Public Policy
Discussion Papers

FEDERAL RESERVE BANK OF BOSTON

No. 13-9

Security of Retail Payments: The New Strategic Objective

Joanna Stavins

Abstract:
The Federal Reserve Financial Services Strategic Plan for 2012–2016 specifies five main policy goals for the next few years. The second of its goals is to "Maintain public confidence in the end-to-end safety and security of clearing and settlement systems." Indeed, in each annual Survey of Consumer Payment Choice (SCPC), respondents consistently rank security as the most important characteristic of payment methods. However, in regressions of consumer payment use, security is not as significant as other payment attributes, such as cost, convenience, or record keeping. We analyze that puzzle by looking closely at how consumers' assessments of payment method security relate to their actual payment behavior, including testing whether consumers are more likely to use payment methods they consider more secure. Econometric results show that concerns about security create an obstacle to the adoption of some of the bank account-based payments—debit cards, online banking bill pay, and bank account number payments—but once adopted, there is no significant effect of security rating on the use of those payment instruments. The reverse is found for more established payment methods—cash, checks, and credit cards: consumers' perception of security does not influence adoption, but it does affect their actual payment use. Policy simulation results show that security improvements applied to individual payment instruments would increase the adoption of some payments, but once those payment instruments were adopted, security improvements would have only a small effect on the use of those payments.

JEL Classifications: D14, D12, G28

Joanna Stavins is a senior economist and policy advisor and a member of the Consumer Payments Research Center in the research department at the Federal Reserve Bank of Boston. Her email address is joanna.stavins@bos.frb.org.

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/ppdp/index.htm.

Claire Greene and Scott Schuh provided helpful comments. Vikram Jambulapati and Sean Connolly provided excellent research assistance.

This version: November 4, 2013

CPRC CONSUMER PAYMENTS Research Center

The Federal Reserve Financial Services Strategic Plan for 2012–2016 specifies five main strategic goals for the financial services policy for the next few years.The second of these goals is to "Maintain public confidence in the end-to-end safety and security of clearing and settlement systems."[1] Indeed, in each annual Federal Reserve Bank of Boston's Survey of Consumer Payment Choice (SCPC),[2] consumers selected security as the most important characteristic of payments, dominating all other options, such as cost, speed, and convenience. Therefore, it seems that the strategic plan is consistent with the consumers' stated preferences. However, there is little information on how these stated preferences correspond to actual consumer payment behavior, which reveals consumers' actual preferences. Because the strategic plan might lead to spending real resources on enhancing the security of the nation's payment system, it is worth analyzing in greater detail what aspects of security consumers view as strengths or deficiencies, and to what extent the perceived security of payments affects consumers' actual behavior. This paper uses recent consumer survey data to address these issues.

Most consumers choose from an array of payment methods when conducting their transactions. While consumers likely know from their own experience how the various payment methods compare in terms of speed of transaction or convenience, they are less likely to understand how secure each of these methods is, unless they have been victims of fraud. For example: "most debit card users do not likely understand that when they choose between 'debit or credit,' they may be making a choice that can affect whether they can successfully enlist their bank's help in resolving a dispute with a merchant that arises after the purchase."[3]

Because consumers consider security the most important feature of payment methods, we expect consumers' perceptions of risk and security of payments to affect their payment choice. This paper analyzes the extent to which the judgments consumers make, as indicated in consumer survey responses, are reflected in their actual payment behavior. Limited literature

[1] https://4site.clev.frb.org/FSPC/docs/fspc/planning/2012/Strategic_Plan.pdf
[2] See http://www.bostonfed.org/economic/cprc/scpc/index.htm for information about the SCPC survey program. The survey has been conducted annually starting in 2008.
[3] Furletti and Smith (2005).

on the subject shows that perceptions of risk may influence how consumers pay: Arango and Taylor (2009) show that perceived risk affects the choice of payment method, and Cope, Rock and Schmeiser (2013) find that consumers who consider mobile banking unsafe are less likely to adopt it. Kahn and Liñares-Zegarra (2012) show that experiencing identity theft or knowing someone who has experienced it influences how consumers pay.

However, in previous regressions of payment adoption and use, the perceived security of a payment method was found to be less important than ease of use or cost. Using the 2008 SCPC data, Koulayev, et al. (2012) found that ease of use, cost, and control over timing are the most important determinants of use, with security explaining less variation in payment choice than any of those features. Schuh and Stavins (2010) and (2013) found similar results using two different cross-sections of the SCPC data. Ching and Hayashi (2010) included an explanatory variable indicating whether consumers believe that a payment method is safe and found the variable to be insignificant. There is little econometric evidence showing that security significantly affects consumer payment behavior. One reason could be that although consumers are concerned about security, security differences among payment methods are not large enough to affect payment behavior (Rysman 2010). It is therefore possible that even though respondents consider security important in a general sense, they do not base their payment decisions on how secure they consider a given payment method.

We compare consumers' responses regarding their perceived risk of payment methods and payment locations to the consumers' actual payment behavior. Econometric results show that concerns about security create an obstacle to the adoption of some of the bank account-based payments—debit cards, online banking bill pay, and bank account number payments—but once adopted, there is no significant effect of security rating on the use of those payment instruments. The reverse is found for more established payment methods—cash, checks and credit cards: consumers' perception of security does not influence adoption, but it affects their actual payment use. Policy simulation results show that security improvements would increase the adoption of some payment instruments, but once these payment methods are adopted, security improvements would have only a small effect on their use.

The rest of the paper is organized as follows. Section 1 motivates the new Federal Reserve strategic objective of security enhancement and shows its implications for consumer payments. Section 2 describes the SCPC data used in this study, focusing on how the survey measures consumers' assessment of security. Section 3 shows how consumers' perception of security of payments varies across demographic groups. Section 4 summarizes consumer assessment of security by transaction location—in person, by mail, over the phone, and online. Section 5 compares security assessment to actual payment behavior, with respect to both adoption and use of payments. Section 6 focuses on the differences between PIN and signature debit card transactions and presents some information on their relative risks, consumer perceptions of their security, and the relationship between those perceptions and actual consumer debit card use. Section 7 shows the model and the results of econometric regressions. Section 8 presents the results of a policy simulation where we simulate security improvements applied to one payment method at a time to assess how consumer payment behavior would change if such improvements were implemented. Section 9 focuses on the way respondents interpret security survey questions and Section 10 concludes.

1. Security as a Federal Reserve policy objective

The Federal Reserve has played a key role in the U.S. retail payments system since its inception, and has emphasized three overriding objectives for its role in U.S. payments policy: safety, efficiency, and accessibility. Although safety or security has always been one of the main objectives, the recent strategic plan emphasizes end-to-end safety and security, thereby including more explicitly the effect on end users, and not just the operational safety associated with the provision of payment services on the supply side. The following quote from the Strategic Plan shows its strong emphasis on safety and security:

> "The 2012–2016 Strategic Plan reflects continuity with the past along with a shift in emphasis for Federal Reserve's financial services. FRFS will continue its longstanding mission to foster the integrity, efficiency, and accessibility of U.S. payments as a major service provider supporting the interbank market. In this role, FRFS will act as service provider, balancing *faster-better-cheaper* services with an emphasis on safety and security

to maintain public confidence in the U.S. payments system, while achieving long-term cost recovery for each service over the next five years."[4]

The Strategic Plan does not specify whether its emphasis on safety and security was motivated by a particular study of security needs. However, a paper issued by the Federal Reserve Financial Services on September 10, 2013 states the following: "The Federal Reserve Banks conducted a gap and opportunity analysis of the payment environment to understand key areas where the payment system could be improved relative to the vision of safe and accessible but faster and more efficient payments on an end-to-end basis." One of the key gaps and opportunities identified in that study was the following: "Consumer fears about payment security sometimes inhibit adoption of electronic payments."[5] It therefore follows that the ultimate goal of this endeavor is to ensure that *consumers* view the payment system as safe and secure.

In the past, the Fed's involvement in payment policy focused on the payment methods where the Fed plays a direct operational role as a service provider, such as checks or ACH. However, more recently the Fed has been also involved in establishing policies for payment methods it does not provide, for example, regulating the interchange fees for debit cards.[6] Therefore the Fed's involvement in improving the payment security could include not only the payment methods where the Fed already has a direct operational role, but also other payment methods. Similarly, any new policy could include the established payment instruments such as credit and debit cards, or newer payment instruments, such as mobile payments, where the Fed has had no direct operational involvement but where security might be a concern.

There are arguments in favor of focusing on security enhancements for both established payments and emerging payments. For example, studies have shown that the EMV payment card standard widely adopted in Europe is more secure for authenticating credit and debit card

[4] https://4site.clev.frb.org/FSPC/docs/fspc/planning/2012/Strategic_Plan.pdf

[5] "Payment System Improvement - Public Consultation Paper," Federal Reserve Financial Services, September 10, 2013 (http://fedpaymentsimprovement.org/wp-content/uploads/2013/09/Payment_System_Improvement-Public_Consultation_Paper.pdf)

[6] http://www.federalreserve.gov/newsevents/press/bcreg/20110629a.htm

transactions than the magnetic stripe standard used in the United States.[7] For emerging payments, there is evidence that security concerns create a major obstacle to their adoption. For example, a consumer survey on mobile payments conducted by the Federal Reserve Board's Division of Consumer and Community Affairs (DCCA) found that among those consumers with mobile phones who do not currently use mobile payments, the main reason for not using the service is concern about security: "For mobile payments, concerns about the security of the technology were the primary reason given for not using services,"[8] and the percentage of the DCCA respondents who mentioned security as the major barrier to adoption actually increased from 2012 to 2013.

Although the Federal Reserve's new strategic plan recognizes the importance of security to end users, it does not identify whether and how future policy changes might affect specific payment methods. This study shows how consumers perceive the current security of payments and how changes in the perceived security resulting from the Fed's security improvements might affect the actual payment behavior of end users in the United States.

2. Data: How do we measure security assessment?

We use the data from the 2010 Survey of Consumer Payment Choice (SCPC) conducted by the Federal Reserve Bank of Boston. The 2010 SCPC is the third annual survey on payment behavior of U.S. consumers.[9] The data contain adoption rates, incidence of use, and number of payments by consumers for nine common payment instruments: cash, checks, money orders, travelers' checks, debit cards, credit cards, prepaid cards, online banking bill payments (OBBP), and bank

[7] EMV is a global standard for credit and debit payment cards based on chip card technology (see http://www.emvco.com/default.aspx). A recent European Central Bank study showed that the EMV standard has contributed to a decline in payment card fraud in Europe (http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf?98e67de22a8fd4c156a3ac2e336309d0). See also King (2012) and Ardizzi (2013) for information on fraud reduction due to transition from magnetic stripe payment cards to EMV chip cards.

[8] "Consumers and Mobile Financial Services 2013," March 2013 (http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf)

[9] Although the majority of the respondents participated in at least two, and often three consecutive annual surveys, the survey instrument changed somewhat each year, and so pooling the cross-sectional samples is not straightforward. Future research will apply the analysis to the pooled data.

account number payments (BANP).[10] Characteristics of payment instruments have been found to be important to consumers who decide whether to adopt and/or use these instruments (Schuh and Stavins 2010, 2013).

For each payment instrument, the SCPC asks respondents to rate that instrument's characteristics, such as cost, speed, and security, on a 5-point Likert scale from least desirable (for example, most risky, most costly) to most desirable (for example, safest, cheapest). The survey questions related to the security of payments are included in the appendix. Although the numerical ratings assigned to the characteristics are consumers' subjective assessments, consumers make their decisions whether or not to adopt and/or use payment instruments based on their subjective assessments, even if such assessments do not align with objective data on the relative risks of each method. Because we are interested in measuring consumer behavior, these subjective assessments of the characteristics provide the appropriate measure of the relative security and risk of each payment method.

