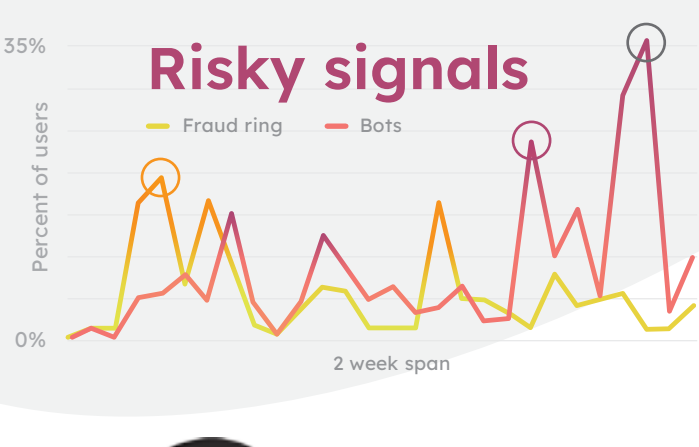
TIMELINE OF A BOT ONSLAUGHT:

What to Do When Half Your Applicants Are Bots

NeuroID

behavioral analytics picked up a bot surge across a consumer financial manager's digital application process.



Orange spikes:
Human risk spikes

Red spikes:
Bot risk spikes

Each one started with a human bad actor testing for weakness, followed by a probe of bots, leading to a flood of bots that lasted for over a week.

Final spike
The set-up pattern of humans ahead of bots became clear, as the fraud-pair worked in tandem toward the huge fraud onslaught.

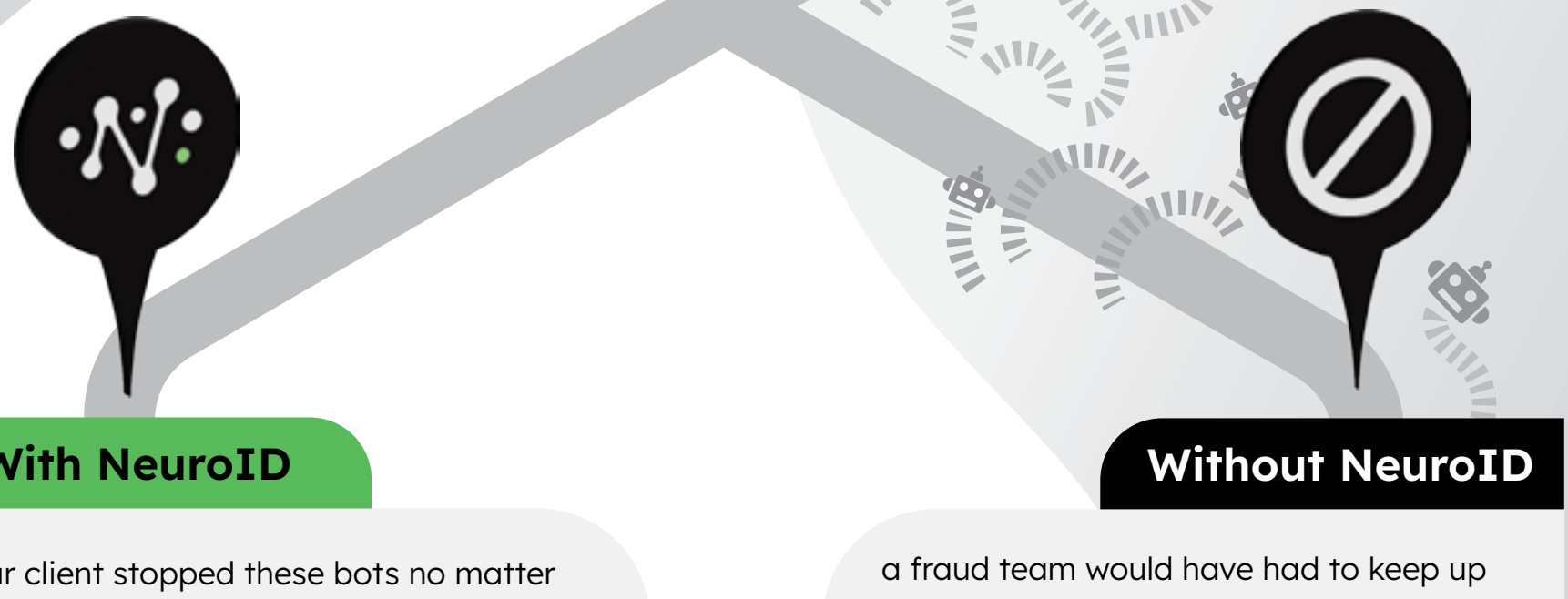
During that week,

50% of all their traffic were bots, nearly triple the bot attack volume

compared to the company's average baseline.

Not only that, but as our customers switched step-ups and controls to adjust one point of entry, the attacks seamlessly changed to another entry-point.

Bad actors were making it past traditional verifications and wouldn't have been caught without the power of behavioral analytics.



With NeuroID

our client stopped these bots no matter how many entry-points they switched to: behavioral traits gave them away instantly.

Without NeuroID

a fraud team would have had to keep up a high-stakes game of whack-a-mole, trying to thwart bots as they switched to a new entry point. Without the behavioral patterns to look for, they also wouldn't have been able to follow trends to find fraudsters who made it past traditional controls.

Want more details on this and other bot trends?

Read our new report, *The Crowd Goes Wild Edition 2: Attack of the Bots*