The state of SMS pumping fraud

The rise in fraudulent SMS traffic

December 2023 – v.1.0

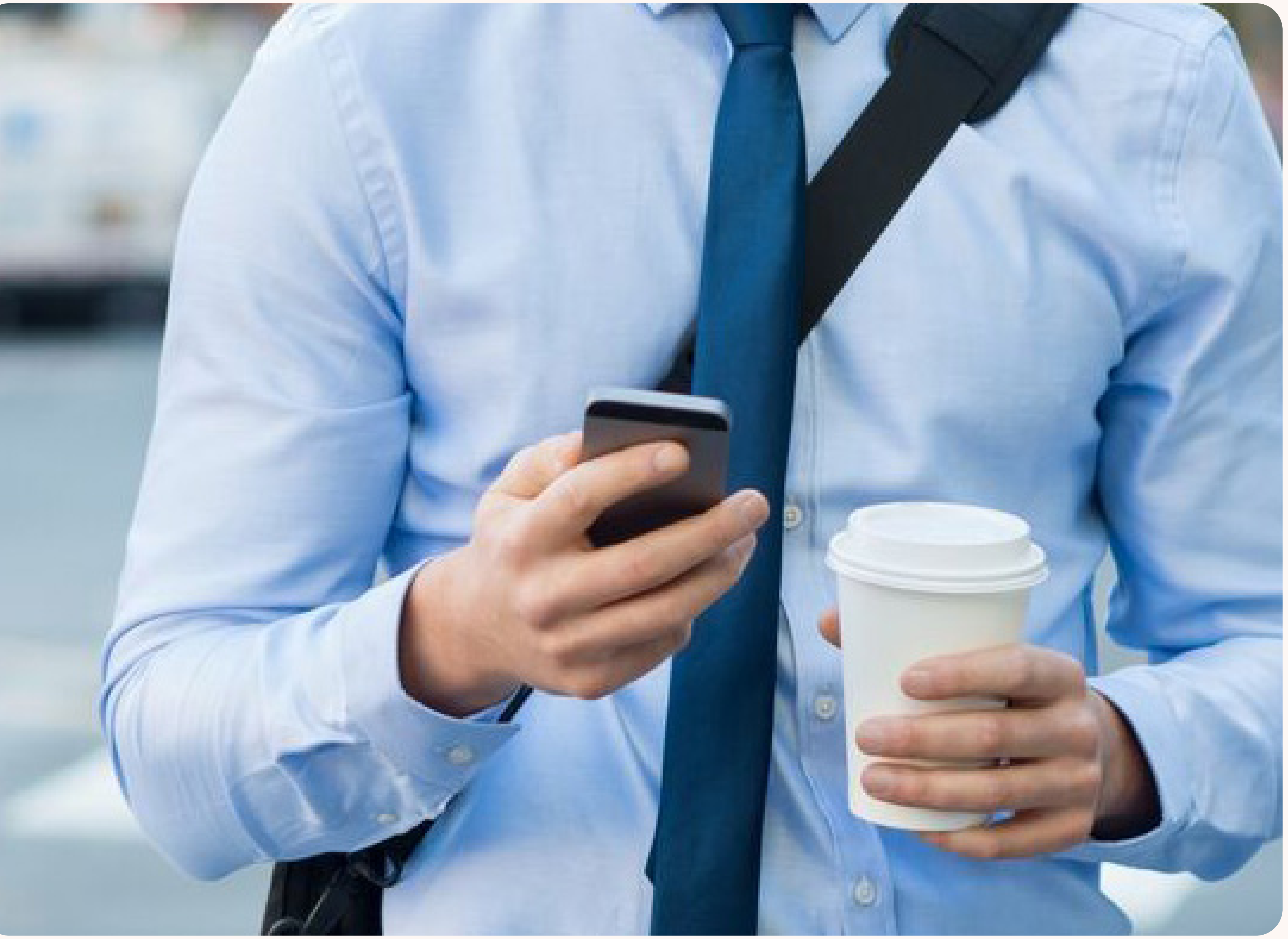
Table of contents

The state of **SMS pumping**

Fraud is one of the biggest concerns for businesses communicating with their customers via SMS. Sudden surges in fraudulent messages can result in significant unexpected costs. However, new technologies leveraging the power of AI can help businesses mitigate the risks of SMS pumping fraud and prevent these wanted expenses.

