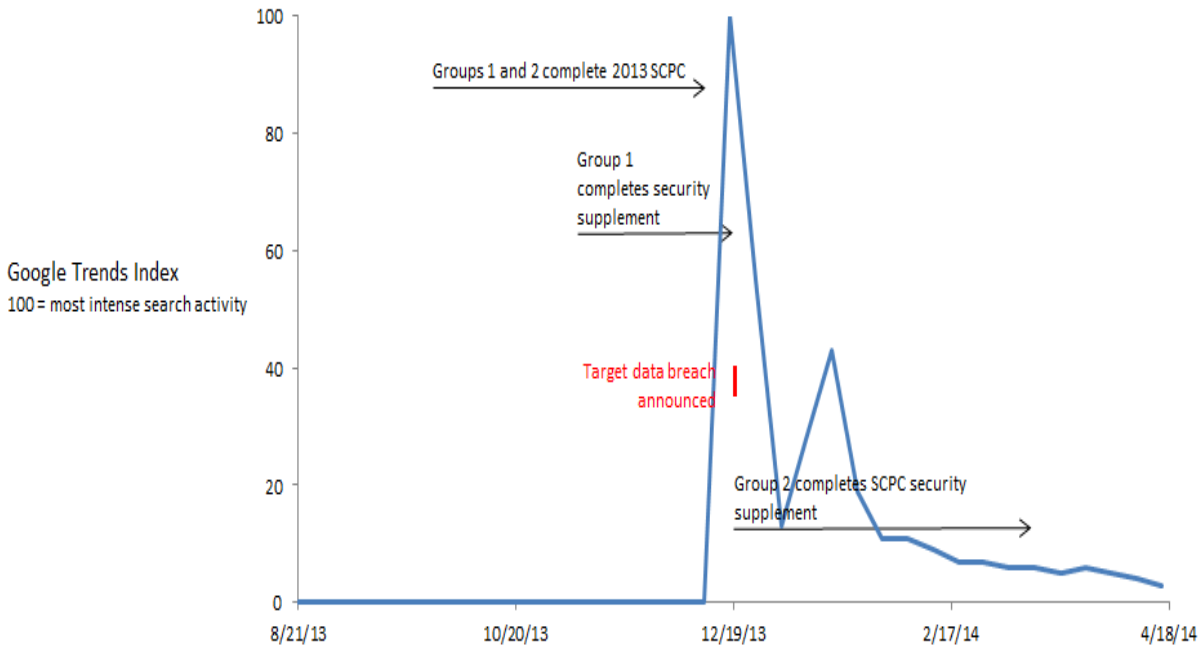
Schuh, Scott, and Joanna Stavins (2013). "How Consumers Pay: Adoption and Use of Payments." *Accounting and Finance Research* 2(2): 1–21.

Schuh, Scott, and Joanna Stavins. 2014. "The 2011 and 2012 Surveys of Consumer Payment Choice." Federal Reserve Bank of Boston Research Data Report 14-1.

Schuh, Scott, and Joanna Stavins. 2015a. "The 2013 Survey of Consumer Payment Choice." Federal Reserve Bank of Boston Research Data Report 15-4.

Schuh, Scott, and Stavins, Joanna. 2015b. "How Do Speed and Security Influence Consumers' Payment Behavior?" *Contemporary Economic Policy* doi: 10.1111/coep.12163.

Appendix A. Data Collection Timeline and Security Questions



Source: Federal Reserve Bank of Boston, Google Trends.
Note: 100 equals most intense search activity on "Target data breach." The spike in searches occurred almost instantaneously following announcement of the breach; software limitations cause it to appear on the figure to have begun slightly in advance of the announcement.

Figure A.1: Timeline of data collection in relation to announcement of Target data breach.

