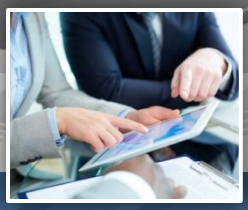


Credit Cards to Smart Cards: How Technology May Need to Shift to Ease Consumer Concerns

By Rockbridge Associates, Inc.

In light of the high profile Target breach in December 2013, there has been a renewed push for updated technology that better protects consumers' personal information when making a purchase. High costs and lack of commitment have prevented successful industry-wide implementation of more secure technology in the past, despite the fact that it has been widely used in Europe for years. However, the breach of Target's systems affected about 70 million credit cards, with the possibility of reaching many more, and suddenly sparked conversation as millions of people realized that it could happen to anyone.

The public is aware of security issues in retailing. Rockbridge explored the topic of compromised information in the National Technology Readiness Survey shortly after the Target incident (February 2014), asking consumers about their awareness of the issue. Awareness of a problem with retailers was widespread, with 86% indicating they had heard some news concerning financial information being compromised and 44% indicating they were "very familiar" with the news.[1]

The perceived impact of security lapses is widespread. Consumers were also asked if they or anyone they knew had financial information compromised when shopping at a retailer – 9% were certain they or a household member had been affected in the past few months.[2] The full extent of the insecurity felt by consumers is reflected by how many believed that it was at least "possible" their household was affected – 28% believed there was at least a chance that their or a member of their household's personal information might have been compromised.[3] Further, 38% thought there was at least a possibility that somebody they know (such as friends, family, neighbors or coworkers) had their information compromised. A full 43% believed it was possible their household or somebody close to them had information compromised in the period of a few months. This suggests that there exists a general worry about the possibility of breaches. In such situations, there are specific responses that companies can take to best salvage goodwill with their customers.

► 43% of consumers believed it was possible their household or somebody close to them had information compromised in the period of a few months.

Consumers expect more than just compensation; they want the problem fixed. The study asked consumers what courses of action they would expect from a retailer in the event that their information was compromised. The top two potential remedies (see Figure 1) are adopting new technologies that make it harder for information to be stolen in the future (70%) and paying for any losses that occur (68%). Many consumers would also consider an apology, free credit monitoring, and help with restoring credit and changing accounts, but these appear to be superficial measures. The message is that retailers should pay for the losses to victims and make sure the problem does not happen again.

[1] *Question: In the past few months, have you seen, read or heard news about consumers' private financial information being compromised when shopping at major retailers?*
[2] *Question: In the past few months, have you or members of your household had private financial information compromised when shopping at a retailer?*
[3] *Question: In the past few months, have any people you know, such as friends, family, neighbors or coworkers, had private financial information compromised when shopping at a retailer?*

The preferred method of responding, if customers had to choose one, is for a retailer to pay for losses that occurred as a result of a breach (37%). After all, since consumers' information was compromised through no fault of their own, why should they be held accountable for the adverse consequences? However, 27% of consumers prefer that the retailer upgrade their technology to prevent the problem in the future. Even though it is too late to undo a breach that already happened, taking steps to prevent another in the future seems an ideal course of action for a company. Following its own problems last year, Target announced the acceleration of their new chip-and-PIN program for smart cards. Target executives plan for the cards to be introduced in early 2015, six months ahead of schedule.[4]

Europe has already been using similar chip-and-PIN credit cards for years. These cards store information on a chip rather than a magnetic stripe and require a PIN to complete the transaction. The chip encrypts personal information and is difficult to duplicate, making it more secure than a magnetic stripe. After these cards were issued in Europe, data theft decreased considerably.[5]

Consumers support better technology (especially if somebody else pays for it). The survey asked consumers to weigh in on the idea of introducing more secure smart card technology with embedded chips to prevent fraud. Nearly two-thirds (65%) think this is a good idea in principle (see Figure 2). However, transitioning to smart cards has costs associated with it due to a new infrastructure of credit card readers.

