Bankrate®

How lawsuits over chip-and-PIN cards affect consumers

By Mike Cetera
July 7, 2016

Three of the nation's largest retailers have sued the big credit card processing firms over how you pay at the register. The lawsuits argue that credit payments networks Visa and MasterCard are compromising security in favor of their bottom lines, leaving consumers vulnerable to fraud.

The lawsuits filed recently by Wal-Mart, Home Depot and the grocery chain Kroger aren't identical, but they share a theme: The new way we "dip" our debit and credit cards isn't secure enough -- and the credit companies know this.

There's much to unpack here, so we'll show how this argument affects consumers in question and answer form.

What are these lawsuits about?

Wal-Mart was first to sue, arguing in a partially redacted lawsuit that it should be able to force debit card users to enter a PIN when they try to pay with their cards.

"PIN verification is significantly more secure and less prone to fraud than signature verification," Wal-Mart argued in its lawsuit. "Signatures can be forged or copied, and cashiers may forget to check the signature on a receipt or (point-of-sale) terminal to make sure it matches the signature on the back of the card."

Wal-Mart last year began requiring that customers use PINs for chip-based debit cards, "declining transactions if a customer refused to enter the identification code," according to Forbes. The company abandoned that policy after Visa told Wal-Mart it was required to allow for signature-based transactions, "citing the terms of its contract with the retailer."

Visa also told Kroger, which owns grocery stores in 35 states, that it was violating the contract and began fining the company after it refused to allow for signature-based transactions. Kroger sued in late June after it said Visa had threatened to cut off its ability to accept Visa debit cards.

"There is no rational basis for Visa to cut off Kroger's ability to accept any or all Visa debit cards unless Visa intended to punish Kroger," according to the lawsuit. "Doing so threatened catastrophic consequences for Kroger's business, including turmoil at the check stand as Kroger customers were unable to pay, and the loss of Kroger customers who insisted on using a Visa debit card to pay and thus went elsewhere to shop."

Home Depot, meanwhile, sued both Visa and MasterCard. It wants to mandate chip-and-PIN for both credit and debit transactions.

The home improvement retailer argues Visa and MasterCard have successfully fought off the implementation of PIN credit cards to stifle competition and inflate the fees it collects from businesses.

"While chip-and-PIN authentication is proven to be more secure, it is less profitable for Visa, MasterCard, and their member banks and it provides a greater threat to their market dominance," the lawsuit claims.

I don't understand. I'm asked to enter my PIN when I pay with a debit card.

True. But, in the case of Wal-Mart, instead of entering your PIN, on some debit transactions you can press a button on the card-reader screen that says "other." That allows you to opt out and sign for your transaction.

In its lawsuit, Wal-Mart says 70% of the dollar value of in-store card payments are made with debit cards. About 10% of debit-card users bypass a PIN and opt to sign to verify their purchase, according to Forbes.

Customers are not asked to enter a PIN on credit transactions.

Wasn't the primary motivation for switching from the traditional magnetic stripe to chips one of security?

Yes! And the chip cards, also called EMV cards, are more secure. Because the chips send a unique, one-time-only, digital code during a transaction, they make counterfeiting cards much more difficult. That static data contained in the stripe on the back of your old cards was easy to steal and to sell on the black market.

So, when you dip your card -- and then are forced to wait extra time for that transaction to go through -- you're making it more difficult for thieves to use your card data to make in-store fraudulent purchases.

That has perhaps led to some confusion that the new cards are the solution to all card fraud.

"The consumer feels like, 'Yes, it's more secure, but it takes longer. But at least now I'm not subject to credit card fraud,'" says David King, senior manager in the internal audit, risk and compliance practice at professional services firm UHY Advisors in Atlanta. "That observation is correct; it does take longer. That assumption (that you're immune to fraud) is incorrect; it's materially incorrect."

Why aren't signature-based transactions as secure?

"Chip-and-PIN cards are more secure (than) chip-and-signature cards because the customer has to provide a 4-digit PIN to complete the transaction. This number must match the number stored on the chip," Huseyin Cavusoglu, an associate professor of information systems in the Naveen Jindal School of Management at the University of Texas at Dallas, said in an email. "Therefore, even if a card with chip-and-PIN technology is stolen, there will be no fraudulent transactions unless the thief knows the PIN."

So it's much harder for a thief to copy the data on your card, but if he stole your physical card, he could use it in a store and have little worry of getting caught when a PIN isn't required.

"We all know you could write 'Donald Duck' as a signature, and the purchase will still process," King says.

In fact, according to the Home Depot lawsuit, "Visa and MasterCard do not require that signatures are verified and even discourage merchants from verifying signatures, for fear that consumers will be less likely to use their payment cards."

In addition to allowing for some in-store fraud, transactions that don't require a PIN also make online fraud much easier to commit.

The motive is money here, right?

That's what the lawsuits argue. The processing firms make more than twice as much money off of signature-based transactions than they do PIN transactions, King says.

And because of the way their contracts with retailers are structured, Visa and MasterCard can route signature-based transactions through their processing centers and charge higher fees, Cavusoglu says.

So retailers would pay less, perhaps significantly less, under chip-and-PIN, while the card processors would be dealt a big blow to their bottom lines. How that would impact what you pay at the register is less clear.

What do Visa and MasterCard say about this?

Visa and MasterCard have argued -- in other countries -- for the superiority of chip-and-PIN transactions, according to the Wal-Mart lawsuit.

In Australia, for instance, the 2 companies urged the Australian Competition and Consumer Commission to allow them to work together to implement mandatory PIN authentication. "Any delay will prolong the period in which fraud perpetrators can take advantage of signature as opposed to PIN as a means of verifying a card at (point-of-sale)," Visa and MasterCard are said to have written according to the Wal-Mart lawsuit.

But following the Home Depot lawsuit, a MasterCard spokesman defended the security of chip cards, telling The Associated Press, "Regardless of how the cardholder's identity is confirmed, the chip makes data much more secure, rendering it almost useless to create fraudulent cards or transactions."

And both Visa and MasterCard have argued that Americans don't want to have to memorize yet one more thing -- after online passwords and other bank PINs.

"American charge cards have never been used with a PIN historically, and it is not an ingrained behavior to use a PIN with a credit card," Seth Ruden, senior fraud consultant at electronic payments company ACI Worldwide, said in an emailed response to questions. "Many feared that a change (like remembering a PIN) in consumer habits could create friction and may even reduce sales."

Is chip-and-PIN the ultimate fraud solution?

Some experts say chip-and-PIN is just part of the answer. Ruden's trifecta of authentication in the form of "what you have" (your card) "what you know" (your PIN) and "who you are" (your fingerprint) is a way to add security, "but we still have a few years to go until this is more widespread."

Cards will be truly secure when they combine EMV (a unique code at the transaction), point-to-point encryption (scrambled data from the merchant to the processor) and tokenization (a secure "token" returned to the merchant in lieu of credit card data), says Dan Fritsche, vice president of solution architecture at Coalfire, a cybersecurity risk and assessment company.

We're not there yet, though, so how does Fritsche protect himself?

"I'd rather have an EMV than a swipe card, but I'd rather have my Apple Pay than EMV," he says. "And I don't do debit."