Note that the main security question asks respondents to "rate the **SECURITY** of each method against permanent financial loss or unwanted disclosure of personal information." This broad concept includes loss of money as well as loss of privacy. While both could occur if—for example—one's credit card or bank account was hacked, some payment instruments most susceptible to theft are also best at protecting one's privacy (for example, cash). If cash is stolen, it is likely to lead to "permanent financial loss," but extremely unlikely to lead to "unwanted disclosure of personal information." Therefore, depending on which meaning of security respondents focus on, their rating could vary. However, respondents are consistently picking security as the most important feature of payment instruments every year. Therefore, security clearly matters to consumers, although it is not obvious from the SCPC results what exactly they mean by the term security, as it is not clear whether a single measure could adequately accommodate all types of losses. We analyze the different interpretations of security in greater detail in Section 9.

[10] Online banking bill payment (OBBP) is an electronic payment made directly from a bank's online banking website. Bank account number payment (BANP) is a payment made by providing one's bank account number to a third party, such as an employer or a utility company. Paper check adoption is measured as either having blank checks or having written a check.

In addition to questions about security of the entire set of payment instruments under consideration, there are questions that relate specifically to debit cards. Respondents answered separate questions about security of various types of debit card payments: PIN, signature, in-person transactions where neither PIN nor signature is required, and online and telephone transactions, where neither PIN nor signature can be entered (also called card-not-present transactions). Although the no-PIN, no-signature debit cards are processed as signature payments, consumers do not view them as signature payments. Instead, consumers view these types of debit payments as much less secure than signature debit, with PIN debit payments considered most secure. We look more closely at the consumers who consider PIN "very secure" and at what payment methods they tend to use. The survey also contains a rich set of consumer demographic and financial attributes, including age, education, gender, race, ethnicity, household income, and net worth.

Because the SCPC has been conducted annually, we looked more closely at panelists to analyze the extent to which respondents have changed their assessment of security over the years. Table 1 shows how consumers rated the security of credit cards for each consecutive two-year period when the SCPC survey was conducted. The table includes only those consumers who responded to the survey in at least two consecutive years. The numbers represent the percentage of consumers for each pair of credit cards' security rating (for example, 5.92 percent of the 2009–2010 sample rated security of credit cards as 3 in year 2009 and as 4 in year 2010). We found that although many respondents stayed with the same security rating from one year to the next, the majority changed their ratings from year to year. For example, a respondent who rated the security of credit cards at 4 is somewhat more likely to pick 4 the following year, but Spearman rank pairwise correlation coefficients among years (shown in the bottom table) are all around 0.3, that is, much lower than 1, which would indicate a perfect correlation of ratings over time.

3. Demographics and importance of security

Respondents were asked to rank the importance of the six payment characteristics that were included in the survey, from the most important (first) to the least important (sixth). Figure 1 shows the percentage of respondents rating each characteristic as the first or second most important. Security was ranked as the most important or the second-most important characteristic by over 70 percent of respondents. However, the ranking varied across the sample. To test which demographic and financial attributes affect consumers' perceived importance of security, we estimated an ordered probit regression, where the dependent variable is each respondent's rating of the importance of security: most important, second most important, … , fifth most important, least important. The results are shown in Table 2. As the results show, older consumers are significantly more likely to consider security as the most important characteristic than younger consumers, while males and higher-income (and to a lesser extent higher net worth) consumers are significantly less likely to view security as an important characteristic of payments. However, the demographic attributes explain only a very small share of the variation in ranking.

To further analyze how consumers' rating of payment security (from very risky to very secure) varies with their demographic attributes, we estimated ordered probit regressions of security rating for each payment instrument as a function of consumers' demographic and income attributes. We estimated the following equation:

$$SEC_{ij} = S(AGE_i, EDU_i, GEN_i, MAR_i, RACE_i, INC_i),$$

where SEC_{ij} is consumer *i*'s rating of the security of payment *j*, and takes on a value from 1 (very risky) to 5 (very secure). SEC_{ij} is regressed on a set of dummy variables indicating consumer *i*'s age range, education level, gender, marital status, race, household income, and household net worth.

Table 3 shows the estimated coefficients from the set of ordered probit regressions. **Gender** has a strong effect on the perception of security: Men consider almost all payment

methods except cash more secure than women do. Above we showed that men also view security as less important than do women, possibly because they consider the payment methods to be secure, and therefore do not perceive lack of security to be a problem.

Age (all relative to those age 35–44): Consumers over 65 years old consider checks, bank account number payments, and online banking bill payments to be more secure, 25 to 34 year olds consider debit and credit cards as significantly more secure.

Education (all relative to those with a college degree): those with the lowest level of education (less than high school) consider checks and online banking bill payments less secure, while those with a high school diploma view debit cards as more secure, but online banking bill payments less secure.

Income (all relative to annual household income of $50K–$75K): lowest income consumers (annual income below $25K) view online banking as less secure, while highest-income consumers (above $100K) view checks as significantly more secure and prepaid cards as less secure. Household net worth has no significant effect on the perceived security when controlling for income.

Marital status (relative to married): single individuals rate credit cards as more secure.

Looking at the way consumers rate the security of different payment methods on average (Figure 2), online banking bill pay got the highest average rating, although it is only slightly higher and weakly statistically significantly higher than the security rating for credit cards, the next highest rated payment method (the difference is significant at the 5 percent level). The average credit card and debit card ratings were not statistically significantly different from each other. Javelin (2011(a)) also found credit and debit cards to be very close in terms of security: in 2010 the incidence of credit card fraud was 1.5 percent and debit fraud 1.4 percent of the overall transaction value.[11]

We looked more closely at respondents who consider each payment instrument "very risky" and at those who consider each payment instrument "very secure." Even though the

[11] According to Javelin (2011(a)), the incidence of credit card fraud declined from 2009 to 2010, although not the dollar value of the losses.

average ratings do not vary much across payment methods (Figure 2), there is a substantial variation across the payment instruments in how many consumers perceive them as very risky or very secure (Figure 3). Respondents felt more strongly about the security of some instruments than others. For example, a relatively large fraction of respondents view cash at the extremes of "very risky" or "very secure." That could be caused by the variation in how consumers interpret security—as financial loss or as loss of privacy. Cash had the highest percentage of respondents who considered it very risky (37.3 percent, followed by bank account number payments (23.8 percent) and prepaid cards (21.1 percent). (All these differences in percentages are statistically significant.) Consumers felt more neutral about the security of checks or debit cards—very few people viewed checks or debit cards at the extremes of "very risky" or "very secure." Check and debit cards were least likely to be considered very risky, with 7.7 and 9.2 percent of respondents considering them very risky, respectively. Credit cards were designated as very risky by 11.8 percent of respondents, somewhat higher than the rate for debit cards.

One possible reason why a relatively large fraction of respondents consider cash either very risky or very secure is that some consumers may primarily fear financial losses (cash very risky), while others may primarily fear loss of privacy (cash very secure). However, since more-educated and higher-income consumers rate cash as very risky, while less- educated and lower-income consumers rate cash as very secure, other explanations seem more plausible. For example, higher-income people have more alternatives to cash than lower-income people do,[12] and thus their elasticity of substitution is higher. So, the disutility from losing money for a high-income consumer is not higher than for the low-income consumer, but rather it is easier for the high-income consumer to switch to an alternative to avoid potential financial losses. However, neither education nor income is statistically significant in a regression of cash security rating (Table 3), so these results are inconclusive.

[12] The data show that the adoption and use of credit cards and online payments are significantly lower for low-income consumers.

4. Security assessment by transaction location

Consumers may rate security of transactions differently depending on the type of interaction with the merchant, rather than on the payment method used. For example, a consumer may view placing an order over the phone as risky not because he used a credit card to conduct the transaction, but because he had to give out personal information—credit card number—over the phone. To measure the effect of transaction location on security ratings, the SCPC asked respondents to rate security by location: in person, online, by mail, by mobile payments, and by phone.

Figure 4 illustrates that consumers view in-person payments as more secure than payments made at any other location: 63 percent viewed in-person payments as "very secure," compared with 10.2 for online payments, 4.9 for payments made by mail or over the phone, and 2.8 for mobile payments. The order was exactly reversed for the fraction of respondents who considered each location as risky. In particular, 18 percent of respondents viewed mobile payments as very risky, compared with only 0.2 percent of respondents who considered in-person payments as very risky.

Ordered probit regressions of security rating by transaction location on demographic and income attributes (Table 4) show that younger people are much more comfortable with mobile payments than older people: older consumers perceive mobile transactions to be significantly less secure than younger consumers do. This finding is consistent with the results of an adoption of mobile banking regression, in which consumers in each consecutive age cohort were progressively less likely to adopt mobile banking (results available from the author). In contrast, older consumers view transactions conducted by mail as significantly more secure than younger consumers do. Age does not have a significant effect on the security rating of online payments. Instead, less-educated and lower-income respondents were significantly more likely to rate online payments as risky, while higher income individuals were significantly more likely to rate online transactions as secure. Lowest-educated consumers were significantly more likely to rate transactions conducted by phone as secure.

Mobile payments' security ratings in the SCPC are similar to Javelin's (2011(b)) security ratings of mobile banking: 5 percent of Javelin's 2010 survey respondents rated mobile banking as "very safe," while 25 percent rated it as "very unsafe."

5. Security assessment and payment behavior

Because consumers rate security as the most important feature of payments, we expect their payment behavior to reflect their perceptions of security, both by payment instrument and by location of payments. In this section, we compare the actual adoption and use of different payment instruments to consumers' security assessments. For some payment instruments, adoption does not seem to be correlated with the security rating. For example, within each subsample with equal credit card security rating (that is, those who rated credit cards as very risky, risky, etc.), about two-thirds of people adopted credit cards. However, as Table 5 shows, adoption of other payment instruments does seem to be correlated with security rating. For example, 66.6 percent of those who considered debit cards "very risky" adopted them, compared with 94.2 percent of those who considered them "very secure." A similar pattern is evident for checks and online bank bill payments, although the increase in the rate of adoption does not always rise monotonically.

Table 6 shows the shares of transactions among all consumers, again for the whole sample and by security rating. For every payment method, consumers who consider it secure or very secure use that method more intensively than those who consider it risky or very risky. This correlation between security rating and payment use does not imply causality, but almost all the differences in mean shares are statistically significant at the 1 percent level.

Location of transactions also matters to consumers, regardless of the payment method used. As Table 7 shows, respondents who rated online transactions as very secure paid a significantly higher share of their bills online (12.4 percent), compared to respondents who rated online transactions as very risky (6.8 percent). In Section 7 below we test whether a security rating significantly affects payment adoption or use when controlling for various demographic and financial variables.

6. Debit cards: Security and use

a. PIN vs. signature

When a consumer swipes his debit card at checkout, he is often asked: "Debit or credit?" The question refers to the distinction between PIN and signature debit card authorization:[13]

PIN: PIN transactions are routed through an electronic funds transfer (EFT) network (e.g., Star, NYCE, Pulse). At the point of sale, a consumer swipes his card and chooses "debit" if asked. He then enters his PIN, which authorizes the transaction and immediately deducts the funds from his checking account. The merchant generally receives the money within days. Sometimes this is referred to as an "online" transaction, because the transactions require an electronic authorization.

Signature: Signature-based transactions are authorized and settled through the same Visa or MasterCard networks used for credit card transactions. At the point of sale, a consumer chooses "credit" if asked. He then signs a receipt (unless the merchant has waived the signature requirement or the card is not present), and the funds are deducted from his checking account, generally within one day of the merchant processing the sale transaction through the Visa or MasterCard network. The merchant usually submits the sale transaction with the rest of his card transactions at the end of the day, and he receives the money within days of this settlement. Sometimes this is referred to as an "offline" transaction, because a PIN debit network does not play a role in processing the transaction.

