

Join the Credit Card Fraud Fight

By Donna Huppler

The fight against credit and debit card fraud has become like a high-speed, high-stakes game of chess for credit union card processors. Each move by the criminals must be countered by the good guys. It becomes a constant battle to protect cardholding members' accounts and assets while not adversely affecting their ability to seamlessly conduct their financial affairs.

To combat the ever-increasing sophistication of the people who steal and trade in card and personal identification numbers and other personal information, it now requires virtually constant monitoring of card accounts to spot deviations from "normal" use that can signal fraud.

This would be impossible without the neural networks processors use as the cornerstone of their antifraud efforts. But it still requires expert human judgment—on top of the complex algorithms these networks use to determine use patterns—to determine whether fraud is in progress.

The networks are unequalled in their ability to alert the card processor that there's an interruption in the ongoing pattern of one or many accounts. Judging whether the interruption is a cause for concern is something that requires expert assessment.

More than ever before, we as processors must make changes on the fly to our authorization parameters and neural network strategies as we spot trends that indicate new techniques criminals use.

For example, one area where we watch closely is the activity connected to merchant accounts. We have seen numerous instances where a spike in activity indicates that someone is using the account to test stolen credit card numbers.

It may be an employee of the merchant doing this, or the merchant's account may have been hijacked by a fraud ring. Or, of course, the merchant could be dishonest.

But whatever the reason, when we see that the normal pattern is a handful of daily transactions for that merchant account, and suddenly the activity level spikes to hundreds of transactions in one day, we know immediately there's a problem.

This is just one scenario in use today. Criminals are getting savvier at patiently keeping the volume and transaction size of fraudulent purchases down so they have a longer period in which to work before an atypical pattern is spotted and a move to shut down an account takes place.

The same is true when they restrict their fraudulent use to geographical areas where the legitimate cardholder lives and works. They know that huge purchases on the Internet, at big-box stores, or out of the cardholder's region will always catch the processor's attention, so they pace themselves and are more "strategic" in where they use compromised card accounts.

Countering this requires an ever more granular approach to neural network monitoring and a lower tolerance for transactions that differ from the normal pattern. If fraud perpetrated against a credit union's credit and debit cardholders is going to be minimized, the network and the experts who manage these systems must be vigilant every hour of the day. They must be able to take the steps necessary to block transactions based on the card, the account, the merchant, the region, and any other risk factor.

It's quite likely that some level of fraud will always be with us. But with the continuing use of increasingly accurate tools and strategies, we can keep reducing the percentage of fraudulent card use and continue the long-term downward trend.

With that approach, everyone wins.

[Donna Huppler](#) is vice president, security manager, for [TNB Card Services](#). Contact her at 972-391-6403.