If you're in a role responsible for managing your company's SMS messaging, such as a product manager or engineer, you may find yourself faced with combatting SMS pumping fraud. In this guide, we will discuss the current state of SMS pumping and its impact on the messaging ecosystem, based on the data and insights we see from our messaging traffic at Twilio in October 2023, and share some strategies on how to protect your business from SMS pumping.

What is SMS pumping?



SMS pumping fraud, also known as Artificially Inflated Traffic, is a type of SMS fraud where fraudsters take advantage of mobile number input fields on websites or in apps to send messages to numbers they control, driving up costs for the business sending them. The fraudsters then get a share of the revenue from these messages.

This is a problem that exists across the messaging ecosystem and that businesses of all sizes and industries face, regardless of their SMS provider. At Twilio, we see that 1.1% of SMS global traffic* is SMS pumping, meaning that billions of messages sent every year could potentially be fraudulent.

One Twilio customer who uses Twilio Verify to send OTPs saved $150,000 by preventing SMS pumping traffic. They were able to accomplish this by enabling Fraud Guard, as well as monitoring their conversion rates and using WhatsApp in place of SMS in regions where they saw higher conversion on WhatsApp.

*Data for October 2023

What is the impact of SMS pumping on businesses, fraudsters, and other players?

The key players in SMS pumping schemes include:

- Fraudsters - the users sending many messages to numbers they control. They are taking advantage of phone number input fields on websites or in apps, such as for one-time passcodes, promotional codes, or app download links, and then get a share of the fraudulently generated revenue from the MNOs.
- Mobile Network Operators (MNOs) - the carriers who are getting additional revenue from the fraud schemes.
- Businesses - those sending the messages to the numbers inputted into their mobile number input fields. They are paying for each message sent.

The mobile network operators and fraudsters benefit from these SMS pumping fraud schemes, as the MNO earns revenue from the messages sent and the fraudsters get a cut of those revenues from the MNO. This is to the detriment of the businesses sending the messages, because they are paying for additional messages to users who will not ultimately convert.

