# TTP Detail – T1496.003

## TTP Information

Name: SMS Pumping

Description: Adversaries may leverage messaging services for SMS pumping, which may impact system and/or hosted service availability.(Citation: Twilio SMS Pumping) SMS pumping is a type of telecommunications fraud whereby a threat actor first obtains a set of phone numbers from a telecommunications provider, then leverages a victim’s messaging infrastructure to send large amounts of SMS messages to numbers in that set. By generating SMS traffic to their phone number set, a threat actor may earn payments from the telecommunications provider.(Citation: Twilio SMS Pumping Fraud)

Threat actors often use publicly available web forms, such as one-time password (OTP) or account verification fields, in order to generate SMS traffic. These fields may leverage services such as Twilio, AWS SNS, and Amazon Cognito in the background.(Citation: Twilio SMS Pumping)(Citation: AWS RE:Inforce Threat Detection 2024) In response to the large quantity of requests, SMS costs may increase and communication channels may become overwhelmed.(Citation: Twilio SMS Pumping)

## Threat-Mapped Scoring

Score: 4.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: impact