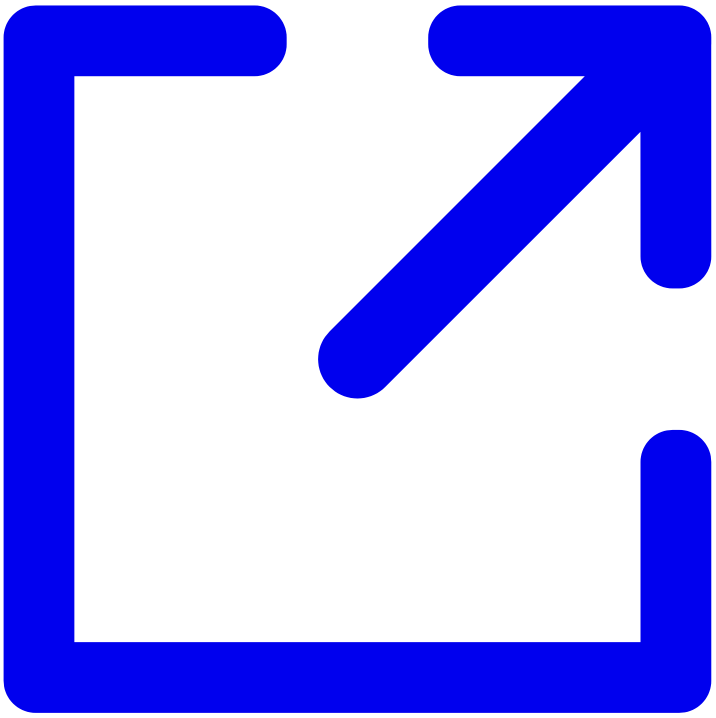
What is SMS Pumping Fraud?

Archived: 2026-04-05 22:25:14 UTC

SMS pumping fraud happens when fraudsters take advantage of a phone number input field to receive a one-time passcode, an app download link, or anything else via SMS. The messages are sent to a range of numbers controlled by a specific mobile network operator



(MNO) and the fraudsters get a share of the generated revenue.

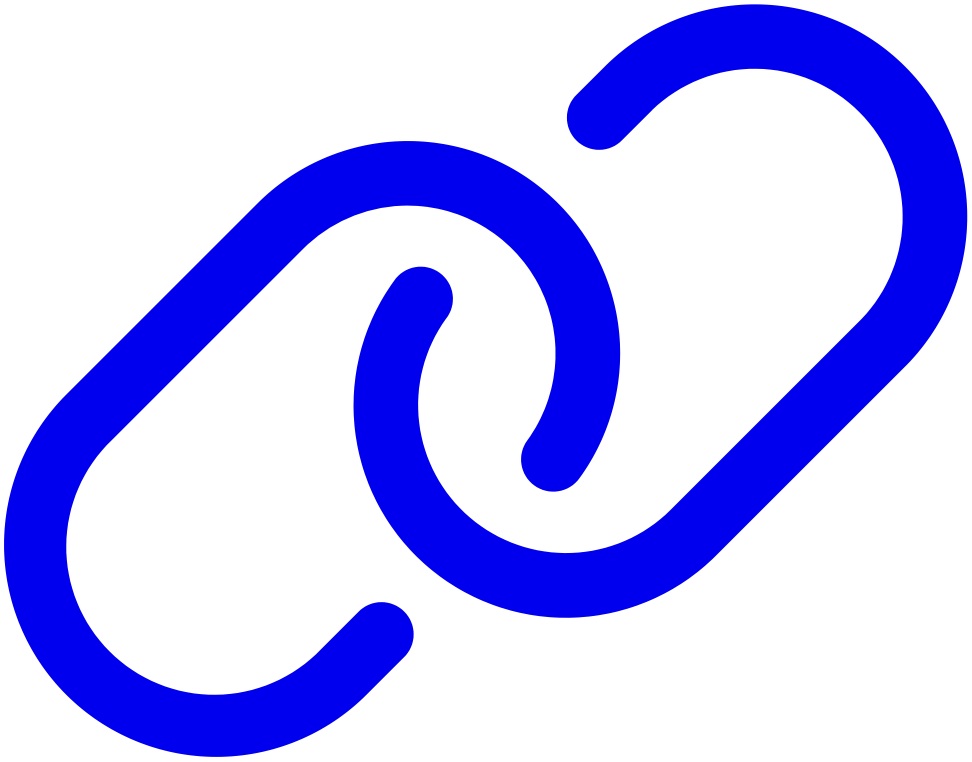
This happens in one of two scenarios:

- The MNO is complicit in the scheme and has a revenue sharing agreement with the fraudsters.