2013 SCPC Administered 9/27/2013–12/10/2013	**SCPC supplementary security survey** Administered 11/6/2013–3/10/2014
Overall security Suppose a payment method has been stolen, misused, or accessed without the owner's permission. Please rate the **SECURITY** of each method against permanent financial loss or unwanted disclosure of personal information.	***Security of personally identifiable information*** Suppose a payment method has been stolen, misused, or accessed without the owner's permission. Please rate the security of each method against unwanted disclosure of personal information such as name, address, telephone number, Social Security number, date and place of birth, mother's maiden name, etc.
	Security of financial wealth Suppose a payment method has been stolen, misused, or accessed without the owner's permission. Please rate the security of each method against permanent financial loss to the owner of the payment method.
	Security of information about of payment transactions Suppose a payment method has been stolen, misused, or accessed without the owner's permission. Please rate the security of the confidentiality of each method against others' finding out what products were purchased, how much was paid, or where the products were bought.

Source: Federal Reserve Bank of Boston.

Note: Survey respondents were asked to rate each of the characteristics on an absolute scale of 1 to 5 for each payment instrument, where 1 was the least desirable (least secure) and 5 was the most desirable (most secure).

Table A.1: Security questions in the 2013 SCPC and supplementary survey.

Appendix B. Detailed Security Assessments, Supplementary SCPC

	Secure or very secure	Risky or very risky
Personally identifiable information		
Cash		
Group 1	72.0	16.6
Group 2	71.1	14.4
Credit card		
Group 1	34.9	42.6
Group 2	23.7*	49.5*
Debit card		
Group 1	37.1	39.7
Group 2	22.9**	49.0**
Wealth		
Cash		
Group 1	32.5	55.5
Group 2	30.9	56.7
Credit card		
Group 1	47.0	33.2
Group 2	50.0	31.2
Debit card		
Group 1	35.4	42.3
Group 2	39.6	36.5
Confidentiality		
Cash		
Group 1	64.0	20.6
Group 2	73.2	13.4
Credit card		
Group 1	32.9	45.3
Group 2	27.1	54.2
Debit card		
Group 1	33.8	42.5
Group 2	26.8	50.5

Source: 2013 SCPC Supplementary Survey, November 6, 2013–March 10, 2014, Federal Reserve Bank of Boston.
Note: Group 1 completed the supplementary SCPC between November 6, 2013 and December 18, 2013. Group 2 completed the supplementary SCPC between December 19, 2013, and March 10, 2014. **Difference is statistically significant at the 5% level. *Difference is statistically significant at the 10% level.

Table B.1 Percentage of respondents choosing each rating.

Appendix C. Relative Characteristics Ratings

The 2013 SCPC survey asked respondents to rate each payment method according to the following characteristics: cost, setup, security, record keeping, acceptance, and convenience. Respondents assessed the characteristics on an absolute scale of 1 to 5 for each payment instrument, where 1 was the least desirable and 5 the most desirable. We computed the average of each respondent's perceptions of each payment method relative to all the other methods. Following Schuh and Stavins (2010), we apply the following transformation:

$$RCHAR_{ik}(j,j') = \log\left(\frac{CHAR_{ikj}}{CHAR_{ikj'}}\right)$$

where k indexes the characteristics (k = cost, setup, security, record keeping, acceptance, and convenience), i indexes the consumer, j represents the payment instrument in question and j' represents every other payment instrument besides j. We construct the average relative characteristic for each payment characteristic k:

$$\overline{RCHAR}_{ik}(j) = \frac{1}{\tilde{J}_i}\sum_{j'\neq j} RCHAR_{ik}(j,j')$$

over all $\tilde{J}_i$ payment instruments for consumer i. Another way of saying this is that for each respondent and for each payment method separately, we average across that respondent's ratings of that payment method relative to each of the other payment methods. For example, $\overline{RCHAR}_{ik}(j)$ for k = cost and j = debit card is the average of the log ratios of debit card cost to the cost of each of the other payment instruments for consumer i. A high value of the variable would indicate that the consumer considers debit cards to be relatively less costly than any of the other payment methods. Note that we construct the characteristics relative to *all* payments, regardless of whether the consumer has adopted them.

