# Reason For Outage (RFO)
# June 27, 2019
# LCR Outage

## Event Summary

On June 27, 2019, thinQ's call routing platform was impacted by a DOS (Denial of Service) incident from 14:55 UTC to 16:49 UTC. Traffic during the period of this event grew in excess of 300% of our normal peak daytime traffic. Additionally, the observed CPS (Calls Per Second) rate was over 500% higher than normal. As a result, our LCR switches were inundated with over 40,000 CPS, which is much higher than our typical peak loads. This incident flooded one of the two data centers that provides outbound termination services.

For the duration of the incident period, this periodically resulted in an inability to place or complete outbound calls, and calls were also dropped. From 15:04 UTC to 15:08 UTC and from 16:07 UTC to 16:42 UTC, no new outbound calls were able to be placed.

## Repair Action

Our engineers immediately began an investigation after notification by our automated alerting system. To alleviate the symptoms of the additional load, system capacity was increased in an attempt to service the additional traffic. During the incident period, we approximately doubled available system resources. Due to the large influx of traffic over a short duration, this action was insufficient to remedy the problem.

Next, the engineering team determined that the massive traffic spike was mostly generated from a single source IP address. Once uncovered, the offending network was blocked and the customer account was suspended. In parallel with taking this action, thinQ's Network Operations (NOC) team contacted the customer by phone and by email to inform them of these events.

The thinQ engineering team has been working hard to improve our network resiliency and redundancy through recent initiatives, including support for DNS SRV and "A" record interoperability. We strongly encourage customers to make this change as soon as possible by following these instructions (PDF).

As a result of this incident, we are also reviewing our ability to rapidly detect and respond to DOS incidents and anticipate further infrastructure improvements.