

Sonar Decision Rules

This is the start of an expensive chain breach. Luckily, the compromised stores are all located in a concentrated area. But the fraud spend, on the other hand, is decidedly national.



Perhaps, you could block transactions far from home.

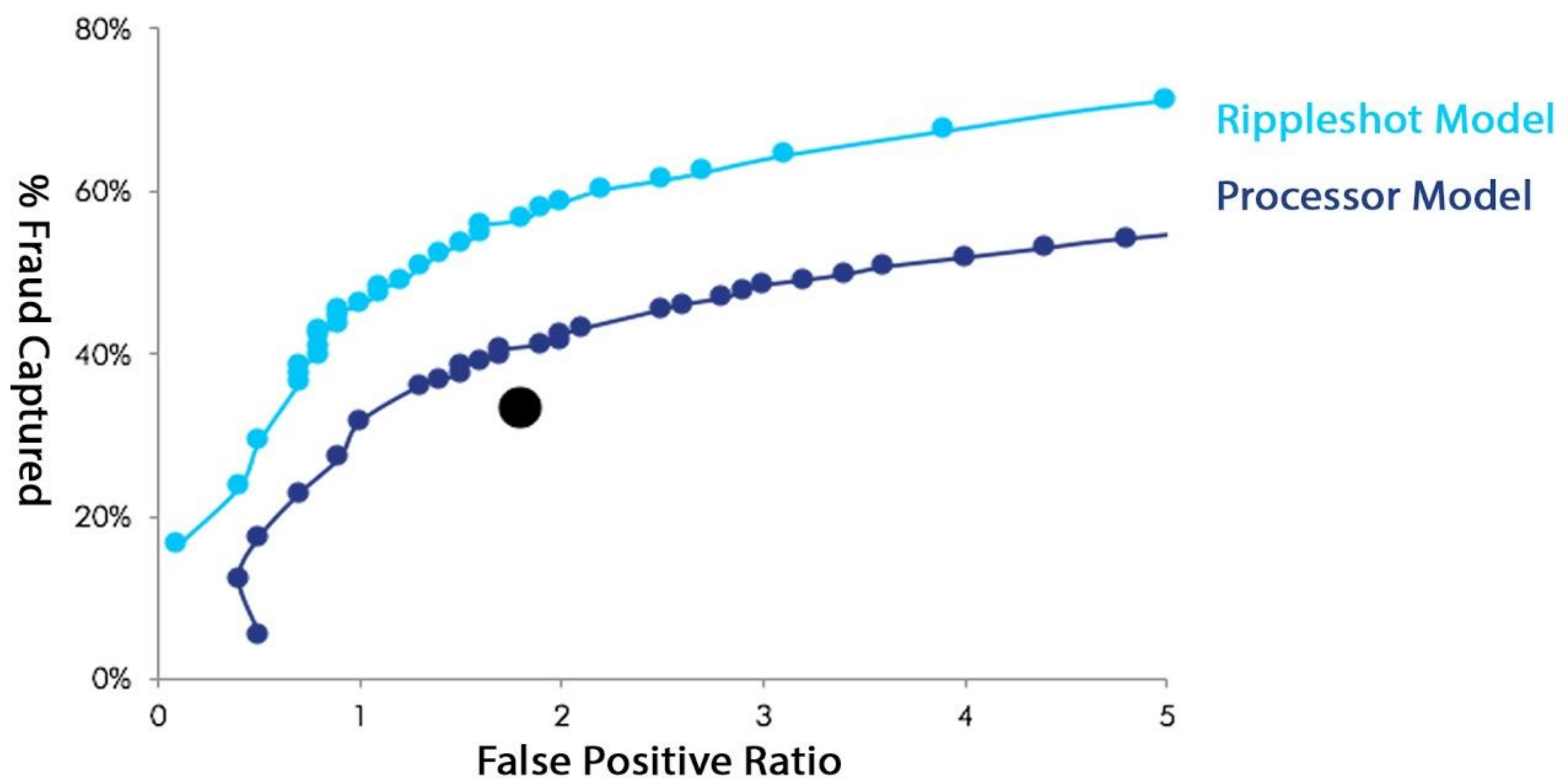
Maybe your analysts are already doing this.

But getting that right requires loads of manual work, and dozens of rules just like this one:

Distance > 150 **OR** undefined
AND
Weekday **NOT IN** Saturday, Sunday
AND
POS Terminal Type ==Mag Stripe
AND
MCC/SIC IN (5541, 5411)
AND
47<NetworkScore<=65
AND
State **NOT IN** (SC, AL, NC, ON, IN, VA, GA, NJ, FL, CT, IL, KY, NV, MD, OH)

Rippleshot has automated rule writing, by providing machine learning generated rules optimized to your data. Most issuers look at their fraud transactions and visually notice some patterns. That's a good start, but humans can miss things. The systematic tree construction employed by Sonar guarantees that we spot the most significant patterns contributing to losses, and write the fewest number of rules to capture the most amount of fraud.

How Sonar's Rules Perform



Using Rippleshot Sonar rules, a client **increased their fraud captured by 70%** - a markable improvement over even the processor-suggested rule set.