The two types of debit card transactions differ in terms of expected losses due to fraud or theft. PIN debit transactions are considered more secure because the cardholder authenticates his card with the PIN, unless the PIN number is stolen. Signature debit transactions cannot be easily authenticated, especially because some merchants waive the signature requirement at the point of sale, and signature debit transactions are used whenever the card is not physically present (in online, mail, or phone transactions), when the likelihood of

[13] Based on "More about Debit Card Fees," http://www.themerchantsguide.com.

a fraudulent transaction is greater. In contrast, PIN debit is accepted only by merchants that have the designated devices to capture PINs. In 2011, PIN debit card fraud losses were estimated at $0.004 per transaction, while signature debit cards fraud losses were $0.031 per transaction. In percentage terms, signature point-of-sale fraud losses averaged 0.08 percent, while PIN point-of-sale fraud losses averaged 0.01 percent.[14] For more details on potential fraud issues related to debit cards, see Sullivan (2010) and Hayashi and Sullivan (2013).

The losses to financial institutions do not imply that consumers suffer the same losses: under Regulation E,[15] a cardholder is liable for no more than $50 per PIN debit transaction if he reports the fraudulent purchase within a specified period of time. For transactions conducted online or by phone, if card issuers do not provide a way for merchants to identify a consumer, consumers do not face any liability under Regulation E.[16] Banks may also provide additional protection to their customers. For example, banks may extend the period of time when consumers are allowed to report erroneous transactions beyond what is specified in Regulation E. For signature debit, Regulation Z limits the consumer liability to $50, and Visa and MasterCard offer the same protection against unauthorized transactions as they do against fraudulent credit card transactions—zero liability for fraudulent transactions.[17] Some banks have been reported to offer the same zero liability to their customers for fraudulent PIN debit transactions. In summary, even though signature debit cards carry higher fraud losses than PIN debit cards, consumers are well protected against incurring those losses by the existing laws and rules.

b. Debit security ratings: PIN vs. signature

In addition to questions about security rating of debit cards in general, the 2010 SCPC also included a breakdown into types of debit card transactions: PIN debit, signature debit, no-PIN/no-signature debit, and debit transactions online. Figure 5 shows the differences in security rating among the different types of debit card transactions. Consumers' assessments are consistent with the evidence that PIN debit is more secure than signature debit: 63.8 percent of

[14] 2012 Pulse Debit Issuer Study (www.pulsenetwork.com).
[15] 12 *C.F.R.* (Code of Federal Regulations) § 205 (2004).
[16] For more details about consumer protections under PIN and signature debit, see Furletti and Smith (2005).
[17] http://usa.visa.com/personal/security/visa_security_program/zero_liability.html and http://www.mastercard.us/zero-liability.html.

respondents consider PIN debit secure or very secure, compared with 51.4 percent for signature debit. Over 41 percent of respondents considered no-PIN/no-signature debit transactions very risky, compared with 3.8 percent for signature debit and 5.3 percent for PIN debit, even though the no-PIN/no-signature transactions are processed the same way as signature debit transactions: Visa and MasterCard allow merchants to eliminate the signature requirement on purchases of less than $25,[18] and contactless cards that consumers can hold next to a reader without a swipe are also considered to be signature transactions. Interestingly, online debit transactions—which do not require PIN or signature—were rated more secure than the no-PIN, no-signature in person transactions: Only 20 percent of the respondents considered them very risky.

We compared respondents' rating of PIN and signature debit security to their preferred way of conducting debit transactions. Table 8 compares security ratings of PIN and signature debit to the stated preferred way. The top panel shows that consumers who consider PIN debit "secure" or "very secure" are at least twice as likely to prefer PIN debit as those who consider PIN as "risky" or "very risky." However, the corresponding results for signature debit (bottom panel) do not reveal a similar pattern: consumers who consider signature debit "very secure" were *less* likely to prefer signature debit than those who consider signature debit "secure" or "neither."

c. Actual debit payment behavior

Next, we test how a consumer's preferred type of debit is reflected in the way the consumer actually pays. The debit card use in the SCPC is not broken down into PIN and signature debit. However, the 2010 Diary of Consumer Payment Choice (DCPC)[19] collected debit card use information broken down by PIN and signature for a subset of the SCPC sample. It is important to keep in mind that consumers may not have a choice of which type of debit to use: while some merchants offer both types of debit and allow consumers to pick PIN or signature (often

[18] The no-PIN, no-signature debit transactions have the same consumer protections as the signature transactions: "Additionally, if a merchant participates in Visa's No Signature Required program, purchases under $25 may not require a signature *or* PIN and still receive Visa's suite of protections." (http://corporate.visa.com/_media/Visa-Debit-Card-Security-Fact-Sheet.pdf).

[19] The DCPC is a collaborative effort of the Federal Reserve Banks of Boston, Richmond, and San Francisco that complements and extends the Boston Fed's Survey of Consumer Payment Choice.

phrased as a question: "debit or credit?"), others may offer only one option. In addition, merchants often waive the signature requirement, resulting in no-PIN, no-signature transactions, even though those transactions are later processed the same way as signature transactions. Although the DCPC asks respondents whether merchants accepted the respondents' preferred payment methods, the responses are not detailed enough to allow us discern who tried to use PIN debit, but was forced to use signature debit instead because PIN debit was not accepted, or vice versa.[20]

We first compared respondents' preferences for PIN vs. signature debit to their actual use of the two types of debit, as reported in the DCPC. Table 9 shows the percentage of all debit transactions conducted with either PIN or signature debit, by the stated preferred type of debit. As the table shows, consumers' behavior is consistent with their stated preferences: Consumers who prefer PIN debit use PIN debit more than twice as often as signature debit (71.2 versus 28.8), and consumers who prefer signature debit use signature debit over three times as often as PIN (75.7 versus 24.3). Use is measured here as a share of the number of all debit transactions.

Next, we compared respondents' actual use of debit—total, PIN, and no PIN—to their assessment of security of debit cards in general. As Table 10 shows, those consumers who consider debit secure or very secure (bottom two rows) use debit cards more intensively than those who consider debit more risky. The pattern is apparent in the case of total debit, PIN, and no-PIN debit, although the difference in the PIN debit share between those who rated PIN debit "very secure" and the other groups is not statistically significant. Correlation between security rating and use may be affected by several factors and consumers may not have a choice as to what type of debit the merchant accepts. For many types of transactions, such as online or phone payments, no-PIN debit is the only option. In addition, consumers may not be aware that no-PIN debit transactions are processed the same way as signature debit, and so may be more skeptical about the security of such payments.

[20] Shy and Stavins (2013).

7. Adoption and use regressions

To test whether consumers' perceived security of each payment instrument significantly affects their payment decisions, we estimated Heckman two-stage regressions of adoption and use of payments, similar to Schuh and Stavins (2010, 2013). Consumers decide whether or not to adopt a payment method in stage 1, and—conditional on adoption—decide how intensively to use the payment method is stage 2.

a. Model

In our model, adoption of a payment method is a function of various characteristics of the payment method, as well as demographic and financial attributes of the consumer. The payment method characteristics are:

$$CHAR = \{SECURITY, ACCEPTANCE, COST, CONVENIENCE, RECORD\ KEEPING\}$$

Consumers assess each of these characteristics for each payment method on a Likert scale of 1–5. These numerical assessments are then used to construct average relative characteristics, as described below.

Adoption of payment method *j* by consumer *i* is modeled as:

$$\Pr(A_{ij} = 1) = A(\overline{RCHAR}ij, X_i, SETUP_{ij}) + \varepsilon_{ij}^{A}, \quad (1)$$

where

$$A_{ij} \equiv \begin{cases} 1 & \text{if consumer } i \text{ has adopted payment instrument } j \\ 0 & \text{otherwise.} \end{cases}$$

$\overline{RCHAR}_{ij}$ is a vector of average characteristics of payment *j* relative to the characteristics of all other payment instruments (created as described below), including the average relative security rating that consumer *i* assigns to payment instrument *j*; X_i is a vector of control variables for consumer *i* (demographic variables such as age, gender, race, education, marital status, income, and net worth). $SETUP_{ij}$ is consumer *i*'s assessment of the difficulty of getting and setting up

payment method *j* relative to the other payment methods. Unlike the other payment method characteristics, *SETUP* affects only adoption and not use.

Conditional on adoption of payment *j*, we model the use of each payment instrument *j* by consumer *i* as follows:

$$U_{ij} = U(\overline{RCHAR}ij, X_i, NUM_{0i}...NUM_{6i}, MR_i^{-1}) + \varepsilon_{ij}^{U}, \quad (2)$$

where $U_{ij} \equiv \left(n_{ij} / N_i\right)$ is the ratio of the number of payments consumer *i* made using payment *j* over the total number of payments made by consumer *i* in a month, and $N_i \equiv \sum_j n_{ij}$ is the total number of payments made by consumer *i* using all payment instruments *j*; $\overline{RCHAR}ij$ and X_i are defined as in equation (1); NUM_i is a set of dummy variables indicating how many other payment instruments consumer *i* has adopted;[21] and MR_i^{-1} is the inverse Mills Ratio from the first-stage Heckman probit model to control for simultaneity of the payment adoption and use decisions.

Characteristics are rated on a 1–5 scale. We are interested in consumers' rating of each payment instrument *j* relative to all the other payment instruments *j'*. Therefore, for each characteristic *k*, we use log relative characteristics as explanatory variables,

$$RCHAR_{ki}(j, j') \equiv \log\left(\frac{CHAR_{kij}}{CHAR_{kij'}}\right),$$

where *k* indexes the characteristics: security, acceptance, cost, convenience, setup, and record keeping; *i* indexes the consumer; and *j* is the payment instrument. In principle, all the relative characteristics could influence a consumer's choice of any payment instrument. However, to facilitate the interpretation of the marginal effects of the characteristics on use, we construct the average relative characteristic for each payment characteristic,

[21] Because we measure the use of each payment *j* as a share of payments made using *j*, and not as the absolute number of payments, the shares are (by design) affected by the number of payment instruments adopted by the consumer.

$$\overline{RCHAR}_{ki}(j) = \frac{1}{J}\sum_{j' \neq j}^{J} RCHAR_{ki}(j, j'),$$

where J = all the payment instruments. For example, $\overline{RCHAR}$ for cost in the check use equation is the average of the log ratios of check cost to the cost of each of the other payment instruments and it measures how a consumer evaluates the cost of checks relative to the cost of all the other payment methods. We expect the coefficients on all the average relative characteristics to be positive, because a higher numerical value of *CHAR* indicates a more positive assessment by a consumer, and we assume that consumers value all the characteristics.

b. Results: Adoption and use of payment instruments

The results of the Heckman regressions are in Table 11. Adoption (stage 1) results are in Panel A, while use (stage 2) results are in Panel B. The security rating is significant in the adoption of debit cards, online banking bill payments, and bank account number payments.[22] However, for each of those payment methods, the effect of every other characteristic on adoption is greater in magnitude than the effect of security (among the coefficients that are significant). Therefore, although consumers view security as the most important payment attribute, other features seem to influence their adoption decisions more heavily. However, the interpretation of the quantitative results is difficult here, because the numerical 1–5 ratings are not related to any objectively measureable factors. We can only discuss the relative importance of the various features on consumers' payment decisions.

Next we turn to the use results. Security significantly affects the use of cash, checks, and credit cards (all at the 5 percent level), but not debit cards, online banking bill payments, or bank account number payments. The results show that concerns about security create an obstacle to the adoption of some of the bank account-based payments, but once adopted, there is no significant effect of security rating on the use of those payment instruments. The reverse is found for more established payment methods: consumers' perception of security does not influence adoption, but it affects their actual payment use. As in the case of adoption, every

[22] Security is also weakly significant in the check adoption regression (at the 10 percent level), but the significance did not hold in other specifications.

other characteristic that significantly affects the use of those payment instruments has a stronger effect on use than security. To the extent that we can draw any conclusions based on the relative magnitude of these coefficients, it seems that even though consumers consistently pick security as the most important attribute of payment methods, and although security is significant in selected adoption and use regressions, consumers' decisions whether or not to adopt and use payments seem to be more strongly affected by other features of payment methods.