Key use cases targeted by SMS pumping

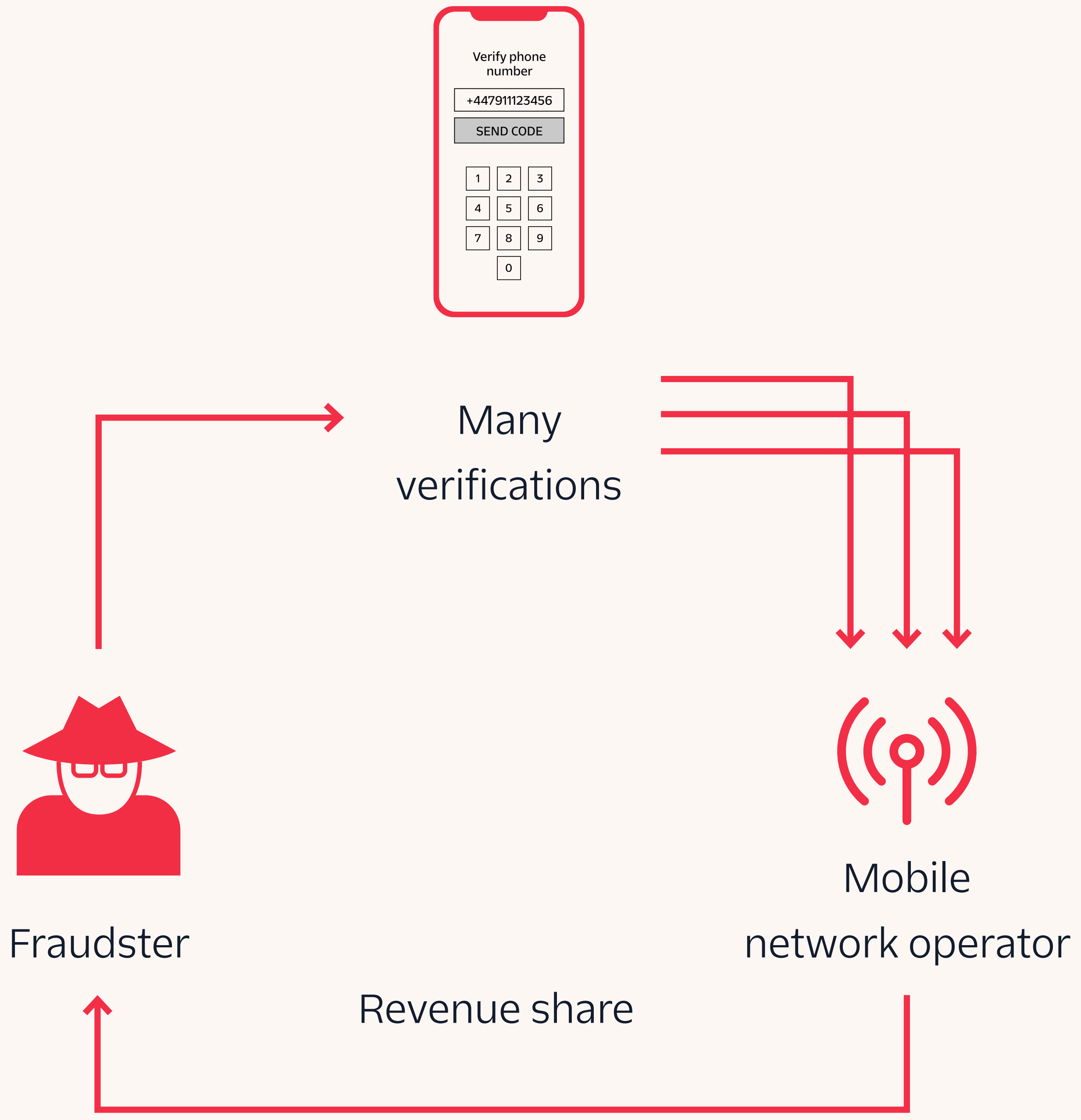
As discussed, fraudsters take advantage of phone number input fields for their SMS pumping schemes. The use cases that are most at risk for SMS pumping are those that utilize these open fields to send an immediate SMS message. The primary use case that experiences SMS pumping fraud is onboarding and verification, followed by marketing and promotional messaging use cases.

User authentication & identity

This is the primary use case targeted by SMS pumping. Businesses send users one-time passcodes (OTPs) to sign up, log in to their accounts, and complete transactions. Fraudsters take advantage of this by having these codes sent to numbers they control.

Marketing & promotions

A secondary use case at risk of SMS pumping fraud is marketing and promotional messaging. This occurs when businesses offer a mobile number input field to send a customer a unique discount code or a link to a product, for example.



