The New York Times | http://nyti.ms/1aPaKdc

THE OPINION PAGES | OP-ED COLUMNIST

Dogged by Data Theft

FEB. 10, 2014

Joe Nocera

"What is stopping us from moving to this kind of technology?" asked a perplexed Senator Amy Klobuchar, Democrat from Minnesota. It was last Tuesday, and the Senate Judiciary Committee, on which Klobuchar sits, was holding a hearing about the recent breaches of Target and Neiman Marcus in which the data from tens of millions of credit and debit cards were stolen.

The technology Klobuchar had in mind is known as chip-and-PIN. The chip refers to a computer chip embedded in a credit or debit card that encrypts data and authenticates the card. The PIN refers to a personal identification number the customer has to use, which, in effect, authenticates the user.

It is no big secret that, from a security standpoint, a chip-and-PIN system is far superior to the magnetic stripe that is the backbone of the credit and debit card systems in the United States. Criminal gangs in Eastern Europe have learned how to penetrate many computer systems of American retailers and "skim" credit card data at the moment a transaction takes place. That kind of theft would be virtually impossible with a chip-and-PIN system.

Nor is it news that much of the rest of the world long ago adopted chip-and-PIN technology; according to MasterCard, 79 percent of terminals in Canada,

Latin America and the Caribbean are “chip-enabled,” a figure that rises to 95 percent in parts of Europe. But, inexplicably, this clearly superior technology has not yet penetrated the United States.

Or maybe it’s not so inexplicable. The main stumbling block, it would appear, is that retailers and bankers have spent way too much time blaming each other for the growing data theft problem — and not nearly enough time worrying about the people whose data have been stolen. Namely, us.

“Why did the U.S. stick with the mag stripe?” said David Robertson, publisher of The Nilson Report. It may not have been best for consumers, but it was “cheap and efficient” for the banks and retailers. What’s more, banks and retailers had a certain amount of fraud built into their business models. Thus, while a hacked card brought big headaches to the customer, it was just another cost of doing business for the other entities involved in the transaction.

Even as Europe and Canada were moving to a chip-and-PIN system, the American banks held back. Fraud at the point of sale dropped dramatically in countries with chip-and-PIN. Still the U.S. held back. Every time there was a push to adopt chip-and-PIN, both retailers and bankers would do the math and come to the same conclusion: It wasn’t worth the trouble.

And when a company did try to adopt it? That’s what Target tried to do around 2003 — only to discover that it was largely a waste of money if nobody else went along. In Europe and elsewhere governments had pushed companies to adopt chip-and-PIN. In the U.S., the banks and retailers needed to be able to work together — spending billions both to manufacture new cards and install new terminals that could read the cards.

There are two things that are likely to change the equation. The first is the Target breach, which, one expert told me, could involve as many as one in every 10 cards in circulation in the United States. Many of the cards are debit cards, which means if the card is used by a crook to make a purchase, it comes directly out of the customer’s bank account. (Target has vowed to indemnify any customer who has losses as a result of the breach.) The Target breach has shown the reputational hit a company can take when its system is breached. It also has had business consequences: the last two weeks of the Christmas season were lousy ones for Target — and the publicity from the breach is considered a prime culprit.

Second, though, Visa and MasterCard have both set forth timetables that

attempt to institute the adoption of embedded-chips technology by the fall of 2015. Although the timetables are not mandatory, they would essentially shift the liability for card losses on to whichever side — the bank or the retailer — has the least secure technology. Although there were various calls for delaying the implementation yet again, those calls stopped once the Target breach took place.

Which is not to say that the banks and the retailers are now seeing eye to eye. When I spoke to a bank lobbyist last week, he told me that the real problem was "a weakness in the internal computer system of large companies that sophisticated criminals have learned to exploit." The retailers, meanwhile, retort that the banks have continually come up with ideas short of chip-and-PIN, none of which ever worked for long before the bad guys figured how to breach them.

The only thing missing from these arguments is the consumer.

A version of this op-ed appears in print on February 11, 2014, on page A27 of the New York edition with the headline: Dogged by Data Theft.
