When Fraud Rings Attack:

DIGITAL INSURERS

neuroID

NeuroID's behavioral analytics enable insurers to target their verification tools on risky cases and reduce friction to known legitimate applicants.

The State of Today's Cybercriminals

The fraud rings targeting digital insurers are extremely cunning, patient, and focused. For example, they often test out different attack strategies to discover how their targets react, and gather as much information as they can in order to land on the best angle of assault. By the time a fraud ring truly attacks, they've already poked holes in the identity verification tools the insurer relies on—and know exactly how to break through at full-scale.

This attack strategy is part of why fraud rings are so difficult to detect. You might have a reassuringly consistent level of fraud attempts, then out of nowhere get hit by a brutal ring that blitzes in to overwhelm your system. And it's never a one-and-done: As soon as they find a weakness, they'll double down and squeeze it as much as they can.

That's what happened to a recent client of NeuroID who was in the midst of implementing a more multi-layered behavioral fraud prevention strategy when . . .

The Client

This digital insurer had tried identity verification step-up methods—resulting in a 10% decrease in low-risk applicants from the increased friction, with no real fraud prevention benefits. While the digital insurer was continuing to test the best way to deflect bad actors and streamline good customers, a fraud ring saw their opening.

The Attack

High-velocity, high-efficiency behavior patterns indicated likely fraud ring activity, with an almost 5x increase in risky session tags (up from 2% to nearly 10% in just three days). Understandably, the digital insurer imposed more onerous identity verification steps in order to try and curb some of the impact.

The Impact

Unfortunately, there were unintended consequences. Before NeuroID's behavioral analytics, blunt force step-up identity verification methods applied to all traffic, reducing genuine applicants and top-line revenue; potentially costing more in losses than actual fraud.

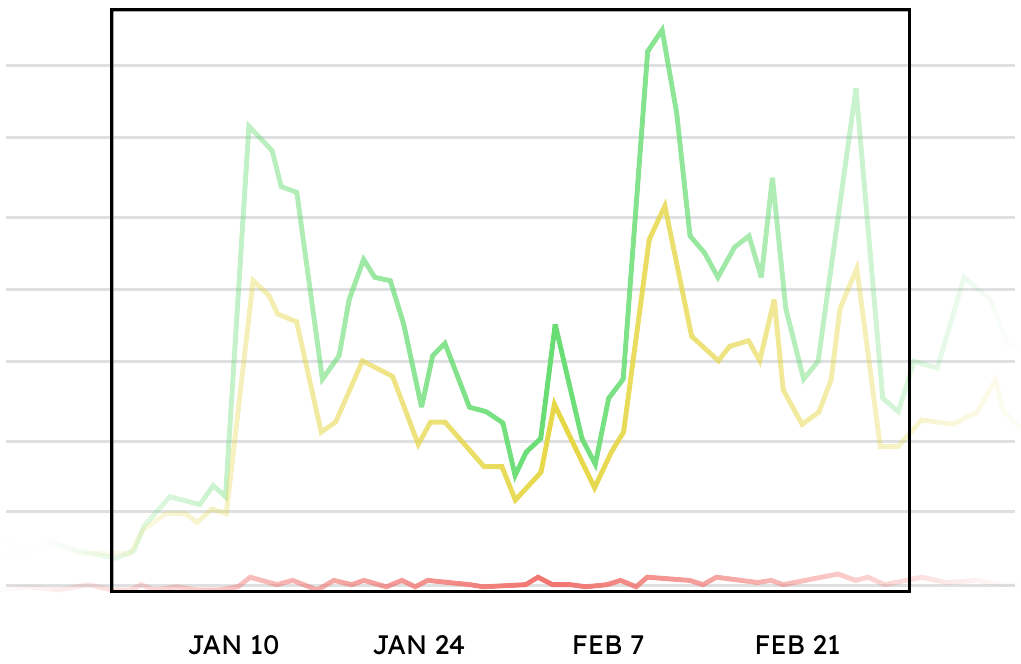
The NeuroID Solution

An increase in step-up verification, if done improperly, can reduce genuine applicants without deterring fraudsters. Fraud rings might still get through if a digital insurer doesn't have the ability to do additional user pre-screening at scale, ideally prior to application submission.

By analyzing how data is inputted into forms in real-time, NeuroID's behavioral analytics enable insurers to target their verification tools on risky cases and reduce friction to known legitimate applicants.

Case studies describe our past work on real cases, but are not intended to guarantee that current or future customers will achieve the same results.

Increased Identity Friction Can Reduce Genuine Applicants



Want to learn more? Schedule a Demo with our insurance specialists.