What Is SMS Pumping Fraud and How to Stop It

By Twilio

Published: 2024-04-10 · Archived: 2026-04-05 19:17:13 UTC

SMS pumping is becoming an increasingly urgent problem for businesses that use SMS messaging channels to communicate with their customers. SMS pumping fraud artificially increases SMS costs, reducing conversion rates. This industry-wide problem affects all providers and is a risk to many businesses.

So what is SMS pumping fraud, and how can your business know if it's been victim to such an attack?

In this blog, you'll learn what SMS pumping is and how it works, along with the ways it can negatively affect your business. Then, discover ways to detect and prevent SMS pumping fraud to protect your organization from an attack.

What is SMS pumping?

Also known as SMS toll fraud, SMS pumping is a type of fraud attack in which bad actors request a high amount of text message traffic from unprotected SMS endpoints. By targeting your automated SMS messaging channels—like one-time passcode (OTP) requests or webform responses—fraudsters can make money from the SMS messages you send them.

Fraudsters target websites and applications that rely heavily on SMS-based OTPs for identity verification and user login. Businesses that typically use OTPs in their user authentication include:

- Banking websites
- E-commerce platforms
- Social media sites
- Ride-sharing or delivery apps

These are just a few examples of businesses that are vulnerable to SMS pumping attacks. Because SMS remains a popular authentication method across various industries, it's crucial to understand the risks and implement robust security measures to protect your organization and customers from this growing threat.

How does SMS pumping work?

In an SMS pumping scheme, attackers use bots to create and send fake OTP requests to businesses. The bots input fake phone numbers into online forms to spoof genuine SMS OTP requests from users. This makes it look like your business is generating real online SMS traffic, but you're paying to send SMS messages to fake numbers that will never result in a sale or conversion.

SMS pumping can be difficult to detect, meaning businesses may unknowingly spend most of their budget on fake "customers."

For example, consider the fictional company PickedClean Organics, a small online business that offers organic product delivery. PickedClean offered promo code for first-time, new customers registering on their website.

When customers confirmed their phone number with an SMS OTP, PickedClean was able to verify one promo code per one real human.

However, a fraudster used automated bots to infiltrate their flow, inserting numerous numbers requesting the SMS OTP. Fraudsters often use a set of phone numbers with similar prefixes.

PickedClean didn't know that many of the numbers were fake, so this influx in requests to set up new accounts triggered many SMS messages, inflating their SMS charges and impacting their overall budget.

SMS pumping fraud had multiple negative effects on PickedClean's business. Below, we'll go over some of the consequences SMS fraud can have on victim organizations.

How does SMS pumping fraud affect businesses?

SMS pumping fraud can negatively affect your business and cause damage, including increasing your SMS costs, lowering conversion rates, and spamming your SMS channels.

Increased SMS costs

When bad actors pump your website forms with fake numbers, your SMS costs increase significantly. Fraudsters can also use fake numbers to trigger a high amount of OTP requests sent to their fake numbers, blasting your servers with SMS requests.

To add insult to injury, the money your business spends on these SMS messages will never yield results. The numbers are fake, and the customers are, too.

Lowered conversion rates

Since you're essentially signing up fake "customers" (bots) or sending OTPs into the void, your user base becomes inflated with "users" who will never convert. This not only artificially lowers your conversion rates, increases cost per conversion, and wastes valuable resources.

Additionally, fraudulent requests can strain customer service by triggering inquiries, and delays in receiving OTPs due to SMS pumping can frustrate genuine users.

In the worst-case scenario, security concerns around fake OTPs might discourage users from trusting SMS verification altogether.

Overwhelmed communication channels

Bots spamming your SMS channels can have a domino effect on your entire system. More than just a slight delay, a surge of fraudulent traffic can overwhelm your resources and lead to these downstream effects:

- Increased downtime: In severe cases, a large-scale SMS pumping attack can even cause system crashes or downtime. This can completely prevent users from receiving any SMS messages, hindering essential actions like logins or password resets.
- Loss of user trust: In an attempt to block fraudsters, businesses may block certain regions or prefixes. This inadvertently can impact real users, frustrating them and causing them to lose trust.

These negative effects can wreak havoc on your organization. But how do you know if your system is getting hit with an SMS pumping fraud? Below, we'll cover the ways you can begin to detect this type of fraud.