Although transforming the rating variables this way collapses some of the information by definition, it creates new variables that are more informative than the numerical ratings provided in the survey. This is so because a rating of 4 for the cost of debit cards, for example, cannot be easily interpreted, but a high rating relative to the ratings given to the other payment

methods reveals whether the consumer considers debit cards to be relatively more or less costly than other payment methods.

Appendix D. Specifications of Security Ratings Regressions

1. Specification of Relative Security Rating Regression

We estimate respondent *i*'s perception of security type *k* for payment *j* in 2013 by using the following OLS specification:

$$\overline{RCHAR}_{jik} = \overline{RCHAR}_{k}(DEM_i, POSTTARGET_i)$$

where $\overline{RCHAR}$ is the average relative security measure described in Appendix C above, *j* = credit cards or debit cards, *k* = overall security or security of personally identifiable information. We estimate four regressions: two regressions for credit cards and two regressions for debit cards, one using the overall relative security (from the main SCPC 2013) and one using the relative security of personally identifiable information (from the SCPC supplement).

DEM_i is a set of variables representing the demographic and financial attributes of respondent *i*, including age, gender, race, education, marital status, nationality, income, employment, geographic region, financial responsibility, household size, home ownership, and bankruptcy history.

$POSTTARGET_i$ is a dummy variable indicating whether respondent *i* completed the supplement SCPC after the Target breach announcement:

$$POSTTARGET_i = \begin{cases} 1 & \text{if respondent } i \text{ completed supplement after announcement} \\ 0 & \text{otherwise} \end{cases}$$

2. Absolute Security Rating Regression Specification

We estimate respondent *i*'s perception of security type *k* for payment *j* in 2013 by using the following ordered probit specification:

$$CHAR_{jik} = CHAR_k(DEM_i, POSTTARGET_i),$$

where $CHAR$ is the absolute security measure, on a scale from 1 to 5, *j* = credit cards or debit cards, *k* = overall security or security of personally identifiable information. We estimate four regressions: two regressions for *j* = credit cards and two regressions for *j* = debit cards, one using the overall absolute security (from the main SCPC 2013) and one using the absolute security of personally identifiable information (from the SCPC supplement).

DEM_i is a set of variables representing the demographic and financial attributes of respondent *i*, including age, gender, race, education, marital status, nationality, income, employment, geographic region, financial responsibility, household size, home ownership, and bankruptcy history.

$POSTTARGET_i$ is a dummy variable indicating whether respondent *i* completed the supplement SCPC after the Target breach announcement:

$$POSTTARGET_i = \begin{cases} 1 & \text{if respondent } i \text{ completed supplement after announcement} \\ 0 & \text{otherwise} \end{cases}$$

Appendix E. OLS Regression Results

Explanatory Variables	Explanatory Variables	Estimated Coefficients	
Post Target	Post-Target	-0.0203	
Age	< 25	0.0033	
	25-34	0.0167	
	45-54	-0.1075	***
	55-64	-0.0663	**
	>= 65	-0.0490	
Gender	Female	-0.0159	
Race	Black	-0.0274	
	Asian	0.0260	
	Other	0.0785	**
Ethnicity	Latino	-0.0112	
Education	Less than High School	-0.0413	
	High School	0.0552	*
	Some College	0.0341	
	Post-graduate	0.0213	
Marital Status	Never Married	-0.0452	*
Nationality	Immigrant	-0.0526	
Income	< $25,000	0.0063	
	$25,000-$50,000	0.0290	
	$75,000-$100,000	0.0306	
	> $100,000	0.0497	
Employment	Retired	-0.0949	***
	Disabled	0.0790	*
	Unemployed	0.0029	
	Homemaker	-0.0026	
	Other	-0.0084	
Geographic Region	Mid-Atlantic	-0.0848	
	East North Central	-0.0868	
	West North Central	-0.0989	
	South Atlantic	-0.0807	
	East South Central	-0.0009	
	West South Central	-0.0682	
	Mountain	-0.0526	
	Pacific	-0.0767	
Bill Pay Financial Responsibility	None or almost none	-0.0330	
	Some	0.0339	
	Most	0.0328	
	All or almost all	0.0224	
Household Shopping Responsibility	None or almost none	-0.0622	
	Some	-0.0531	
	Most	-0.0050	
	All or almost all	-0.0226	
Household Size	Household size	0.0105	
Home Ownership	Owns home	-0.0392	*
Bankruptcy	Within last 12 months	-0.1544	
	Within last 7 years	0.0143	
	Observations	1882	

Table E1. Dependent variable: Relative ratings of overall security of debit card.