We test whether taking into account the relative importance of security changes our results. We might be underestimating the effect of security on payment adoption and use because we do not take into account how important security is to the consumers. In other words, consumers rate the security of each payment instrument the same way they rate other characteristics (on a 1–5 scale), but security is more important to them, and so we would expect those ratings to weigh more heavily in their decision making. To test that, we weight all the characteristic variables by their importance ranking to each respondent, so that the characteristic that is ranked as the most important to a consumer received the largest weight, while the least important one received the lowest weight.[23] As a result, a characteristic that is considered very important by a consumer—such as security—is weighted more heavily in the regressions than a characteristic that is considered less important.

Although the magnitude of the estimated characteristics coefficients increased when we weighted the characteristics based on their relative importance, the effect of security remained lower than the effect of the other characteristics, and the statistical significance level was not affected. So even when the relative importance of security is incorporated into the regression, security significantly affects selected consumer payment decisions, but the estimated effects of security on payment method adoption and use are not as high as the estimated effects of the other characteristics.

[23] Respondents were asked to rank the importance of each payment characteristic from "least important" (1) to "most important" (6). To account for the differences in ranking across consumers, weights were constructed at the respondent level as the characteristic *k's* rating over the sum of all characteristics ratings for respondent *i*: $\omega_{ki} / \sum \omega_{ki}$ where *k* is acceptance, setup, cost, convenience, record keeping, or security. For example, if security was most important, and each characteristic was rated differently, security's weight would be 6/(1+2+3=4+5+6) = 6/21. The weights were constructed to add up to 1 for each consumer. The SCPC allows respondents to rank payment characteristics equally, so equally important characteristics received equal weights.

The effect of security on payment adoption and use is similar to that found in Schuh and Stavins (2013), which used the 2008 SCPC survey data. In that study, security was found to significantly affect the adoption of online banking bill payments and bank account number payments, and to affect the use of cash, checks, debit cards, and prepaid cards (surprisingly, the effect on the use of online banking bill payments was negative).

c. Results: Payments by location and type

To isolate the effects of security rating on payment method choice from the effect of security on transaction location, we estimated payment use at each location separately: the point of sale transactions only, online purchases only (nonbill), and online bill payments only. In each case, the adoption-stage regression remains the same. By limiting the sample this way, we minimized the effect of location to isolate it from the effect of payment method adoption and use. We assume here that a consumer first selects a payment location (in person or online), and then chooses a payment instrument. An alternative model might allow the selection of the payment instrument to be independent of the location choice.

To test whether consumers' perceived security of payment *location* significantly affects their payment use, we included the perceived security of point-of-sale transactions in the point-of-sale use regression, and the perceived security of online transactions in the online purchase and online bill use regressions.

The use results for the point of sale (Table 12, Panel A) are similar to those for the whole sample, but at a lower level of significance: security rating affects cash use at the point of sale, but only at the 10 percent level. Even for cash, other characteristics—cost, convenience, and record keeping—have a more significant effect on payment use, and the coefficients on those terms are greater in magnitude. The results for online nonbill transactions, that is, purchases made online (Table 12, Panel B) show that those who rated credit cards as more secure had a higher share of online credit card transactions. However, the effect of debit card security rating has a negative effect on online debit purchases. Security rating does not significantly affect payment use for online bill transactions (Table 12, Panel C). The perceived security of point of

sale transactions is positive and significant in the use of cash at the point of sale, and the perceived security of online transactions is significant in the use of BANP for online purchases.

8. Policy simulation: Effects of security improvement on consumer payment behavior

As mentioned, payments security is one of the main strategic goals for the Federal Reserve for the next few years. Although it is not yet clear how this goal will translate into action, we assess the effects of potential Federal Reserve policy intervention resulting in enhanced security of payments. We assume that an intervention would improve security of a single payment method, for example credit cards, and would result in higher perceived security of that payment method for consumers. To assess the effect of such a policy, we simulate security improvements applied to one payment method at a time, while leaving the security of the remaining payment methods unchanged. We are interested in answering the following question: *how would consumer payment behavior change if security of payments improved?*

We use our estimated model of adoption and use to assess consumer response to an improvement in the security of various payment instruments (one at a time): debit cards, credit cards, online banking bill payments, and bank account number payments. We selected these four payment instruments because we expect that security enhancements might involve either improved safeguards for online banking (thereby affecting OBBP or BANP), or an introduction of EMV (thereby affecting debit cards or credit cards). Although cash and checks could also become more secure, we assumed that it is less likely that the Federal Reserve would focus on those payment instruments.

The experiments let us estimate the effect on own adoption and use, as well as the effect on the adoption and use of all the other payment methods resulting from an improvement in security. These simulations assume that consumers would be aware of and value any improvements in payment security that the Federal Reserve might implement. It is possible that even a substantial investment by the Federal Reserve in security enhancements might not be noticed by consumers, and would therefore not result in any change in these subjective ratings.

To calculate a predicted change in the adoption and shares, we simulate an increase in each consumer's assessment of security for a particular payment method:

$$CHAR'_{SEC,ij} = \begin{cases} CHAR_{SEC,ij} + 1 \text{ if } CHAR_{SEC,ij} \leq 4 \\ CHAR_{SEC,ij} \text{ if } CHAR_{SEC,ij} = 5 \end{cases},$$

where i indexes consumers and j indexes the payment instrument whose security rating has been changed, for j = debit cards, credit cards, online banking bill payments, and bank account number payments. We conduct each simulation separately, for one payment method j at a time, resulting in four separate experiments. For consumers who already rated a given payment method as "most secure" (the highest level, value of 5), we did not change their assessment. Recall that the average relative security rating for payment instrument j is a function of the security rating of all the other payment instruments j'. Therefore, in each experiment, we re-calculate the average security ratings relative to all the other payment methods and then apply the new ratings to the original fitted model for that payment instrument.

Table 13 shows the results of the policy simulation. The top panel shows predicted adoption (percentage of consumers who are predicted to adopt each payment method), while the bottom panel shows predicted shares. The first column in each panel shows the predicted values based on the original 2-stage Heckman model: the top panel is based on the first stage of the Heckman model (probit), and the bottom panel is based on the second stage of the Heckman model (OLS). Each subsequent column shows the results of a separate simulation, where we artificially increase the security rating for one payment instrument at a time—debit cards, credit cards, OBBP, and BANP—in turn.

Recall that in the adoption stage, security had a positive and significant effect on the adoption of debit cards, BANP and OBBP (Table 11, Panel A). Our simulation shows that increasing the perceived security of debit cards raises predicted debit card adoption from 80.05 percent to 82.61 percent. When increasing the perceived security of credit cards, we see that the predicted credit card adoption actually drops slightly, because the coefficient on security was negative, but not significant. When increasing the perceived security of BANP, the predicted

adoption of BANP increases from 70.47 percent to 72.26 percent. When increasing the perceived security of OBBP, the predicted adoption of OBBP rises from 53.24 percent to 55.23 percent. Thus the simulated effect of an increase in perceived security on that payment instrument's own predicted adoption is small, but statistically and economically significant. The simulated effects of an increase in perceived security of a payment instrument on the adoption rates of other payment instruments are all below 1 percentage point.

We test the significance of each change in predicted adoption and use by applying paired *t*-test, that is, we calculate the difference in predicted adoption and use for the same consumer before and after each simulation, and then take the mean of these differences. Note that applying a paired *t*-test is much more likely to lead to rejecting the hypothesis that the predicted behavior before and after simulation is the same (the statistics are equal) than testing whether the predicted means are equal. Thus, even though the means of the predicted adoption rates across the entire sample do not change much under the simulated experiments, all the changes are statistically significant for every experiment. Despite the statistical significance, the predicted changes in the adoption rates of other payment instruments are very small and therefore not economically significant.

In the use stage, security had a positive and significant effect only on the share of cash, check and credit (Table 11, Panel B), and the three coefficients were very small. Only one of these payment methods—credit cards—are included as one of our simulated security improvements. It is therefore not surprising that almost all of the changes in predicted shares are below 1 and several of them are close to 0. In the case of credit cards, the predicted share increases by 0.78 percentage points as a result of the simulated security enhancement to credit cards. As was the case with the changes in the adoption rates above, all the changes in predicted use shares are statistically significant for every experiment. However, most of the aggregate predicted changes are very small and therefore not economically significant.

Our policy simulation predicts that an improvement in security that might result in shifting consumers' perception from "very risky" to "risky" or from "secure" to "very secure" would increase the adoption of some payment instruments, but once adopted, would have only a small effect on the use of those payments. Debit cards are one of the payment methods whose

adoption would be positively affected by improved security, implying that the incentive to financial institutions to implement fraud reduction policies included in the Federal Reserve Board rules in response to the Durbin Amendment was warranted.[24] Other payment methods included in our simulated policy experiment involve online payments (OBBP and BANP), suggesting that addressing technology risk as part of the security enhancements might help consumers overcome their barriers to adopting those payment methods. More detailed data on what types of risk consumers are concerned with would help pinpoint where the resources might best be spent.

9. How do consumers interpret security?

As we discussed above, respondents' interpretation of security is likely to vary. In particular, concerns about security may mean fear of a financial loss or fear of loss of personal information or privacy. Consumers' payment behavior will likely vary depending on their interpretation. Cash ratings provide one way to identify the two interpretations: Respondents whose security concerns focus on the risk of financial loss can be expected to rate cash as "very risky," while those who are mostly concerned about loss of privacy can be expected to rate cash as "very secure." This is because lost or stolen cash almost always leads to financial loss, but not to loss of privacy or of personal information.

We analyzed the effect of security rating on payment behavior by those who rated cash as "very secure" and those who rated cash as "very risky." For those who are concerned about financial loss (cash rated very risky), higher security rating increased their probability of adopting bank account number payments, while for those who are concerned about loss of privacy (cash rated very secure), high security rating lowered their probability of adopting bank account number payments.

In addition, personal experiences may be expected to affect consumers' assessment of payment method security. Consumers who experienced a theft of a payment method might

[24] The rule included an incentive to debit card issuers to implement fraud-prevention policies: "rule that allows for an upward adjustment of no more than 1 cent to an issuer's debit card interchange fee if the issuer develops and implements policies and procedures reasonably designed to achieve the fraud-prevention standards set out in the interim final rule." (http://www.federalreserve.gov/newsevents/press/bcreg/20110629a.htm)

assess that method as less secure than those who did not have such experiences. However, security ratings by those who had experienced a theft of a payment method were not significantly lower than security ratings by those who lacked such personal experiences (results available from the author). Unfortunately not all respondents answered the question about their experiences, preventing us from including the variable in the regressions.

Finally, we address the statement in Rysman (2010) that the reason there is almost no regression evidence on issues of security is that consumers perceive all payment methods as equally secure. We test whether the standard deviation of security ratings is lower than the standard deviation of the ratings for other characteristics. We find evidence that that is indeed the case: the standard deviation of consumers' ratings of security is 1.288, while the standard deviation of consumers' ratings of the other characteristics ranges from 1.532 to 1.687. Moreover, the standard deviation of consumers' ratings *within* each payment method (for example, check only, or credit card only) is *higher* for security than for other characteristics. This indicates that consumers rate the security of all payment instruments similarly, and thus the variation in security ratings arises from differences across individuals, and not from differences in ratings across payment methods.

We therefore find that even though consumers consider security to be the most important feature of payments, they perceive differences in security among payment instruments to be relatively small. Consumers base their payment decisions on the other characteristics as much as or even more than on the perceived security of the various payment methods.