Figure 1. Responses for Addressing Security Breaches (1230 Respondents)

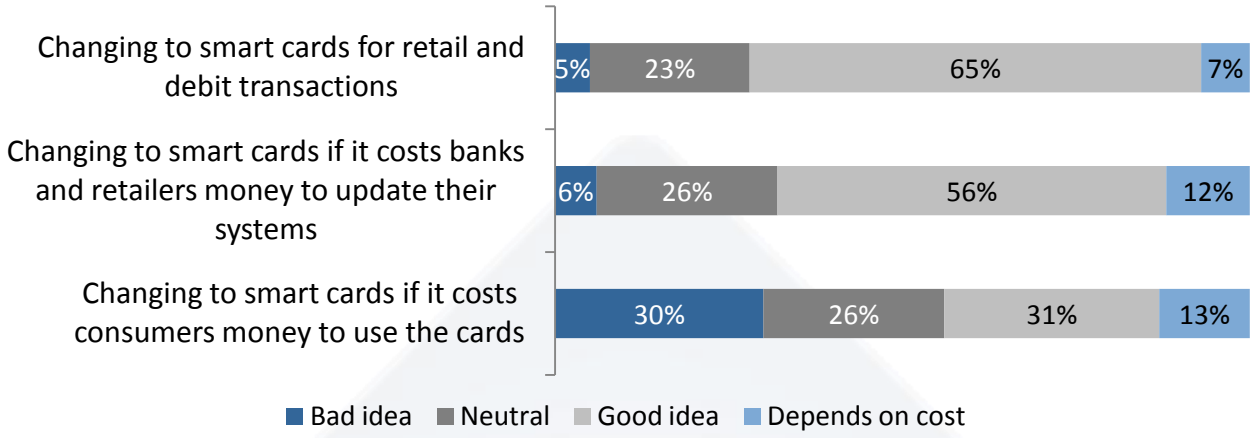
Type of Response	Potential Response	Preferred Response
Adopt new technologies that make it harder for information to be stolen	70%	27%
Pay for any losses that occur as a result	68%	37%
Provide free credit monitoring services	53%	9%
Issue apologies	53%	1%
Offer identity theft consultant to help restore credit	51%	9%
Help customers close and reopen accounts	48%	6%
Not charge for purchases where information was stolen	38%	10%
Offer customers a discount on merchandise	29%	2%

Question: When consumers' private financial information is compromised when shopping at a retailer, what (if anything) do you feel retailers should do for these customers? If the retailer could do only one thing, which of the following should it be?

[4] *Source: John Mulligan, "Time for Smartcards," Target Corporation, 4 February 2014.*

[5] *Source: Heather Long, "Why is the US a decade behind Europe on 'chip and pin' cards?" The Guardian, 27 January 2014.*

Figure 2. Public Opinion on Smart Cards



Question: Some countries use "smart cards" for credit and debit transactions. They are more secure than the magnetic stripe cards used mainly in the U.S. because they have information embedded on computer chips in the cards. What do you think about changing to smart cards for retail and debit transactions in the U.S.? What do you think about changing to smart cards for retail and debit transactions in the U.S. if it costs banks and retailers money to change their systems to accept these cards? What do you think about changing to smart cards for retail and debit transactions in the U.S. if it costs consumers more money to use the cards?

A majority of consumers (56%) still think smart cards are a good idea if it costs banks or retailers money to change their systems, but those in favor become a minority if it costs consumers more money to use the cards. If the cost to use smart cards is absorbed by consumers, just as many consider it a bad idea (30%) as a good idea (31%). Our survey did not specify the costs to consumers, so the actual acceptance may depend on exactly how the change impacts costs to them.

About the Study: the 2014 National Technology Readiness Survey is based on an online survey of 1230 U.S. adults sampled at random from a consumer research panel. The survey was conducted in February 2014, and results are weighted to match Census data. The margin of error for the study is +/ - 3 percentage points. The study is co-sponsored by Rockbridge Associates, Inc. and the Center for Excellence in Service at the Robert H. Smith School of Business, University of Maryland, College Park.

Summing it up, there is widespread awareness among consumers of security lapses by retailers and a surprising number believe they or someone they know has been affected. There is support for better technology for retail transactions, so long as industry and not consumers pay for it. Consumers believe that protecting their personal information is a pressing issue, and that it can be mitigated with better technology. Changing to smart cards could have other benefits as well, such as allowing American consumers to use their credit cards more easily when traveling abroad. Some U.S. credit cards currently do not work with European readers and those that do work require a PIN, which travelers must request from their bank in advance.

In order for the transition to be successful this time, banks and retailers both must commit to the switch; Target's attempt to implement chip-and-PIN cards in 2001 was unsuccessful because no other companies transitioned with them. Regardless of the large costs for all parties involved, the renewed push for more secure technology seems to be making headway more than ever before. Banks are beginning to issue chip-and-PIN cards, and hope to complete the transition by the end of 2015. Retailers will then be liable if they do not have the appropriate card readers, which could provide an incentive for them to front the costs of updated credit card reader infrastructure.[6]

[6] *Source: Heather Long, "Why is the US a decade behind Europe on 'chip and pin' cards?" The Guardian, 27 January 2014.*