Many verifications

Fraudster

Mobile network operator

Revenue share

SMS pumping **trends**

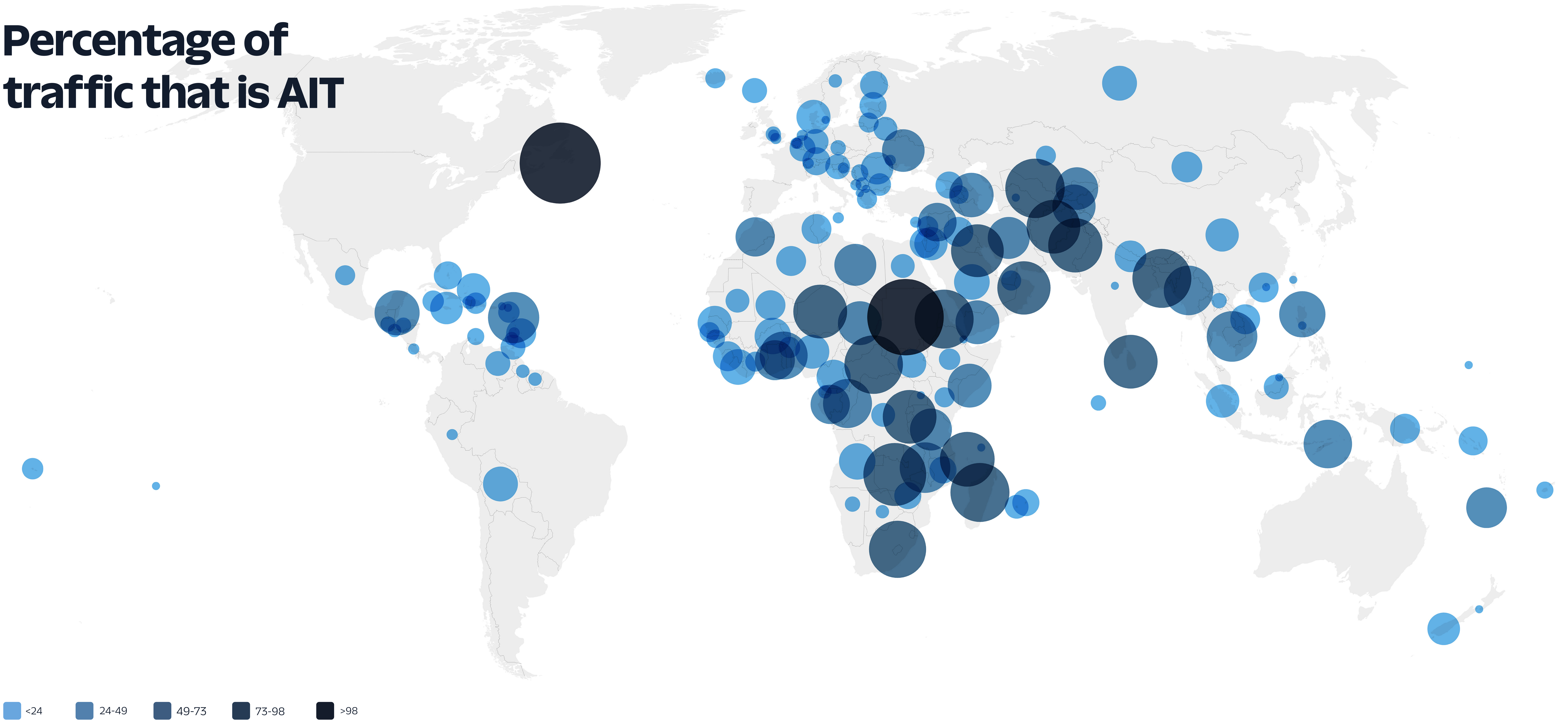
SMS pumping is an increasing problem that many businesses face

Upon audit, Twilio saw that 1.1% of the global SMS traffic was SMS pumping in October 2023, and when you exclude the US and Canada, where this isn't as much of an issue, 5.4% of all international traffic was SMS pumping. The Mobile Ecosystem Forum estimates that by 2025, 2.62 trillion A2P SMS messages will be sent each year, which means that every year billions of messages being sent are potentially fraudulent, creating a big problem for businesses.