Source: 2013 SCPC and authors' calculations.
Note: All respondents answered before the Target breach was announced.

Explanatory Variables	Explanatory Variables	Estimated Coefficients	
Post-Target	Post-Target	-0.0711	*
Age	< 25	-0.0469	
	25-34	0.0501	
	45-54	-0.0189	
	55-64	-0.0083	
	>= 65	-0.0080	
Gender	Female	-0.0471	**
Race	Black	-0.0071	
	Asian	0.1343	**
	Other	-0.0110	
Ethnicity	Latino	-0.0586	*
Education	Less than High School	-0.1065	*
	High School	-0.0661	**
	Some College	-0.0692	***
	Post-graduate	0.0078	
Marital Status	Never Married	0.0340	
Nationality	Immigrant	-0.0591	
Income	< $25,000	-0.0697	**
	$25,000-$50,000	0.0014	
	$75,000-$100,000	0.0771	**
	> $100,000	0.0981	***
Employment	Retired	-0.0292	
	Disabled	0.0464	
	Unemployed	0.0338	
	Homemaker	0.1092	**
	Other	-0.0120	
Geographic Region	Mid-Atlantic	-0.0627	
	East North Central	-0.0365	
	West North Central	0.0000	
	South Atlantic	-0.0467	
	East South Central	-0.0427	
	West South Central	-0.0641	
	Mountain	-0.0387	
	Pacific	-0.0611	
Bill Pay Financial Responsibility	None or almost none	-0.0113	
	Some	-0.0363	
	Most	0.0235	
	All or almost all	0.0544	*
Household Shopping Responsibility	None or almost none	-0.0353	
	Some	0.0407	
	Most	-0.0028	
	All or almost all	-0.0268	
Household Size	Household size	0.0011	
Home Ownership	Owns home	0.0187	
Bankruptcy	Within last 12 months	-0.1030	
	Within last 7 years	0.0147	
	Observations	1883	

Table E2. Dependent variable: Relative ratings of overall security of credit card.

Source: 2013 SCPC and authors' calculations.
Note: All respondents answered before the Target breach was announced.

Explanatory Variables	Explanatory Variables	Estimated Coefficients	
Post-Target	Post-Target	-0.1129	***
Age	< 25	0.0436	
	25-34	0.0276	
	45-54	-0.0312	
	55-64	-0.0309	
	>= 65	-0.0478	
Gender	Female	-0.0056	
Race	Black	0.0274	
	Asian	-0.0232	
	Other	-0.0310	
Ethnicity	Latino	0.0052	
Education	Less than High School	-0.0264	
	High School	0.0244	
	Some College	0.0311	
	Post-graduate	0.0363	
Marital Status	Never Married	-0.0228	
Nationality	Immigrant	-0.0152	
Income	< $25,000	0.0581	**
	$25,000-$50,000	0.0464	*
	$75,000-$100,000	0.0555	*
	> $100,000	0.0240	
Employment	Retired	-0.0236	
	Disabled	-0.0307	
	Unemployed	-0.0006	
	Homemaker	-0.0607	
	Other	-0.0507	
Geographic Region	Mid-Atlantic	-0.0337	
	East North Central	-0.0681	
	West North Central	-0.0305	
	South Atlantic	-0.0550	
	East South Central	0.0229	
	West South Central	-0.0294	
	Mountain	-0.0621	
	Pacific	-0.0337	
Bill Pay Financial Responsibility	None or almost none	0.0479	
	Some	0.0827	**
	Most	0.0178	
	All or almost all	0.0446	
Household Shopping Responsibility	None or almost none	-0.0183	
	Some	-0.0161	
	Most	-0.0178	
	All or almost all	-0.0221	
Household Size	Household size	-0.0012	
Home Ownership	Owns home	-0.0392	*
Bankruptcy	Within last 12 months	0.0052	
	Within last 7 years	0.0219	
	Observations	1870	

Table E3. Dependent variable: Relative ratings of security of personal information of debit card.