- The MNO is unknowingly exploited by the fraudsters.

In the second case, smaller MNOs get paid by larger MNOs for subscribers and traffic, so a fraudster can create a fake company and promise large amounts of traffic. The MNO may not care what the source of the traffic is and ends up supporting the fraud. In either case, you're more likely to see this type of fraud occur with smaller operators.

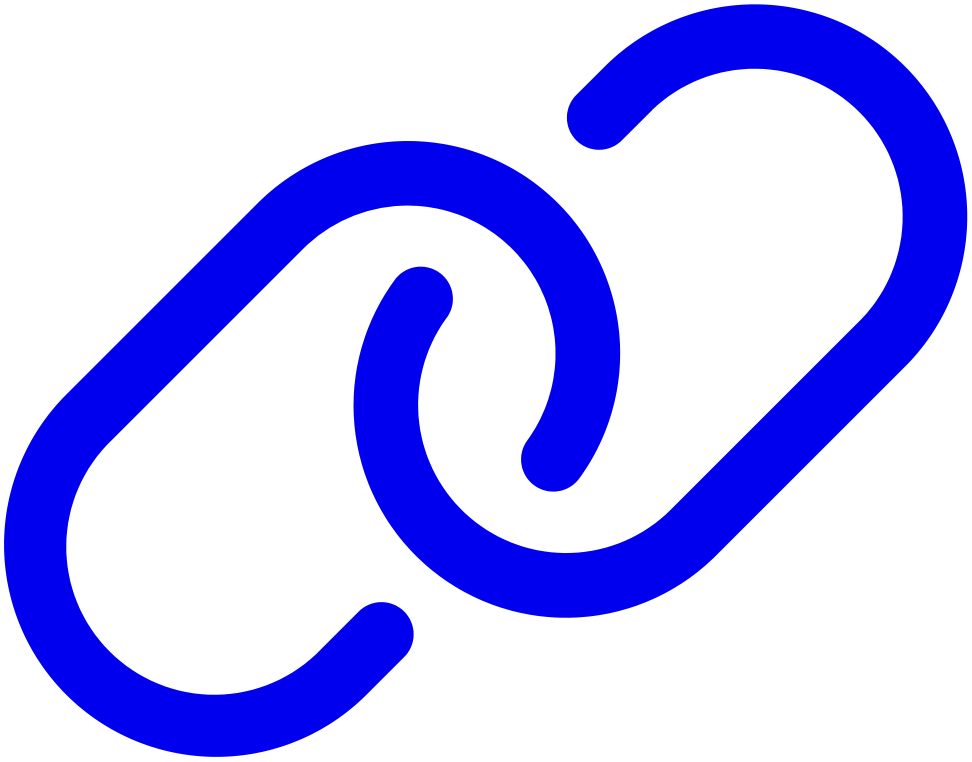
Signs of an SMS pumping attack



You will likely see a spike of messages sent to a block of adjacent numbers (i.e. +1111111110, +1111111111, +1111111112, +1111111113, etc.) controlled by the same MNO.

