Non-EMV compliant retailers are on the hook for fraudulent transactions, including the chargebacks they are not liable for

February 2, 2016

NEW YORK – Forbes this week put the spotlight on the liability shift following the October 1, 2015, EMV compliance deadline for U.S. retailers.

"The reason for the mandate is very straightforward," writes Paula Rosenblum of Forbes in her piece, "The Nightmare Continues: Banks Using New Payment Standards To Soak Retailers." "As my partner Brian Kilcourse often describes, banks and the credit card industry pushed for it to transfer risk from the banks to retailers. Consumers had no credit card related risk before, and they still don't. But retailers who are not EMV compliant now assume the liability for fraudulent transactions arising from stolen credit cards."

Gray Taylor, executive director of Conexxus, noted in NACS Daily on October 1 how banks are getting out of the risk business by shifting liability onto retailers. "Controlling the societal cost of fraud is squarely on the merchants' back—the least enabled stakeholder in the payments ecosystem to implement further structural safeguards," he said.
Four months into EMV compliance in the United States, only 6% of merchants made the mandate deadline and only 8.5% of merchants are EMV ready, noted Greg Buzek of IHL Group. "But it is the stories from frustrated CIOs we heard that are the real kicker," he writes.

"When banks sent retailers that were not EMV compliant the bills for fraudulent transactions as promised, they sent every single chargeback…even the ones the guidelines say the retailers were not liable for!" writes Buzek. "Lost and stolen cards are not supposed to be charged to the retailers for fraudulent transactions. So for instance, if I stole your chip card and went to the store and used it…that is a legitimate card, but I'm not a legitimate user. EMV as implemented as chip and signature would not catch me doing this if you had not reported it lost or stolen yet. But because of greed and/or laziness from the banks, all of these charges are being passed on to the retailers."

Taylor told NACS Daily that banks are taking a "charge them all back" approach to chargebacks, which will have dire consequences for small to mid-size retailers, who can scarcely afford dedicated chargeback staff.

Buzek also points out that retailers are now storing Track 2 data so that they have an audit trail to fight the merchant and acquiring bank for fraudulent charges, which is the data retailers had been mandated not to store several years ago as part of the PCI-DSS. As Rosenblum adds, the "data included in those old-fashioned mag stripes."

Rosenblum points out that the retail industry "spent a fortune on complying with a standard (PCI-DSS) that was never going to be adequate for preventing data theft. And it wasn't. Now they're spending another fortune on card readers and software when the banks haven't even cleaned up the card side of the equation. And in managing this untenable situation, they're undoing the other paltry standard they spent a fortune on in the first place."

"The constant mandates from card brands are death by a thousand cuts," Taylor said. "The failure to provide a long-term strategic plan for upgrading the largest payment system in the world is unconscionable and hurts small business the most. Retailers have had three major 'drop everything' payments upgrades mandated to them over the past eight years—and not one of them mandated PIN authentication, the most effective way of reducing fraud. To make matters worse, we will have to invest another few billions on tokenization, mobile and encryption, which we know are just around the corner after we install EMV.