10. Conclusions

Security is one of the five main strategic goals in *The Federal Reserve Financial Services Strategic Plan for 2012–2016*. Consumers consistently pick security as the most important attribute of payment methods in each annual Survey of Consumer Payment Choice, but their decisions whether or not to adopt and use payments are only modestly affected by their perception of the

security of each payment method, because they perceive differences in security across payment methods to be relatively small.

Security can be interpreted differently by different people. Respondents who are more concerned about their financial loss (those who view cash as risky) are more likely to adopt bank account number payments, while those who are more concerned about loss of their personal information (those who view cash as secure) are less likely to adopt bank account number payments.

Our policy simulation shows how security enhancements affecting individual payment instruments might change the way consumers pay. However, any effect of policy change will depend on where the resources are spent. For example, technology improvements affecting online payments are likely to have a different effect from a policy targeting more secure payment card standards. In order to decide how the resources should be spent, more information is needed on what exactly consumers are concerned about when it comes to the security of payments.

References

Arango, Carlos and Varya Taylor. 2009. "The Role of Convenience and Risk in Consumers' Means of Payment." Bank of Canada Discussion Paper No. 2009-8.

Ardizzi, Guerino. 2013. "The Impact of Microchip on Payment Card Frauds," mimeo, presented at the European Central Bank and the Banque de France joint conference on "Retail payments at a crossroads: Economics, Strategies and Future Policies," October.

Ching, Andrew and Fumiko Hayashi. 2010. "Payment Card Rewards Programs and Consumer Payment Choice," *Journal of Banking and Finance* 34: 1773–1787.

Cope, Alice M., Alexandra M. Rock, and Maximilian D. Schmeiser. 2013. "Risk Perception, Risk Tolerance and Consumer Adoption of Mobile Banking Services." mimeo.

Furletti, Mark and Stephen Smith. 2005. "The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Credit and Debit Cards." Federal Reserve Bank of Philadelphia Discussion Paper, January.

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

Hayashi, Fumiko and Richard J. Sullivan. 2013. *Fees, Fraud and Regulation: Forces of Change in the Payment Card Industry*, Federal Reserve Bank of Kansas City Payments System Research Briefing, April.

Javelin Strategy Research. 2011(a). "2011 Identity Fraud Survey Report." www.javelinstrategy.com

_____. 2011(b). "2011 Mobile Banking Financial Institution Scorecard." www.javelinstrategy.com

Kahn, Charles M. and José M. Liñares-Zegarra. 2012. "Identity Theft and Consumer Payment Choice: Does Security Really Matter?" mimeo.

King, Douglas. 2012. "Chip-and-PIN: Success and Challenges in Reducing Fraud." Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, January.

Koulayev, Sergei, Marc Rysman, Scott Schuh, and Joanna Stavins. 2012. "Explaining Adoption and Use of Payment Instruments by U.S. Consumers." Federal Reserve Bank of Boston Working Paper No. 12-14.

Rysman, Marc. 2010. "Consumer Payment Choice: Measurement Topics," in *The Changing Retail Payments Landscape: What Role For Central Banks?* Federal Reserve Bank of Kansas City conference proceedings, pp. 61–81.

Schuh, Scott and Joanna Stavins. 2010. "Why Are (Some) Consumers (Finally) Writing Fewer Checks? The Role of Payment Characteristics." *Journal of Banking and Finance* 34: 1745–1758, August.

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

Shy, Oz and Joanna Stavins. 2013. "Measuring Merchant Steering of Consumer Payment Choice: Lessons Learned From Consumer Surveys." Federal Reserve Bank of Boston Research Report No. 13-1.

Sidel, Robin. 2007. "As Card Fees Climb, Merchants Push PINs." *The Wall Street Journal*, January 16.

Sullivan, Richard J. 2010. "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options." Federal Reserve Bank of Kansas City Economic Review, Second Quarter, pp. 101–133.

Table 1: Security Ratings of Credit Cards over Time (2008–2011)

	2009				
2008	1	2	3	4	5
1	4.77	4.19	0.93	3.02	1.28
2	3.95	9.77	4.19	7.09	1.40
3	1.40	3.95	3.60	4.53	1.28
4	2.56	8.72	5.23	14.07	3.37
5	0.47	2.21	0.81	4.30	2.91
n = 860					

	2010				
2009	1	2	3	4	5
1	3.59	5.12	1.64	3.43	1.06
2	3.65	10.30	4.65	9.24	1.58
3	1.22	2.85	3.49	5.92	1.27
4	2.06	5.44	5.23	13.95	4.44
5	0.58	1.22	1.00	3.33	3.75
n = 1,893					

	2011				
2010	1	2	3	4	5
1	2.76	4.28	1.30	2.65	0.62
2	2.76	8.56	3.94	7.49	1.69
3	1.30	4.00	4.11	6.36	0.79
4	2.42	6.93	6.08	15.65	4.56
5	0.28	1.46	0.84	5.12	4.05
n = 1,776					

Note: Respondents were asked to rate each payment instrument from “very risky” (1) to “very secure” (5). The numbers inside the table represent the percentage of respondents with a given rating. Read down for ratings in the earlier year and across the row for the corresponding rating in the later year. For example, among respondents who rated the security of credit cards as 4 in 2008, 14.07 percent rated it as 4 in 2009. The numbers within each table sum to 100.

Credit Card Security: Spearman Rank Pairwise Correlation

	2008	2009	2010	2011
2008	1			
2009	0.28	1		
2010	0.30	0.32	1	
2011	0.28	0.29	0.33	1

Sources: Survey of Consumer Payments 2008–2011.

Table 2: Ordered Probit Predicting Importance of Security

Age	
Under 25	-0.30 *
25 to 34	-0.13
45 to 54	0.16 **
55 to 64	0.32 ***
Over 65	0.39 ***
Education	
Less than high school	-0.24
High school diploma	0.10
Some college	0.18 ***
Graduate degree	-0.10
Gender	
Male	-0.17 ***
Marital status	
Separated	-0.15 *
Widowed	-0.02
Single	-0.10
Income	
Less than $25,000	-0.04
$25,000 to $49,999	-0.02
$75,000 to $99,999	-0.19 **
Greater than $100,000	-0.21 ***
Net Household Worth	
Less than $50,000	0.00
$50,000 to $99,999	-0.02
$250,000 to $500,000	-0.06
Greater than $500,000	-0.16 *
Race	
Black	0.19 *
Asian	0.23
Other	0.11
Ethnicity	
Latino	0.12
N	1,990
Pseudo *R* -squared	0.02

Source: 2010 Survey of Consumer Payment Choice (SCPC).

Note: Dependent variable is ranking of the importance of security from "Least Important" (1) to "Most Important" (6), compared with other payment characteristics.

Table 3: Ordered Probit (Absolute Security Rating, by Payment Instrument)

Variables	Cash	Check	Debit Card	Credit Card	Prepaid Card	OBBP	BANP
Age							
Under 25	0.002	0.021	-0.165	-0.164	-0.018	-0.220	-0.183
25 to 34	-0.050	0.095	0.210 **	0.195 **	0.026	0.026	0.066
45 to 54	-0.038	0.055	-0.009	0.020	0.018	0.011	0.000
55 to 64	-0.036	0.173 **	-0.063	0.007	-0.006	-0.038	-0.041
Over 65	-0.067	0.421 ***	-0.079	0.146	-0.137	0.157 *	0.204 **
Education							
Less than high school	-0.116	-0.342 *	-0.087	-0.270	-0.059	-0.451 **	-0.217
High school diploma	0.058	-0.011	0.162 **	-0.041	0.035	-0.164 **	0.025
Some college	0.042	-0.053	0.082	-0.092	-0.013	-0.039	0.028
Graduate degree	-0.045	-0.028	-0.005	0.108	0.029	-0.076	0.003
Gender							
Male	0.074	0.092 *	0.143 ***	0.217 ***	0.131 ***	0.136 ***	0.110 **
Marital status							
Separated	-0.092	0.018	0.038	0.021	0.023	0.058	0.047
Widowed	0.154	-0.069	0.069	-0.013	0.022	-0.068	0.093
Single	0.136	0.056	0.056	0.185 **	0.067	0.005	0.068
Income							
Less than $25,000	0.109	0.040	0.092	-0.072	-0.023	-0.213 **	0.022
$25,000 to $49,999	0.047	0.097	0.128 *	0.040	-0.073	-0.103	-0.063
$75,000 to $99,999	-0.057	0.120	0.098	0.120	-0.141 *	0.072	0.120
Greater than $100,000	-0.120	0.137 *	0.115	0.084	-0.134 *	0.113	0.076
Net Household Worth							
Less than $50,000	0.115	0.031	0.059	-0.063	-0.010	0.066	-0.027
$50,000 to $99,999	0.048	0.023	-0.028	0.038	0.020	0.032	-0.084
$250,000 to $500,000	0.042	-0.099	0.014	-0.172 *	-0.009	-0.039	-0.048
Greater than $500,000	0.031	0.044	-0.067	0.029	-0.038	0.047	-0.010
Race							
Black	-0.091	-0.071	0.058	-0.158	0.160 *	-0.004	0.142
Asian	0.092	0.141	0.028	-0.116	-0.168	-0.154	0.123
Other	-0.021	0.029	0.337 **	0.160	-0.003	0.082	0.338 **
Ethnicity							
Latino	0.048	-0.075	-0.012	0.006	0.028	0.072	-0.153
N	1983	1982	1981	1983	1981	1982	1982

Source: 2010 Survey of Consumer Payment Choice (SCPC).

Notes: Respondents were asked to rate each payment instrument from "very risky" (1) to "very secure" (5).

Table 4: Ordered Probit (Absolute Security Rating, by Location)

Variables	In Person	Online	By Mail	By Phone	Mobile
Age					
Under 25	0.010	-0.037	-0.304 *	0.075	0.101
25 to 34	0.256 **	0.036	-0.245 **	0.077	0.005
45 to 54	0.148 *	-0.056	0.093	-0.059	-0.243 ***
55 to 64	0.242 ***	-0.010	0.160 **	-0.053	-0.282 ***
Over 65	0.176 *	-0.021	0.206 **	-0.128	-0.318 ***
Education					
Less than high school	-0.289	-0.472 **	-0.172	0.313 *	0.279
High school diploma	0.158 *	-0.122	-0.074	-0.086	0.047
Some college	0.095	-0.041	-0.124 *	-0.154 **	0.016
Graduate degree	-0.004	0.019	0.045	0.051	0.022
Gender					
Male	0.068	0.029	0.016	-0.016	0.123 **
Marital status					
Separated	0.008	0.082	0.054	-0.060	0.075
Widowed	0.039	0.073	0.130	-0.116	0.173
Single	0.043	0.122	0.079	-0.043	-0.029
Income					
Less than $25,000	-0.016	-0.271 ***	0.039	-0.015	-0.141 *
$25,000 to $49,999	-0.009	-0.057	0.043	0.009	0.012
$75,000 to $99,999	-0.107	0.225 ***	0.099	0.033	0.085
Greater than $100,000	-0.172 **	0.216 ***	0.093	0.054	0.075
Net Household Worth					
Less than $50,000	-0.033	0.003	0.085	-0.050	-0.036
$50,000 to $99,999	0.140	0.057	0.002	-0.269 ***	-0.004
$250,000 to $500,000	-0.008	0.136	0.001	-0.099	-0.047
Greater than $500,000	-0.034	0.052	0.038	-0.017	0.087
Race					
Black	-0.106	-0.250 ***	-0.051	0.155	-0.012
Asian	-0.204	-0.013	-0.072	-0.337 *	-0.088
Other	-0.164	-0.059	-0.069	0.108	0.035
Ethnicity					
Latino	0.149	0.013	-0.303 **	-0.068	0.056
N	1990	1990	1990	1990	1989

Source: 2010 Survey of Consumer Payment Choice (SCPC).

Notes: Respondents were asked to rate each payment location from "very risky" (1) to "very secure" (5).