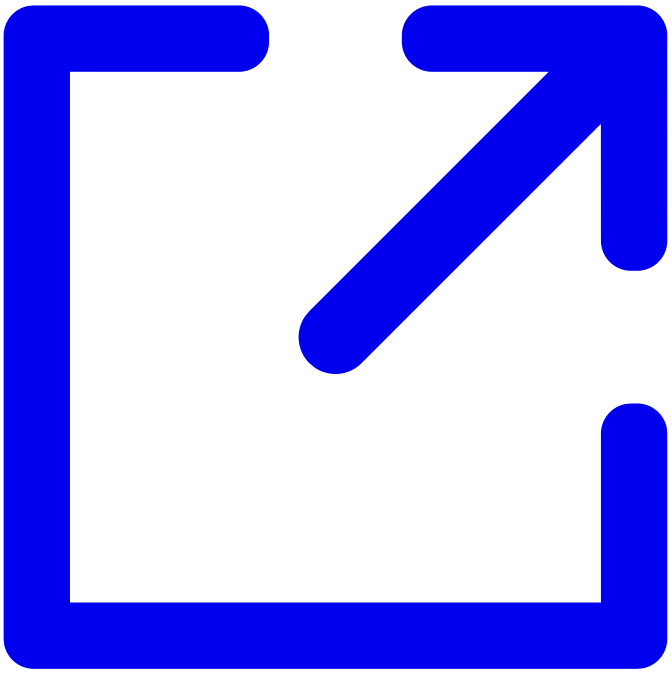
If you're sending SMS for a one-time passcode (OTP) use case, you will likely not see a completed verification cycle.

Fight SMS pumping fraud with Twilio



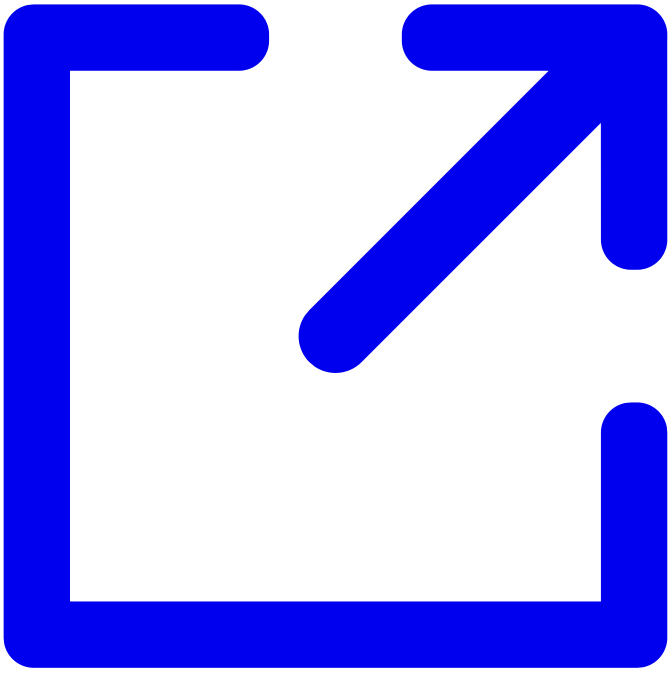
- **Verify Fraud Guard** : Verify is the market leading dedicated authentication and identity solution perfect for preventing SMS Pumping. Twilio recommends enabling the Verify Fraud Guard on your account. When enabled, this feature will block the transmission of suspicious and likely fraudulent SMS messages preventing unnecessary charges to your account.
- **Verify Geo Permissions** : Review your Verify Geographic Permissions and disable all countries that you do not plan to send messages to.

- **Programmable Messaging SMS Pumping Protection** : If migration to Verify isn't possible due to your configuration and you are using Programmable Messaging instead, be sure the SMS Pumping Protection feature is enabled. When enabled, it will block the transmission of suspicious SMS messages.
- **Programmable Messaging Geo Permissions** : Review our SMS Geo Permissions Guide and check the appropriateness of your Geographic Permissions in Console