Source: 2013 SCPC and authors' calculations.
Note: Group 1 answered before the breach was announced; Group 2 (post-Target) answered after the breach was announced.

Explanatory Variables	Explanatory Variables	Estimated Coefficients	
Post-Target	Post-Target	-0.0421	
Age	< 25	-0.0282	
	25-34	-0.0078	
	45-54	-0.0457	*
	55-64	-0.0242	
	>= 65	-0.0678	*
Gender	Female	-0.0224	
Race	Black	-0.0061	
	Asian	0.0302	
	Other	0.0049	
Ethnicity	Latino	-0.0347	
Education	Less than High School	-0.0406	
	High School	0.0155	
	Some College	0.0142	
	Post-graduate	-0.0091	
Marital Status	Never Married	0.0207	
Nationality	Immigrant	0.0460	
Income	< $25,000	-0.0145	
	$25,000-$50,000	0.0325	
	$75,000-$100,000	0.0586	**
	> $100,000	0.0292	
Employment	Retired	0.0032	
	Disabled	-0.0143	
	Unemployed	-0.0153	
	Homemaker	0.0086	
	Other	0.0351	
Geographic Region	Mid-Atlantic	0.0087	
	East North Central	0.0050	
	West North Central	0.0612	
	South Atlantic	0.0443	
	East South Central	0.0440	
	West South Central	0.0035	
	Mountain	-0.0007	
	Pacific	0.0102	
Bill Pay Financial Responsibility	None or almost none	0.0062	
	Some	0.0151	
	Most	0.0610	*
	All or almost all	0.0281	
Household Shopping Responsibility	None or almost none	-0.0101	
	Some	-0.0052	
	Most	0.0021	
	All or almost all	-0.0175	
Household Size	Household size	0.0001	
Home Ownership	Owns home	0.0160	
Bankruptcy	Within last 12 months	-0.0780	
	Within last 7 years	-0.0047	
	Observations	1872	

Table E4. Dependent variable: Relative ratings of security of personal information of credit card.

Source: 2013 SCPC Supplementary Survey and authors' calculations.
Note: Group 1 answered before the breach was announced; Group 2 (post-Target) answered after the breach was announced.

Appendix F. Robustness Checks

Our baseline specification (Appendix D) includes several demographic variables in order to control for any inherent differences between Group 1 and Group 2. However, very few coefficients on the demographic variables were significant in the regressions. In order to address concerns with overfitting due to a small number of consumers in Group 2 and a large number of variables, we ran various robustness checks using more parsimonious specifications to see whether our initial results still hold.

In particular, we applied the following alternative specifications by changing the set of variables included in DEM_i:

a) We included age as a continuous variable instead of age cohorts; we also dropped the U.S. regions, as none of the corresponding estimated coefficients were significant in our original specification.
b) In addition to the modifications described in the previous bullet point, we dropped household shopping responsibility, household size, and bankruptcy variables. None of those variables were significant in the original specification.
c) We further reduced the number of estimated parameters by dropping and/or combining categories. Specifically, for DEM_i we included only age, age squared, and the following indicators: female, white, Latino, being employed, receiving post-graduate education, and having household income greater than $100,000.

For each of the specifications described above, the estimated coefficient on the post-Target indicator remains very close to that in the original specification and remains significant at the 1 percent level in the regression of the relative ratings of security of personal information of debit cards. Moreover, the post-Target coefficient remains insignificant whenever the original estimated coefficient was insignificant. In the regression of the relative ratings of overall security of credit cards, specifications (a) and (b) led to estimated coefficients for the post-Target indicator that are no longer significant at the 10 percent level. However, the estimated coefficients did not change much.

Overall, the above robustness checks support our findings from our baseline specification described in Appendix D.