NW Financial Review
UPDATE

NorthWestern Financial Review, October 2016 Edition

Web Watch

By Justin Dullum *Sun, Oct 02, 2016*

Fraud prevention expert shares best practices.

Card fraud: Prevention relies on more than chips

Chicago-based tech company Rippleshot has developed cloud-based software designed to detect real-time debit and credit card fraud. Kaleigh Simmons, Rippleshot's director of marketing, talked with NorthWestern Financial Review about the company's flagship software and the general state of card security.

Q. Can you frame the threat of card fraud? What's the frequency of abuse and what does it cost banks and consumers?

Over the past year, card issuers in the United States have lost $10.9 billion to fraud. When you look at credit, debit and prepaid portfolios together, issuers are losing an average of $5.90 per card in circulation — just due to fraud. And this year in particular is bad because criminals are trying to get away with as much counterfeit fraud as possible before EMV is more widely adopted. We've all seen it in the headlines, too — the swath of hospitality breaches, the MICROS POS breach, Wendy's, etc.

It's costing banks a pretty penny to deal with this. Not only do they need multiple layers of protection and detection tools to identify fraud, but then they have the cost of reissuance, which is usually somewhere between $11 and $15 for every card they replace, plus the cost of reimbursing the customer for the fraudulent purchase. This is in addition to the risk they take by disturbing the customer with a new card and the chance that they'll stop using it altogether. It's a big problem.

Q. Describe your technology and how it works?

Rippleshot is transforming the way banks detect fraud through a cloud-based technology solution, Sonar, which leverages machine learning and data analytics to proactively pinpoint when and where a card compromise occurred. We know the average compromised card passes through not one, but three compromised merchants, which makes tackling this problem even more difficult. Sonar takes that into account, and ranks a bank's entire portfolio by risk — specifically how likely each card is to go fraudulent in the future. This can significantly lower unnecessary reissuances. But what about the remaining cards? Sonar also provides automated decline rules, customizable by the bank's comfort level around false positive ratio versus amount of fraud captured. These rules have provided considerable lift over nearly anything that a bank currently has in place, while also trimming the total number of rules being fired.

Sonar is fueled by transaction data, so for each client we onboard, we require a series of data streams — gathered either from the financial institution directly, or through the card processor. Sonar is easily accessible from any web browser and all data and reports are exportable CSV files that clients can then import into their portfolio management system.

Q. What are some common types of anomalies in card use that might slip past a detection system?

One that sticks out right away is that fraudsters are getting particularly good at buying and spending cards in the ZIP code that they're from. This makes it incredibly difficult for traditional detection systems that are looking at variables like distance from the cardholder location, to predict fraud when it happens.

Q. What are some of the best practices you'd recommend to consumers to keep them from being compromised?

ATMs and gas pumps are big targets right now because they have more time to become EMV compliant. The Rippleshot team is probably more paranoid than most, given the business we're in, but we always give the card readers a little tug before swiping— just to be sure there's not a skimming device on top.

Q. It seems the general message around the advent of chip cards finally hitting the U.S. is we're all much better off. How much truth is there to this, and how weary should banks and customers be?

We are probably a year or more out from having enough penetration on both sides (bank and merchant) for it to have a significant impact, but eventually, counterfeit card fraud will decline, just as it has in every other country where chip cards have been deployed. The problem is that fraud numbers as a whole have climbed even higher in almost every single one of those countries because the criminals just shift their efforts online. We've already seen the shift to card-not-present fraud for clients that have issued chip cards, and expect the trend to continue.

Now, if you're a bank, you're probably thinking — well, I can just charge all of this CNP fraud back to the merchants. And you're right, but I'd challenge you to think about fraud outside the loss line item in your budget. I'd challenge you to think about customer disturbances, and how your customers are continuing to see fraud and don't know — or care — about the behind the scenes chargeback policies. False positives can cause back-of-wallet behavior. And so can reissuances — nearly 20 percent of cards that get reissued never get reactivated. That's lost revenue and potentially lost customers. And these problems aren't going away because chip cards are here.