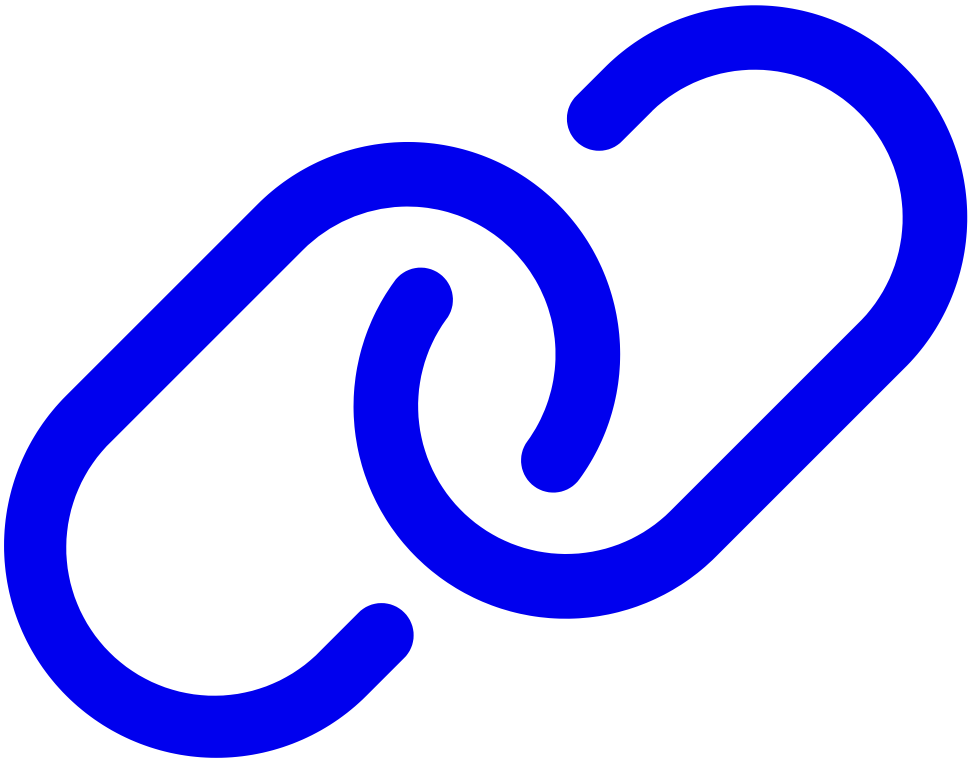
. Disable all countries that you do not plan to send messages to.

- **Lookup Line Type Intelligence** : Use Lookup Line Type Intelligence to get the line type of a number, then only send SMS to mobile numbers. You can also use this API request to determine the carrier and block carriers that may be (knowingly or not) causing inflated traffic. Learn more about how to build a carrier block list with Lookup in this blog post



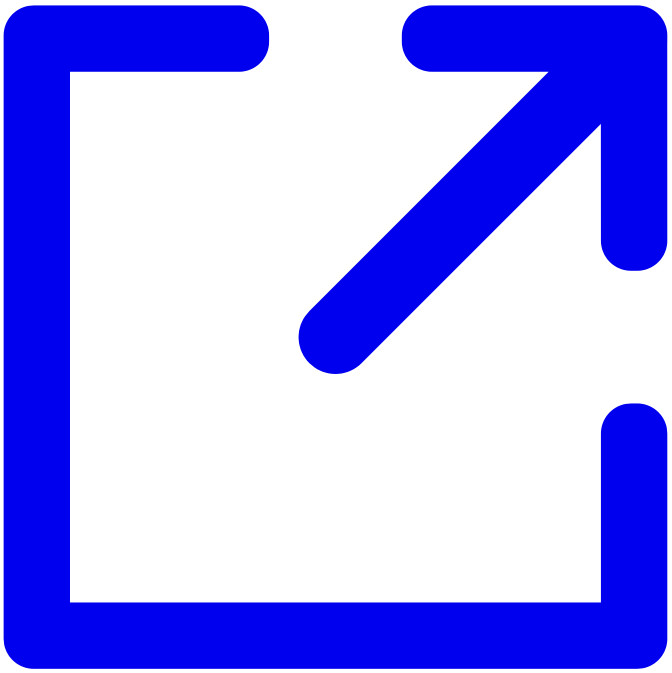
.

Related content



- Verify Fraud Guard
- Programmable Messaging SMS Pumping Protection
- Anti-Fraud Developer's Guide

- Best practices for phone number validation during new user enrollment



- Verification and two-factor authentication best practices