Table 5: Percentage of Respondents Who Adopted Each Payment Instrument (total and by security rating)

	Cash	Check	Debit Card	Credit Card	Prepaid Card	OBBP	BANP
Total	100.0	87.0	78.4	70.3	38.2	48.7	64.8
Security ratings							
Very risky	99.9	76.2	66.6	70.8	35.2	24.8	57.0
Risky	100.0	85.4	70.1	67.4	36.3	42.0	66.5
Neither risk nor secure	100.0	82.3	69.8	64.6	39.7	36.7	61.0
Secure	100.0	94.2	88.4	74.2	39.1	58.8	73.2
Very secure	100.0	92.0	94.2	71.8	41.5	71.5	67.8

N = 2,102

Source: 2010 Survey of Consumer Payment Choice (SCPC).

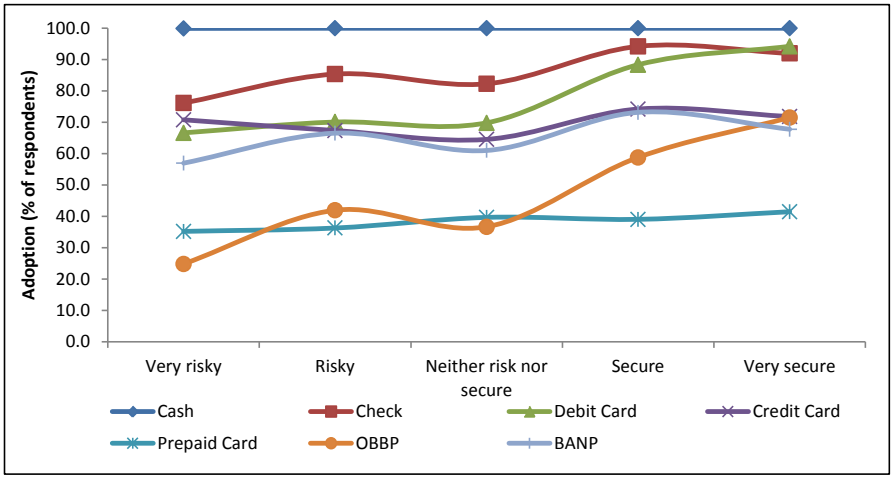


Table 6: Percentage Share of Transactions by Payment Instrument, All Consumers (total and by security rating)

	Total	Security ratings		
		Risky or very risky	Secure or very secure	Difference in Means
Cash	30.38	27.25	31.96	***
Check	11.80	10.50	14.68	***
Debit	27.33	24.42	32.75	***
Credit	16.70	12.46	19.68	***
Prepaid	1.22	1.17	1.93	**
Bank account number				
Overall	5.69	5.36	6.41	**
Bill payments	4.31	4.08	4.73	*
Online bill payments	2.23	2.15	2.50	
Online bank bill payment	4.84	3.50	6.52	***

N=2,102

Source: 2010 Survey of Consumer Payment Choice (SCPC).

Notes: sampling weights were used to correct for differences between the sample composition and the target population - U.S. noninstitutionalized population 18 years of age and older. The benchmark distributions against which the American Life Panel is weighted are derived from the Current Population Survey (CPS).

Significance level: * 0.10 ** 0.05 *** 0.01

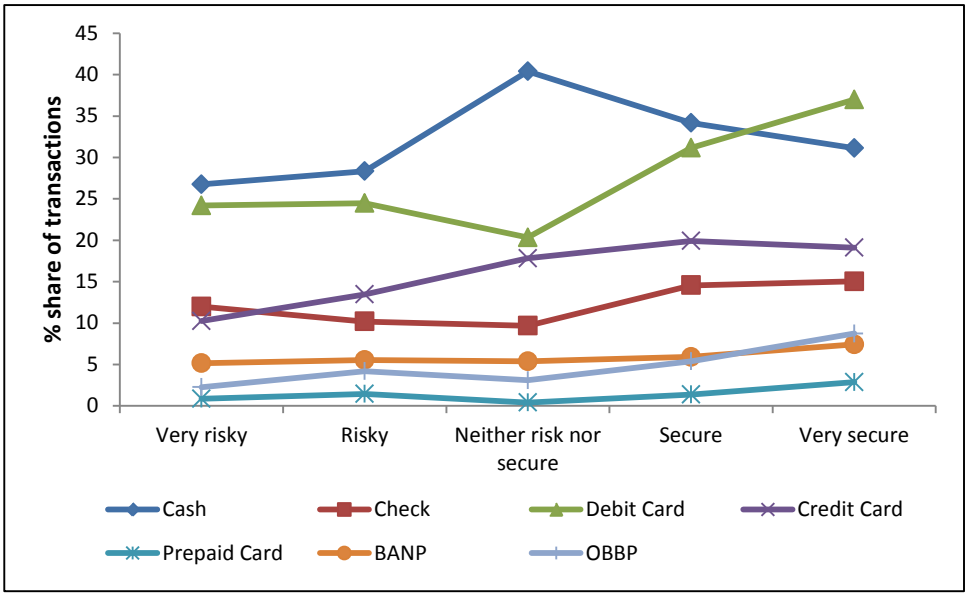


Table 7: Percentage Share of Transactions by Security Rating and Location (all consumers)

	In Person	Online Nonbills	Online Bill Payment
Total	57.8	5.1	8.7
Security ratings			
Very risky	38.8	5.2	6.8
Risky	52.7	4.1	7.5
Neither risk nor secure	55.3	4.7	7.5
Secure	58.6	5.7	9.3
Very secure	58.1	6.2	12.4
N = 2,102			

Source: 2010 Survey of Consumer Payment Choice (SCPC).

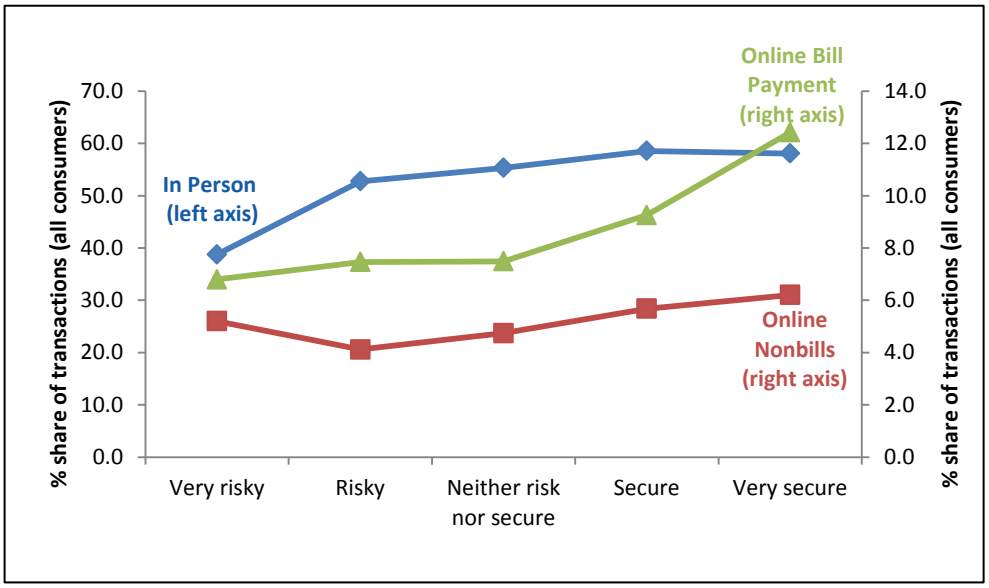


Table 8: Preferred Debit Authorization by Security Ratings (percent of respondents)

PIN debit security rating	% Prefer PIN debit
Very risky	22.0
Risky	27.2
Neither risk nor secure	24.5
Secure	52.8
Very secure	61.9
Signature debit security rating	**% Prefer Signature debit**
Very risky	21.3
Risky	25.9
Neither risk nor secure	32.2
Secure	33.6
Very secure	25.2
N = 1,236	

Source: 2010 Survey of Consumer Payment Choice (SCPC).
Note: Each cell shows the percentage of respondents who prefer a given type of debit, broken down by the corresponding security ratings for that type. For example, 27.2 percent of respondents who considered PIN debit "risky" selected "PIN debit" as their preferred way of conducting debit transactions.

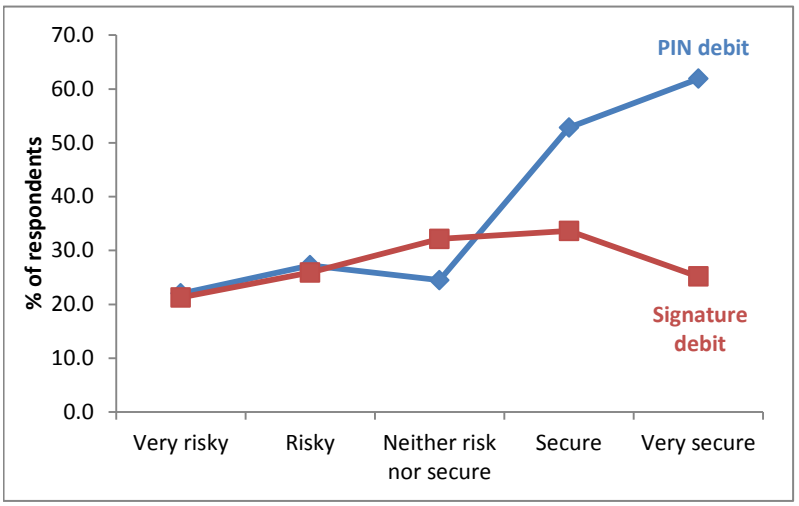


Table 9: Preferred Debit Mode by Percent Usage (all consumers)

	Shares from Diary of Consumer Payment Choice	
	PIN debit	Signature debit
Total	54.8	45.2
Preferred mode		
PIN debit	71.2	28.8
Signature debit	24.3	75.7
Either	67.1	32.9
Neither	0.0	100.0
N = 197		

Source: 2010 Survey of Consumer Payment Choice (SCPC), 2010 Diary of Consumer Payment Choice (DCPC).

Note: Each cell shows the share of debit transactions that are conducted using a given type of debit, broken down by the preferred way to conduct debit transactions. For example, for those consumers who prefer PIN debit, 71.2 percent of their debit card transactions were conducted using PIN debit.

Table 10: Percentage Share of Use by Debit Security Rating

	Shares from Diary of Consumer Payment Choice		
	PIN debit	No PIN debit	All debit
	(1)	(2)	(1+2)
Total	15.5	11.8	27.3
Debit security ratings			
Very risky	11.0	9.8	20.8
Risky	11.8	10.1	21.9
Neither risk nor secure	15.5	9.7	25.2
Secure	17.7	13.1	30.8
Very secure	21.2	15.6	36.8
N = 297			

Source: 2010 Survey of Consumer Payment Choice (SCPC) and 2010 Diary of Consumer Payment Choice (DCPC).
Note: Each cell shows the share of all transactions that were conducted using a given type of debit, broken down by the security ratings of debit in general. For example, among those consumers who considered debit "very secure," 36.8 percent of their transactions were conducted using debit.

