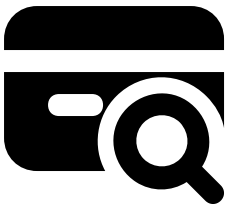
Identifying BIN Fraud

An international bank enlisted 2OS to help spot and stop BIN Attacks. After analyzing the client's data, 2OS identified four new rules that were effective in picking up previously undetected attacks while also minimizing the false positive rate.

What is BIN Fraud

The Bank Identification Number (BIN) refers to the first 6-8 digits of a credit card number. These digits indicate what bank and product type the card belongs to.

BIN Fraud occurs when a fraudster gets hold of a valid BIN and then runs a script to generate the remaining card digits. These kinds of attacks are usually accompanied by a large increase in Internet transaction volume, and serious BIN Attacks can overwhelm call centers and cause reputational problems for banks.



RESULTS

Stop Attacks Sooner

Able to spot BIN attacks early and prevent them from continuing all day

Spot Attacks Across Merchants

Identify cases where fraudsters test card at smaller merchant before moving to a larger merchant for a big purchase

Detect Complex Fraud Algorithms

Can pick up on a variety of advanced algorithms fraudsters might use when running their scripts to cycle through card numbers

Mitigate False Positives

Rules work in conjunction to accurately identify fraud instances without tagging a large number of valid transactions

2nd Order solutions