

# When Fraud Rings Attack:

## O N L I N E L E N D E R

How ID Crowd Alert™ locked out an aggressive fraud ring of 2K+ cybercriminals and caught them before any real damage was caused.



aggressive & coordinated attack



proactive detection



high-cost loss prevention

### The Client

This online lender was expanding their product line to include demand deposit accounts (DDAs). As part of that roll-out, they were still assessing the levels of fraud and appropriate prevention strategy. They knew a high level of fraud attempts was expected, so they were diligently formalizing their automatic step-up standards. Meanwhile, a sophisticated fraud ring was testing their systems—and noted that vulnerability.

### The Attack

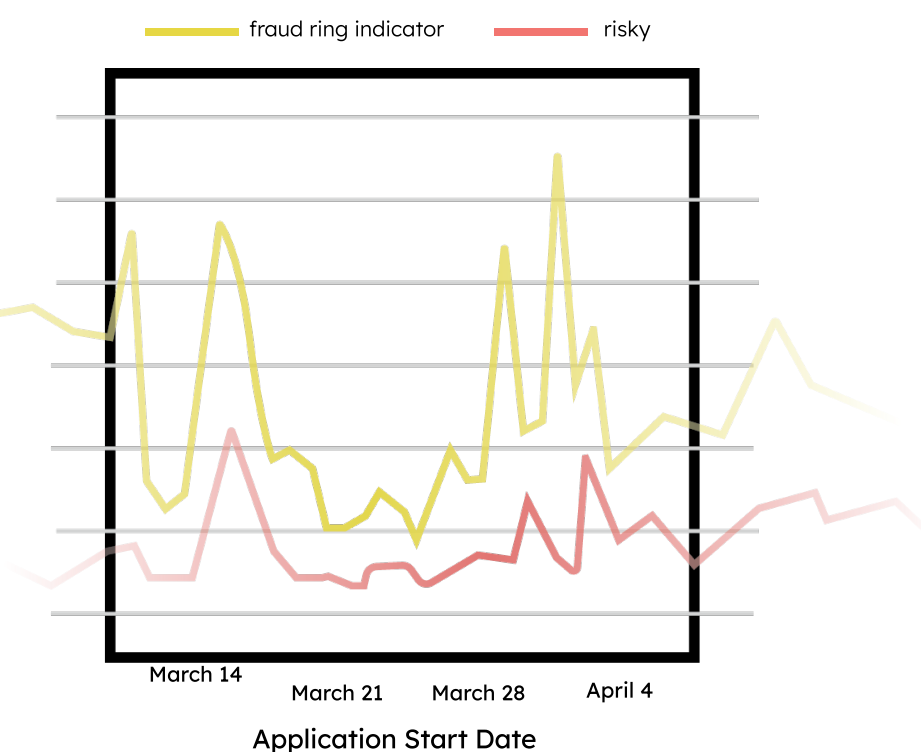
Coordinated fraudsters attempted to open DDAs at a frenetic volume and velocity using stolen PII. This fraud ring had a unique brute-force attack style that far transcended even the high-fraud rate attempts that this lender expected.

### The Impact

Behavior indicated automation beyond typical levels, as more than 70% of users input PII in abnormal patterns. With this high-paced attack clogging the onboarding process, the door was open for any fraudsters making it through to create real damage.

### The NeuroID Solution

The increased velocity of risky traffic spiked ID Crowd Alert's fraud indicators, sounding the alarm that many of these new applicants were unfamiliar with the PII they were entering. ID Crowd Alert also showed that this was likely a highly coordinated attack, with the capabilities for extreme damage if left unchecked.



### ID Crowd Alert™

- ✓ Alerted to a spike in behavior indicating an influx of applicants unfamiliar with the PII they inputted
- ✓ Flagged indicators related to the velocity of the fraud, signifying that this was a coordinated attack that would do exponential levels of damage if left uncontained
- ✓ Behavioral analytics sub-segmented the risky population to look for specific behaviors associated with fraud rings across the risky applicants, providing additional insight into the intent of that fraud

### The Result

The online lender **locked out 2K+ cybercriminals** attacking their system.

Learn more at [neuro-id.com](https://neuro-id.com)