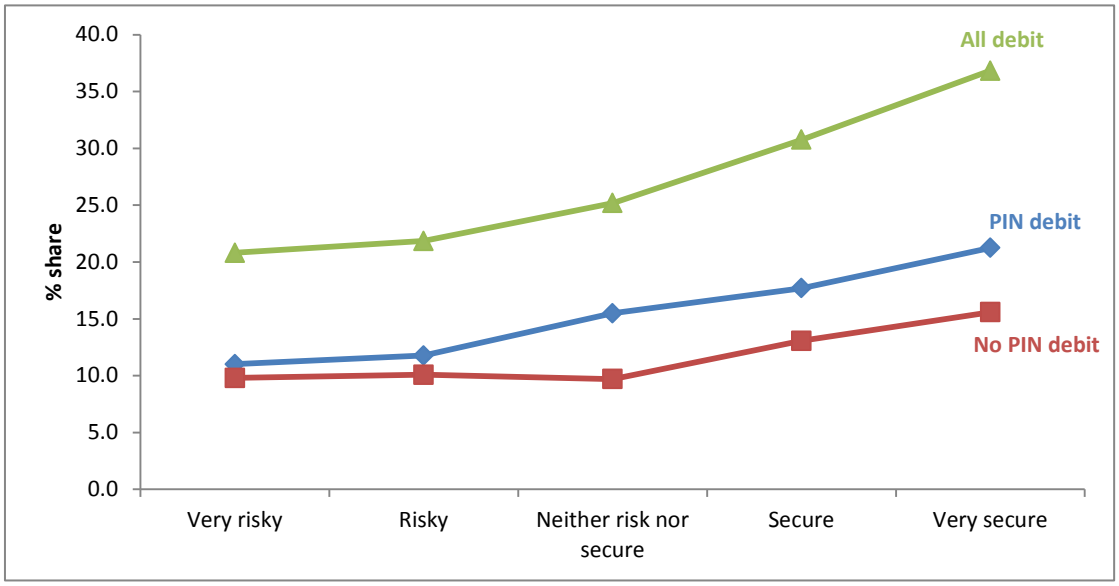


Table 11: Regression Results for Payment Instrument Adoption and Use

Panel A: Probit regression of adoption (Heckman 1st Stage)

	Cash[a]	Check	Debit	Credit	Prepaid	Bank Account	Online Bank Bill
Characteristics							
Security		0.28 *	0.36 ***	-0.10	0.08	0.14 **	0.22 ***
Acceptance		-0.20	0.47 ***	0.23	-0.04	0.17 **	0.25 ***
Cost		0.05	0.74 ***	0.10	0.19 **	0.33 ***	0.60 ***
Convenience		0.04	0.90 ***	0.55 ***	0.09	0.13 *	0.76 ***
Setup		0.60 ***	0.44 **	0.81 ***	0.16 *	0.31 ***	0.56 ***
Records		0.53 **	0.46 ***	0.74 ***	-0.01	0.26 ***	0.41 ***
N		1,958	1,956	1,959	1,953	1,938	1,953
Psuedo *R* -squared		0.33	0.21	0.33	0.03	0.09	0.19

Panel B: Regression of use (Heckman 2nd Stage)

	Cash[b]	Check	Debit	Credit	Prepaid	Bank Account	Online Bank Bill
Characteristics							
Security	0.01 **	0.02 **	0.01	0.03 **	-0.01	0.00	0.00
Acceptance	-0.01	0.01	0.03	0.01	0.02	0.00	0.01
Cost	0.06 ***	0.02 *	0.04	0.12 ***	-0.05 **	0.02	0.03
Convenience	0.07 ***	0.10 ***	0.18 ***	0.17 ***	0.00	0.02 **	0.01
Records	0.04 ***	0.06 ***	0.05 **	0.09 ***	0.03 ***	0.00	0.06 ***
Inverse Mills		0.01	-0.15 ***	0.04	-0.19 *	-0.02	-0.04
N	1,920	1,840	1,556	1,602	710	1,366	1,029
Adjusted *R* -squared	0.13	0.17	0.22	0.26	0.14	0.02	0.06

Source: 2010 Survey of Consumer Payment Choice (SCPC).

Notes: Coefficients on the demographic and income variables are not shown here, but all were included in the regressions.

a: Cash adoption was almost universal.

b: Cash use estimated with OLS.

Table 12: Regression Results for Payment Instrument Use at Point of Sale

Panel A: Regression of use (Heckman 2nd Stage: Point of Sale)

	Cash[a]	Check	Debit	Credit	Prepaid	Bank Account	Online Bank Bill
Characteristics							
Security	0.01 *	0.01	0.00	0.02	0.00		
Acceptance	-0.01	0.01	0.03	0.02	0.01 *		
Cost	0.05 ***	0.00	0.05 **	0.09 ***	-0.01 *		
Convenience	0.06 ***	0.05 ***	0.13 ***	0.12 ***	0.00		
Records	0.03 ***	0.02 ***	0.04 *	0.08 ***	0.01 ***		
Security_POS[b]	0.01 ***	0.00	-0.01	0.01	0.00		
Inverse Mills		0.01	-0.12 ***	0.03	-0.05		
N	1,899	1,792	1,550	1,594	702		
Adjusted *R* -squared	0.09	0.11	0.19	0.24	0.05		

Panel B: Regression of use (Heckman 2nd Stage: Online Nonbill)

	Cash[a]	Check	Debit	Credit	Prepaid	Bank Account	Online Bank Bill
Characteristics							
Security			-0.01 *	0.00 *	0.00	0.00	
Acceptance			0.00	0.00	0.00	0.00	
Cost			0.00	0.01 ***	-0.01 *	0.00	
Convenience			0.01	0.01 **	0.00	0.00	
Records			0.00	0.00	0.01 **	0.00	
Security_OP[b]			0.00	0.00	0.00	0.00 ***	
Inverse Mills			-0.02	0.00	-0.06 *	0.00	
N			1,502	1,572	695	1,335	
Adjusted *R* -squared			0.03	0.08	0.12	0.03	

Panel C: Regression of use (Heckman 2nd Stage: Online Bill)

	Cash[a]	Check	Debit	Credit	Prepaid	Bank Account	Online Bank Bill
Characteristics							
Security			0.00	0.00		0.00	0.00
Acceptance			-0.01	0.00		0.00	0.01
Cost			0.00	0.01 ***		0.01	0.01
Convenience			0.00	0.00		0.01 ***	0.02
Records			0.00	-0.01		0.00	0.04 ***
Security_OP[b]			0.00 *	0.00		0.00	0.00
Inverse Mills			-0.02	-0.01		0.00	-0.02
N			1,479	1,524		1,313	990
Adjusted *R* -squared			0.05	0.02		0.02	0.04

Source: 2010 Survey of Consumer Payment Choice (SCPC).

Notes: Coefficients on the demographic and income variables are not shown here, but all were included in the regressions.

a: Cash use estimated with OLS.

b: Security rating for the location of payment - in person (point of sale), and online.

Table 13: Predicted Adoption and Use with a Simulated Increase in Security Rating

			Predicted Adoption: Payment Security Rating Increase[a]			
		Predicted Adoption From Original Probit Model	Debit Card	Credit Card	BANP	OBBP
Adoption (% of Consumers)	Payment Instrument					
	Cash[b]					
	Check	94.30	94.19	94.19	94.16	94.19
	Debit	80.05	82.61	79.64	79.55	79.67
	Credit	82.02	82.10	81.47	82.13	82.10
	Prepaid	37.61	37.45	37.46	37.41	37.47
	BANP	70.47	70.23	70.24	72.26	70.25
	OBBP	53.24	52.87	52.89	52.80	55.23

			Predicted Share: Payment Security Rating Increase[a]			
		Share From Original Heckman Model	Debit Card	Credit Card	BANP	OBBP
Use (% Share)	Payment Instrument					
	Cash[c]	25.52	25.44	25.44	25.44	25.49
	Check	14.15	14.03	14.02	14.02	14.09
	Debit	36.85	37.03	36.82	36.81	36.83
	Credit	24.41	24.27	25.19	24.26	24.34
	Prepaid	20.93	20.99	21.00	20.99	20.96
	BANP	9.64	9.66	9.66	9.52	9.65
	OBBP	12.46	12.45	12.45	12.45	12.53

Source: 2010 Survey of Consumer Payment Choice (SCPC).

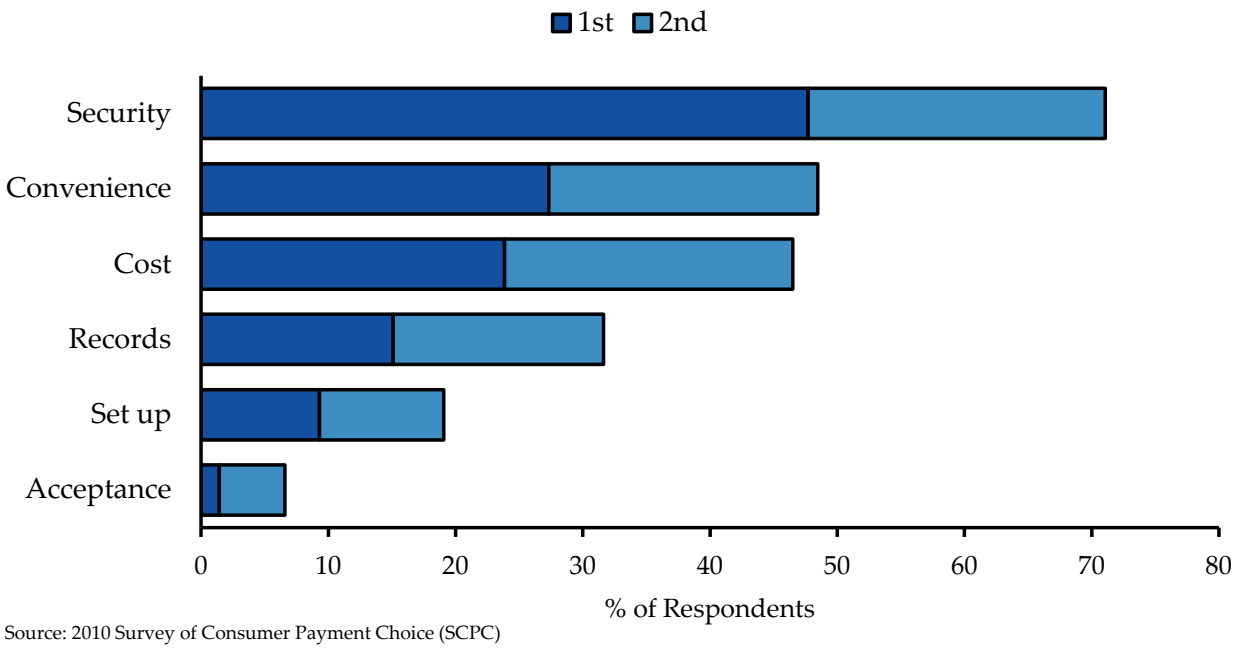
Notes: Coefficients on the demographic and income variables are not shown here, but all were included in the regressions.

a: Each column shows the results of a separate simulation in which the security rating of the column payment instrument was increased by 1 for respondents who did not rate the payment instrument "very secure (5)"

b: Cash adoption was almost universal.