How to detect SMS pumping fraud

Now that you know what SMS pumping fraud is, how can you tell if it's currently affecting your business? Detecting SMS fraud can be tricky, but here are four things to look out for:

1. Monitor customer OTP verification

Keep an eye on how many successful OTP attempts come into your system, particularly those sent from countries in which you don't conduct business.

Typically, successful OTP attempts should originate from locations where you have a legitimate customer base. In cases of SMS pumping behavior, fraudsters often use a large pool of phone numbers to trigger OTP requests. These numbers can include international numbers, resulting in successful OTP attempts from countries where you don't have many customers.

2. Track unexpected SMS traffic spikes

Another metric to track is unexpected SMS traffic spikes. Your business will typically send a steady amount of SMS messages weekly. Unless you expect a boost in SMS traffic due to a recent campaign or sale, sudden spikes can indicate bots are targeting your business in an SMS pumping attack with an increased number of OTP requests. SMS fraud bots can use fake phone numbers to request one-time passcodes, triggering a high amount of SMS spend. Again, unless you're expecting a boost in OTP requests, keep an eye out for OTP request spikes.

3. Investigate rapid OTP requests from adjacent phone numbers

A common indicator of SMS pumping fraud is when you receive OTP requests from phone numbers with similar number patterns. For example, you receive 50 OTP requests in a few minutes. The phone numbers are sequential and end in 1000, 1001, 1002, 1003, 1004, and so on.

This is a pretty good sign that a bad actor is trying to get you to send illegitimate messages.

4. Analyze incomplete web forms

Analyzing form completion patterns can help identify automated bot activity associated with SMS pumping. Bots might struggle to fill out forms accurately or consistently, which can be a sign that it is not genuine users submitting your web forms.

How to prevent SMS pumping

Twilio offers several in-house solutions to help prevent SMS pumping. Let's take a look at some security features you might consider to safeguard your business from SMS pumping fraud.

Verify Fraud Guard

Verify Fraud Guard works by analyzing your current and historical SMS traffic for unusual patterns. When Fraud Guard detects fluctuations in SMS destination traffic, aka SMS pumping fraud, it automatically blocks the prefix of the destination of the suspected fraud.

As the first SMS pumping solution to hit the market, Verify Fraud Guard has saved Twilio customers $62.7 million in fraudulent costs between June 2022 and October 2024. Verify also provides a global network optimized for delivery and conversion, multiple channels including push notifications, WhatsApp, voice, and email, and the ability to abstract away the complexity of omnichannel user verification.

SMS pumping protection for Programmable Messaging

If you already use our Programmable Messaging API to send notifications, marketing messages, or other messages, you'll automatically benefit from SMS pumping protection, which has the following benefits:

- It utilizes automatic fraud detection to identify and block SMS messages flagged as suspicious for SMS pumping attempts.
- It analyzes your current and historical SMS traffic for unusual patterns that deviate from your typical messaging activity.

This convenient, built-in SMS pumping protection provides extra security and peace of mind for your business.

Lookup SMS Pumping Risk Score

Lookup SMS Pumping Risk Score employs a unique risk assessment model that considers data from Twilio's network, incorporating signals from Verify Fraud Guard along with other indicators related to risky carriers, unusual SMS traffic patterns, and low conversion rates. This comprehensive approach helps determine the likelihood of a phone number being associated with fraudulent SMS activities. The Lookup API uses real-time risk signals to detect fraud and trigger step-up authentication when needed.

Other solutions

In addition to these built-in options, you can take additional steps for fraud prevention:

- Consider setting limits like disabling geo permissions for countries where you don't conduct business.

- Set rate limits on messages sent to the same mobile number range or prefix.
- Explore less SMS-reliant options for user verification to reduce your attack surface:
- Email-based OTPs are generally less susceptible to the large-scale network abuse that SMS pumping inflicts.
- Set up an authenticator app that generates time-based one-time passwords. This reduces the need to send SMS.
- Use hardware tokens that plug into your computer and generate unique codes. These are secure from hacking because they are pieces of hardware that a fraudster would need to physically own to hack into a system.

Secure text verification with Twilio Verify

No matter how your business uses messaging, Twilio offers a solution to protect your business from experiencing SMS pumping fraud. Though the amount of fraud each business experiences will fluctuate month to month, Fraud Guard has already protected customers from over 569 million fraud attempts.

Fraud not only affects your company's bottom line, but it can also damage your reputation and customer trust. Learn more about the rising costs of digital fraud. If you're ready to get started with Twilio Verify or want more information on how Twilio can help you prevent SMS fraud, talk to sales today.
