Fishy CNP Fraud Rising

technology risk management fraud protection

Summary: One online payments expert sees fraud growing at an even faster rate than digital sales. With all of this in mind, what can community banks do?

Along the lines of how ridiculous people can be, we recently covered a story on hot dog water, and today shift to one on fish pedicures. Some believe that putting your feet in a tub full of "doctor fish" that nibble at your dead skin increases circulation and provides you with smoother feet. We don't know. But judging by the picture here, it is as crazy as drinking used hot dog water, if you ask us.

Speaking of crazy things in banking, look no further than what has been going on in the five years since EMV (Europay-Mastercard-Visa) chip cards were introduced in the US.

Card fraud at the merchant point of sale has gone down, but merchants and banks alike are finding what goes down must invariably come up too. Ah well, at least the big credit card companies (Visa, Mastercard, Amex, Discover) have waived the signature requirement on the decent machines.

But let's return to our discussion. We note that since retailers first began accepting chip cards 5Ys ago, counterfeit card fraud has decreased by 66%, as EMV chip cards are harder to spoof than the previous magnetic stripe versions, according to Visa. But, just as air in a balloon that is being squeezed will move away from the pressure, so too has card fraud. It has moved from physical point of sale (POS) to online transactions, where fraud is increasing at a 26% clip, according to one expert.

According to the Fed's, "2017 Financial Institution Payments Fraud Mitigation Survey", 75% of banks experienced fraud losses in 2016, and 96% of debit card issuers faced card fraud losses. At least 90% of US payment cards will have a chip by 2020, according to the Fed. However, 63% of banks reported increased fraud loss over 2015. So, what can community banks do?

Be aggressive in establishing rules for suspicious activity. One GA-based community bank works with its core processor to actively create and enforce rules that trigger notifications and block suspicious card activity. Also, one layer of security generates customer notifications when questionable or irregular transactions occur, which has been a helpful measure for customer peace of mind.

Allow for customers to "turn off" their cards easily. Many banks are coming around to the idea that customers should control when to activate their payment cards, and when to turn them "off". Many banks recognize this is the best way to put control back in the hands of customers, when something seems off while protecting the bank too.

Work with outside providers. Last fall, Visa announced its card-not-present (CNP) authentication tool. It gives community banks the ability to add Visa's 3-D Secure authentication protocol, without negatively impacting service levels. Using 3-D Secure, issuers and merchants can access the card company's real-time, secure, information-sharing pipeline. They can then send transaction data to the issuer to verify each transaction.

No matter what the next crazy idea is out there, we know some people will try it out. In the meantime, at least bankers can sleep easier knowing their customer transactions are better protected through EMV chip adoption and continued diligence.

STRESS TESTING & INSIGHTFUL EVALUATION

To satisfy important regulatory expectations, your bank can use our impactful credit stress analyzer (CSA) to evaluate your loan portfolios on both earnings and capital. To learn more, email us or visit our website today.