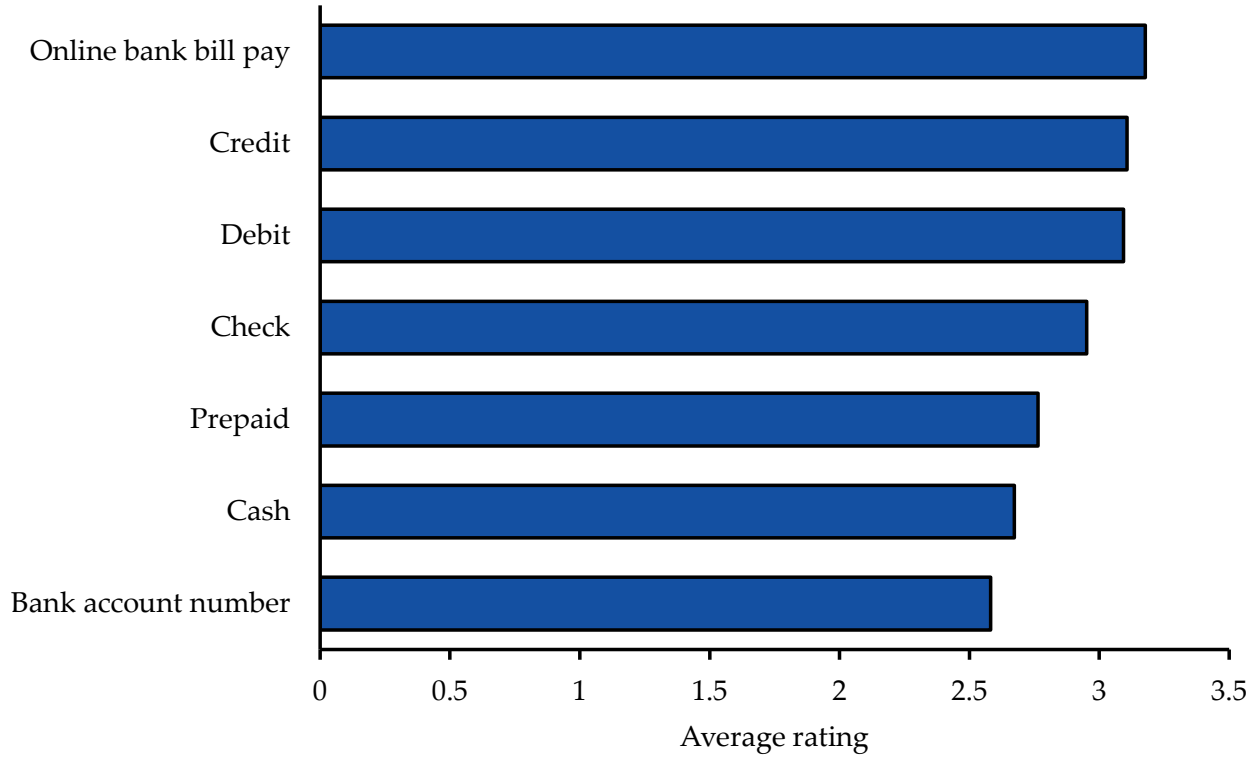
c: Cash use estimated with OLS.

Figure 1: First and Second Most Important Attributes of Payment Instruments



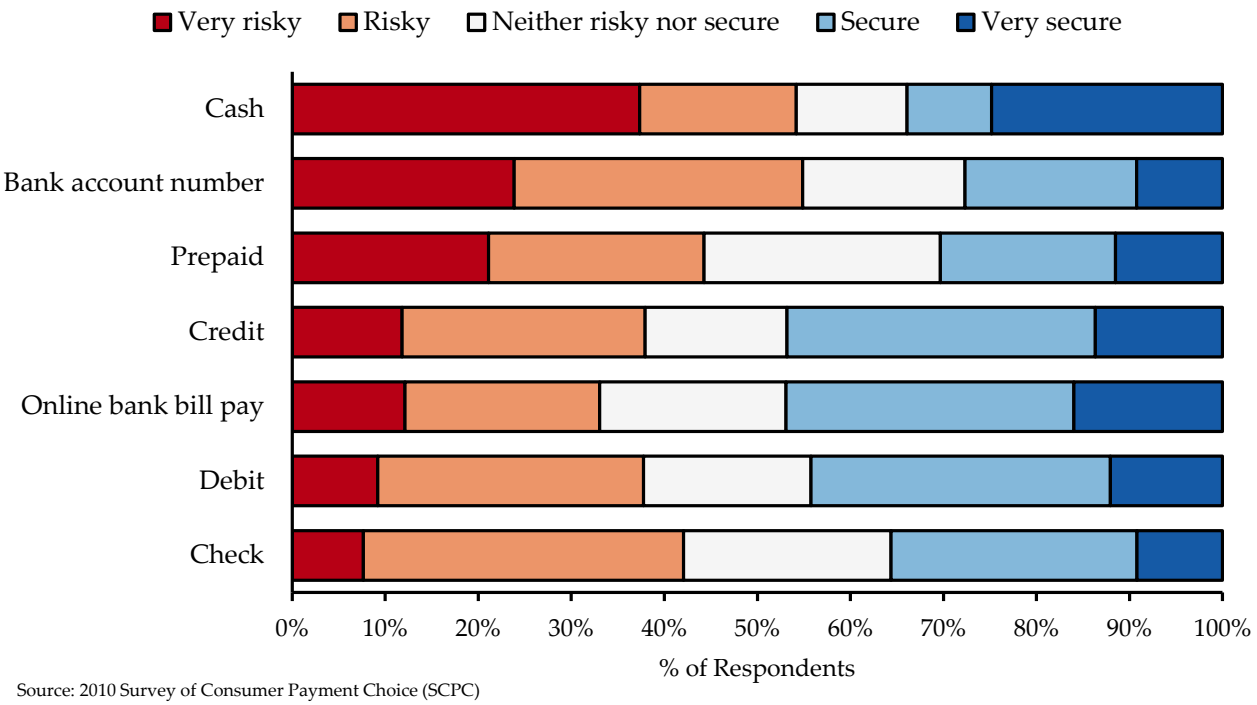
Source: 2010 Survey of Consumer Payment Choice (SCPC)

Figure 2: Average Security Rating, by Payment Instrument



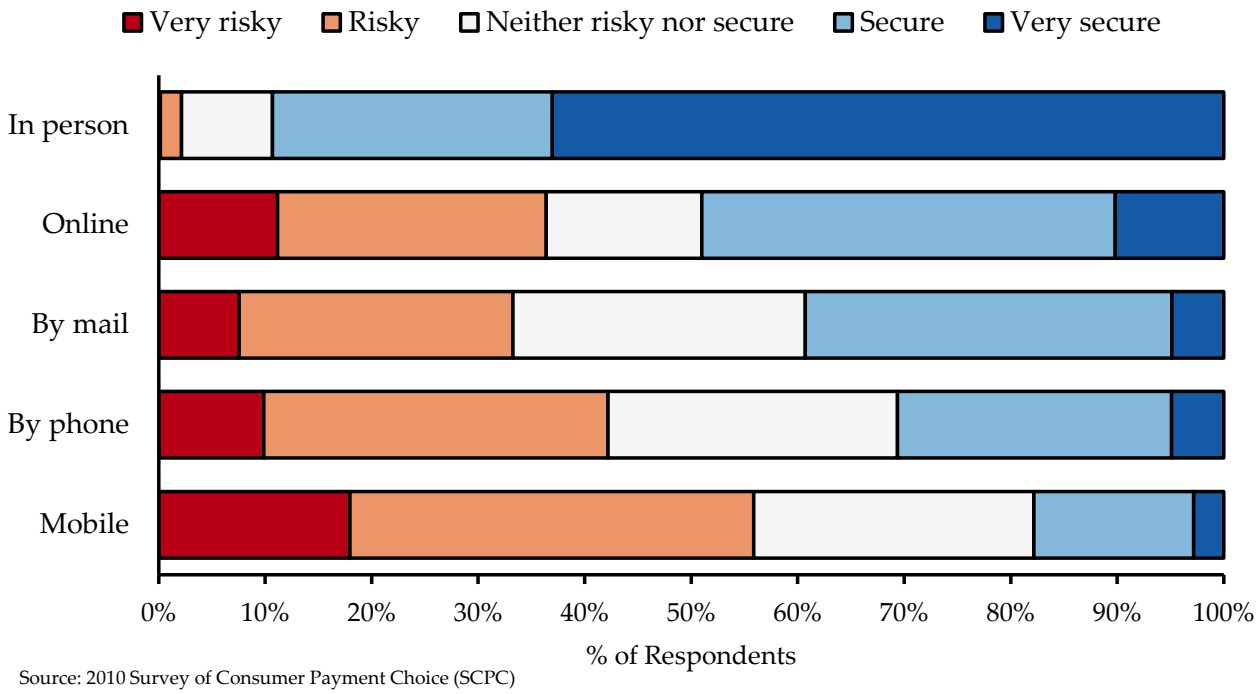
Source: 2010 Survey of Consumer Payment Choice (SCPC)

Figure 3: Security Ratings, by Payment Instrument



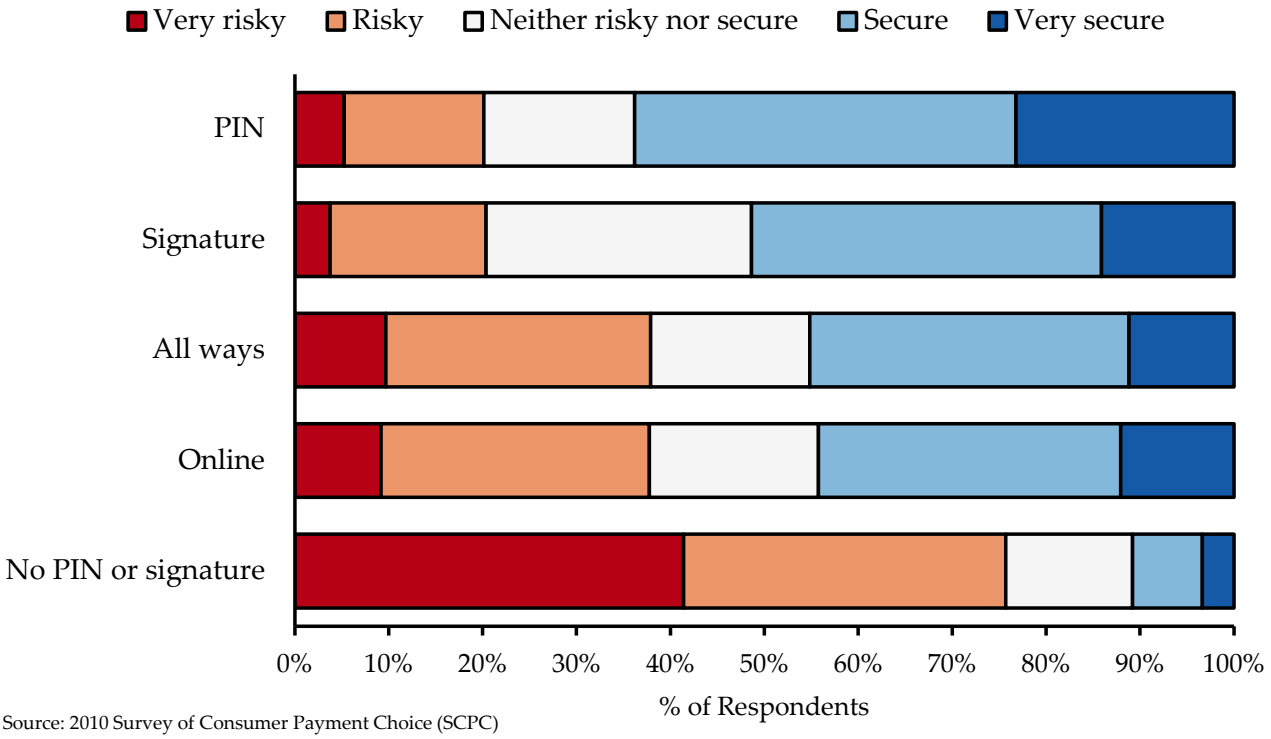
Source: 2010 Survey of Consumer Payment Choice (SCPC)

Figure 4: Security Ratings, by Location



Source: 2010 Survey of Consumer Payment Choice (SCPC)

Figure 5: Security Ratings, by Debit Mode



Source: 2010 Survey of Consumer Payment Choice (SCPC)

Appendix: 2010 SCPC Security Questions

Payment Instrument 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."

"1	2	3	4	5
Very Risky	Risky	Neither Risky Nor Secure	Secure	Very Secure"

Payment Characteristic Rating:
"Please rank the importance of each payment characteristic when you decide which payment method to use."
(Randomized order)
"Acceptance for Payment
Getting & Setting up
Cost
Convenience
Payment Records
Security"

Payment Location Security:
"How do you rate the **security** of the following **locations** of making a payment?"
(Randomized order)
"In person
Online
By mail
By phone
Mobile"

Debit Card Security:
"Debit card payments sometimes require you to

- Enter a Personal Identification Number (PIN)
- Give your signature
- No PIN or signature, typically for small dollar values
- Card number entered online

How would you rate the security of each type of debit card transaction?"