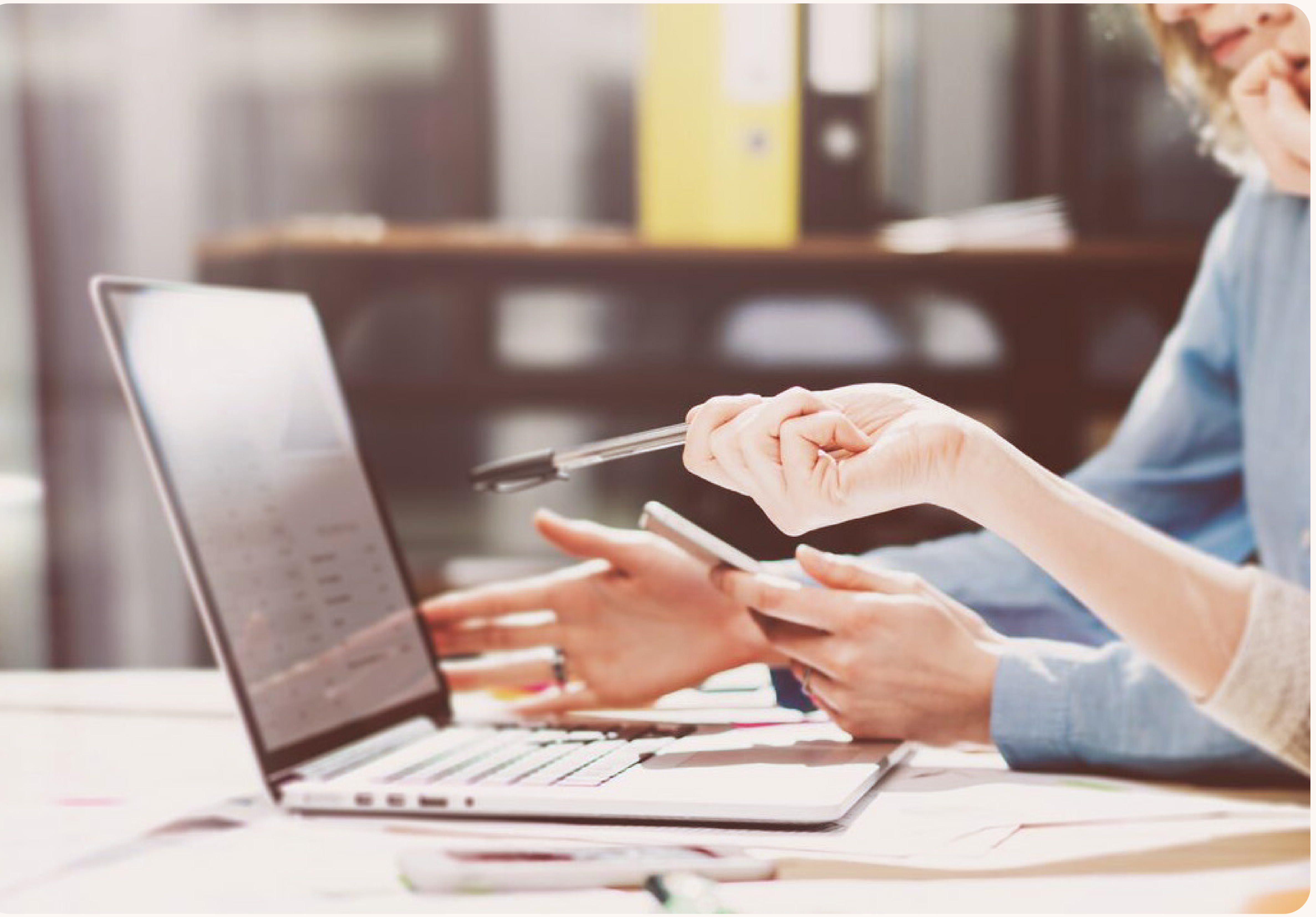
Global businesses need to be aware of regions where SMS pumping is more prevalent

SMS pumping is a global problem, but if a business is operating in certain regions or countries, they may be more at risk for SMS pumping fraud. Based on our data, we see that countries in Africa and the Middle East experience a higher rate of fraudulent traffic. Businesses that operate in regions that experience a higher rate of SMS pumping should consider taking additional measures to prevent fraud.

