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

BUSINESS DAY

Chip Credit Cards Give Retailers Another Grievance Against Banks

By **RACHEL ABRAMS** NOV. 16, 2015

The employee perched on a stepstool by the checkout at Trader Joe's in Union Square in Manhattan is like an air traffic controller: Register 6 for one customer. Register 9 for the next.

The routine helps move traffic quickly through the store, where the lines can often snake around the aisles of whole grain cereal, mixed nuts and Fair Trade coffee. Trader Joe's, like many retailers around the country, recently upgraded its payment terminals around the Oct. 1 deadline to accept debit and credit cards with a new security chip.

The timing, retailers say, could not be worse.

The new terminals are often slower, meaning that the long lines during the busy year-end holiday season will grow longer.

"If they couldn't get it done before 10/1, I doubt many are going to have the appetite to turn it on between now and the end of the year," said Mark Horwedel, chief executive of the Merchant Advisory Group, which advocates on behalf of retailers. "This is make-it-or-break-it sales season for the merchant community."

The new chip cards are also at the center of a growing dispute that has pitted two of America's most prominent industries — banking and retailing — against each other, and pulled in attorneys general and even the Federal Bureau of Investigation in the process.

But the debate involves more than whether consumers will be adequately protected during a season that has been rife with security breaches: The battle could affect the long-simmering war over the billions of dollars in interchange fees that merchants pay to process credit and debit transactions.

“That is the crux of the matter,” said David Robertson, publisher of The Nilson Report, a payments industry publication. “The real savings is not about fraud, the real savings is about interchange.” Last year, merchants paid about $61 billion in interchange fees, Mr. Robertson said, compared with about $30 billion in fraud losses.

The fight involves new payment cards, issued over the last year, that come with a small square security chip that can help make in-person transactions more secure. Retailers complain that they have spent billions of dollars upgrading their payment terminals to accommodate a system that cuts down only on the fraud shouldered by banks, not merchants. Chip and PIN, long the standard in Europe, would help retailers verify not just the card, but the person using it.

Writing to their colleagues in October, two attorneys general sounded a warning bell: The new security chip would not go far enough to make transactions safer. Credit cards needed a PIN, too.

“If we continue to settle for weaker standards here, we will continue to pay the price,” wrote Sam Olens, the Republican Georgia attorney general, and George Jepsen, his Democratic counterpart in Connecticut. They urged top prosecutors in other states to sign a separate letter to Visa, MasterCard, JPMorgan Chase, Bank of America and other institutions, pushing them to adopt the chip-and-PIN technology.

Banking groups were swift to issue their own statement, saying that merchants had been “spreading an outdated narrative.” In November, a spokesman for Mr. Olens confirmed that he had taken his name off the letter.

“While the attorney general still supports chip and PIN, we have no further comment at this time,” the spokesman, Nicholas Genesi, wrote in an email.

On Monday, Mr. Jepsen and eight other attorneys general sent the financial

institutions a revised version of the letter. While they urged the adoption of chip and PIN "as soon as possible," the prosecutors made it clear that they were seeking neither a deadline nor a law to make such adoption mandatory.

"We are sensitive to the concern that locking into the law any particular card security technology may pose risks to future innovation and/or give rise to incompatible technical requirements in different jurisdictions," they wrote.

Banks insist the chips and a signature are enough, and argue that retailers are seeking to deflect attention from the real threat to consumers: weaknesses in retailers' security systems that have allowed hackers to steal credit card data in a series of breaches. And they point out that by some estimates, only about half of retailers, or even fewer, will be able to process chip-enabled cards by the end of the year.

"We think the focus should be for retailers to turn on their chip readers and use the technology that's available to them," said James Chessen, the executive vice president and chief economist at the American Bankers Association, an industry trade group.

Banks, too, are lagging. By some estimates, only 19 percent of cards in circulation were chip-enabled by Oct. 1. Retailers were to upgrade their payment terminals to accept chip cards by that date, or become liable for fraud.

Most of the big banks will still be issuing new cards into next year.

While large retailers have spent billions of dollars upgrading their equipment, small businesses also say that the new cards are overly burdensome without adding enough protections. Jared Scheeler, who sits on the board of the National Association of Convenience Stores, testified in front of the House Small Business Committee last month. He said, "It does not appear that the card companies took into consideration the realities of operating a small business when they came up with their transition plans."

