

U.S. Stores Are About to Pay Up for Security

IGHT NOW, if someone steals your credit card information, it's a cinch for thieves to use it to make a counterfeit card. If that happens and they buy, say, a diamond necklace, your bank is on the hook to pay the damage. But not for long. Starting this

fall, it will be individual stores (or jewelry dealers) and their insurers that will have to pay the bills for counterfeit credit card fraud. And many retailers are very, very unhappy about it.

The new rule, or "liability shift," will take effect on Oct. 1. It's meant to encourage retailers and banks to adopt securer payment technology: EMV chip-enabled credit cards and card readers, which render criminally crafted cards—ones that use stolen magnetic strip data—ineffective. If banks issue the securer cards, then they're no longer responsible for counterfeit fraud. If retailers install the new card-reading systems, then the liability shifts back to the banks.

The problem is that the upgrades are expensive (the

NEW RULES ARE MAKING CARDS MORE SECURE, **BUT FRAUD MAY BE A** STEP AHEAD

cards and card readers will cost a collective \$6.8 billion, according to Javelin Strategy and Research]. And they won't solve everyone's woes-especially the stores'.

"It's causing some consternation in the retail community," says Mallory Duncan, head of the National Retail Federation. "We're being asked to improve the flaws in [the banks'] system," he says of the billions that retailers will pay for new card readers. [Visa, for its part, points out that the new cards will be an investment as well.)

But there's an even pricier problem looming: The counterfeit fraud prevented by chips in stores is all but quaranteed to shift online. Javelin estimates that "card-not-present" fraud will explode from \$10 billion last year to \$19 billion in 2018, when the equipment upgrade should effectively be completed. That's a 90% surge. And merchants will, as always, have to cover the costs of digital scams.

So, the dilemma: If a retailer shells out for new gear, the investment will do nothing to stave off fraud growing quickly online. On the other hand, if the retailer skips the upgrade, then it could become the weakest link in the fraudster food chain, effectively painting a bull's-eye on its back.

Neither option is appealing for stores. "Merchants are at the short end of the stick," says Gartner analyst Avivah Litan.

The bright side? Ameri-

cans will get in-store security upgrades that are long overdue. The U.S., with its complex ecosystem of competing parties and interests, is one of the last developed countries to adopt EMV chip technology. The U.K., Australia, and Canada have already done so and added an extra layer of security: a protective PIN, known only to each cardholder, that must be entered to authorize transactions. China went a step further, pushing contactless payment cards that use a tap instead of a swipe or dip.

That may be cold comfort for merchants facing down online card fraud, though, where the deck is decidedly stacked against them. -Robert Hackett



RAW DATA SUSHI IN AISLE FOUR

SUSHI SALES AT GROCERY STORES OVER THE PAST 12 MONTHS. YEAR TO DATE, SUSHI HAS MADE UP 3% OF ALL GROCERY-STORE DELISALES.

INCREASE IN GROCERY-STORE SUSHI SALES OVER THE PAST FOUR YEARS.

PEOPLE AFFECTED BY A SALMONELLA OUTBREAK THIS YEAR LINKED TO TUNA ROLLS.