Percentage of traffic that is AIT



Strategies to **mitigate the risks** of SMS pumping fraud



Monitor conversion rates

For one-time passcodes, track the rate at which users who request a code convert. If you see a drop in conversion rates, that's a good indicator to look into whether you may be experiencing SMS pumping fraud, which can cause a decrease in conversion rates.

Twilio Verify Fraud Guard includes the Verify SMS Fraud Insights dashboard, which enables users to track allowed verification attempts, fraud blocked attempts, success rate, and estimated cost savings. This allows you to see whether there are any unusual trends that could indicate increased fraud.

Those who are using the Feedback API along with Twilio's Programmable Messaging API get an OTP Conversion Report to track OTP Conversions as well as OTP Messages Attempted. This allows users to monitor their OTP conversion rate and take action if a downturn occurs, such as enabling SMS Pumping Protection to block SMS pumping with the Programmable Messaging API.

Set geographic limits

Certain countries or regions are more likely to experience SMS pumping fraud. A good way to prevent SMS pumping is to use geo-permissions to disable messaging in countries where you do not do business. This ensures you don't experience any unwanted messaging in those markets, and you can always re-enable messaging to those countries if your business strategy changes.

For example, Twilio Verify has Geo Permissions which enable you to prohibit or enable sending messages to specific countries, so you can block countries where you do not do business. This enables you to prevent any fraud that might occur in that market. Users can also set geographic permissions for Programmable Messaging.

Use rate limits

Another strategy for mitigating SMS pumping fraud is to utilize rate limits. This gives you the ability to set a maximum number of messages you want to send to the same number or mobile prefix in a minute, which lessens the number of messages fraudsters can send, reducing the potential fraudulent costs. SMS providers like Twilio enable you to set rate limits for your messaging.

Check whether a phone number has been used in fraud schemes

If you want more granular control over whether to block traffic to a particular number, you can inform your risk engine, with the SMS Pumping Risk Score in Twilio's Lookup API. This API provides you with a score for the risk that a phone number has been involved in SMS pumping. This way, you have additional information to make your own decisions about what traffic to block or allow for a given use case, region, or to align with your business strategy.

Enable machine learning-driven SMS pumping detection and prevention technology

Thanks to the power of AI, more advanced SMS pumping prevention technologies are now becoming available. These tools use historical data and machine learning to analyze traffic and automatically detect and block SMS pumping fraud. This helps to mitigate the risk of SMS pumping without you needing to take additional action once the feature is enabled.

Twilio Verify Fraud Guard provides 100% guaranteed protection from SMS Pumping fraud, included in Twilio's purpose-built API for verification use cases. From its initial availability in May 2022 through October 2023, Verify Fraud Guard has saved customers more than US$40.2 million in fraudulent costs by automatically preventing SMS pumping fraud.

And for non-verification use cases or those looking to manage their own phone number pool, Twilio now offers SMS Pumping Protection built into the Programmable Messaging API to automatically detect and block SMS pumping traffic.

US$40.2M+ saved with Twilio Verify Fraud Guard

Conclusion

Although the trends related to SMS pumping illustrate how big of a problem this can be for businesses, thankfully there are a variety of strategies businesses can turn to to prevent SMS pumping fraud. Get started with Twilio today to unlock the benefits of Verify Fraud Guard and our other tools to block SMS pumping.

Empower your business against SMS pumping

Explore Twilio's Advanced Fraud Guard Solutions. Discover how our cutting-edge technology and industry-leading expertise can help protect your SMS communications from SMS pumping attacks.

Get started today.

twilio

Today’s leading companies trust Twilio’s Customer Engagement Platform (CEP) to build direct, personalized relationships with their customers everywhere in the world. Twilio enables companies to use their communications and data to add intelligence and security to every step of the customer journey, from sales to marketing to growth, customer service and many more engagement use cases in a flexible, programmatic way. Across 180 countries, millions of developers and hundreds of thousands of businesses use Twilio to create magical experiences for their customers.
For more information about Twilio (NYSE: TWLO), visit: www.twilio.com.