Mr. Scheeler testified that it cost the average convenience store $26,000 to upgrade its gas pumps and point-of-sale terminals; average annual profit at convenience stores is about $47,000.

But because of “exorbitant” swipe fees and other liabilities, Mr. Scheeler said, merchants will end up bearing “far more than 100 percent of the cost of fraud.”

For years, retailers and banks have fought over the fees that merchants pay for every credit or debit transaction. Congress handed retailers a victory by ordering the Federal Reserve to cap the fees on debit transactions as part of the Dodd-Frank financial reform act of 2010.

The Fed set the cap at 22 cents, plus 0.05 percent of the purchase value. No cap exists for credit card transactions, which are typically more expensive.

But retailers thought that 22 cents was too high, and unsuccessfully took the Fed to court. In a court filing, Senator Richard Durbin, Democrat of Illinois, said the agency had succumbed to “heavy lobbying by the banking industry.” Senator Durbin championed the original amendment to the Dodd-Frank act that instructed the Fed to review debit cards.

Banks say interchange fees help cover the cost of fraud. Retailers argue that fees should therefore decrease if fraud is reduced.

“PIN is the leverage merchants are looking for to get action from Congress,” said Mr. Robertson, the Nilson Report publisher. “That’s why they’re constantly trying to get the public on their side by talking about security.”

Mallory Duncan, the senior vice president of the National Retail Federation, an industry trade group, said reducing interchange fees was not the driving issue behind the chip-and-PIN debate.

“I don’t think it’s leverage, it’s a question of whether or not the card companies have been telling the truth about what goes into making the interchange fees,” Mr. Duncan said.

Security specialists generally agree that a chip-and-PIN system is more secure than chip-and-signature for in-person transactions. A security chip without a PIN helps verify the legitimacy of the card, but not the user.

That helps cut down on the effectiveness of counterfeit cards, but not online fraud or in situations where a card is lost or stolen. But Stephanie Ericksen, the

vice president of risk products for Visa, points out that merchants are not held liable for fraud committed with lost or stolen cards processed on the network, one of the world's largest. (Mr. Duncan argues that, despite the policy, retailers end up paying for nearly a third of such fraud anyway.)

"We certainly support issuers and merchants if they want to move to PIN," she said, but Visa did not offer an incentive to do so. Instead, Ms. Ericksen said that Visa was investing in more "dynamic" security solutions, such as more advanced data encryption methods and biometric authentication.

In early October, the F.B.I. issued a warning that chip-and-signature cards were still vulnerable to fraud. The original announcement seemed to incorrectly indicate that banks were issuing chip-and-PIN-enabled credit cards, and urged consumers to use the PIN instead of a signature whenever possible. The bureau also warned that the new cards "can be counterfeited using stolen card data obtained from the black market."

The American Bankers Association quickly called the bureau to clarify some "misinformation," Mr. Chessen said, and the bureau revised its statement. The new warning does not say that the cards can be counterfeited.

The bureau changed the advisory to "clarify the security safeguards associated with EMV technology and to highlight some of the potential vulnerabilities fraudsters and cybercriminals may try to exploit," Jillian Stickels, an F.B.I. spokeswoman, wrote via email.

"Given the clear consumer benefits of chip and PIN, why are banks hesitating to require both?" Martha Coakley, a former attorney general of Massachusetts, said in an opinion article she co-wrote that was published in September. "The truth is that, for banks and card networks, the status quo is lucrative; they don't want to change."

The Retail Industry Leaders Association, a trade group, confirmed that it had hired Ms. Coakley as a consultant, as well as Jon Bruning, a former attorney general of Nebraska, to help make its case.

Correction: November 16, 2015

An earlier version of this article misstated the cap on debit transaction fees set by the Federal Reserve. It is 22 cents plus 0.05 percent of the purchase value, not 5 percent.

Hiroko Tabuchi contributed reporting.

A version of this article appears in print on November 17, 2015, on page B1 of the New York edition with the headline: Chip Cards Give Stores New Gripe Vs. Banks .
