Whitepaper

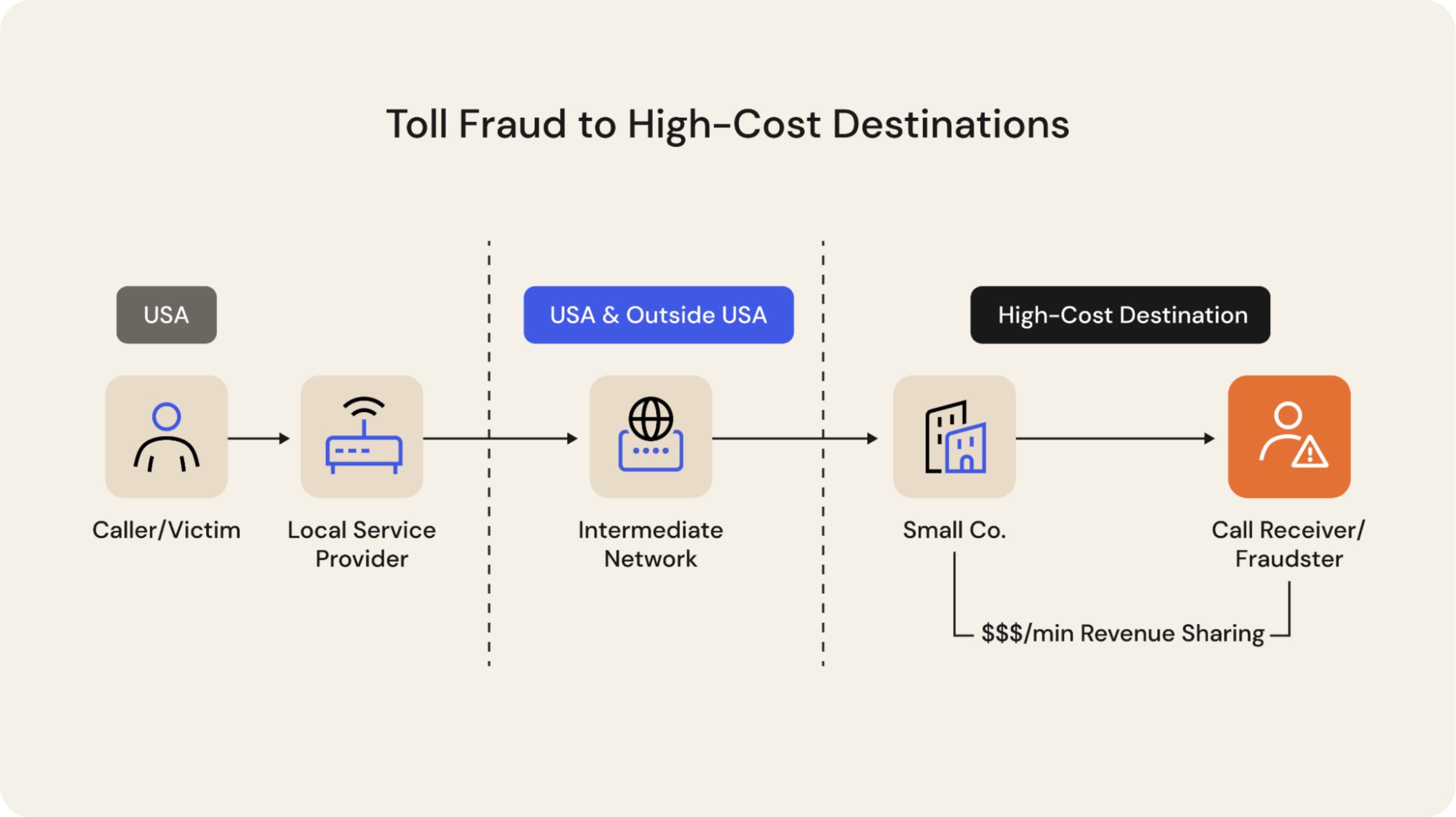
Handling toll fraud and SMS pumping with Twilio in Auth0

Contents

Overview

Phone usage is highly prevalent in today's business world. We spend a lot of time on our phones, and they're convenient, therefore, it makes sense to integrate various processes with them. On one hand, conducting business on a cell phone makes things easier and boosts user adoption, but on the other hand, it raises the chance of fraud. In this whitepaper, we'll discuss the types of fraud that can occur and how to prevent them.

At Okta, we recognize that using a phone number as an identifier facilitates user adoption and simplifies the overall process.That being said, we also recognize that when we integrate telephones into the operations of our businesses, we open ourselves up to two distinct sorts of fraudulent activity.



01

Toll fraud

Hackers frequently focus their attention on phone verification or two-factor authentication routines, intending to create a large number of voice calls to premium-rate lines. Toll fraud involves gaining unauthorized access to premium-rate or international phone services and primarily targets the voice communication sector. Calls made using fake information result in significant financial losses for service providers because criminals take advantage of security flaws in the telephone infrastructure.

Common motivations behind toll fraud

Financial gain

The primary motivation for toll fraud is often financial. The perpetrators are motivated to cut costs for either themselves or the organizations they work for. Consequently, they look for ways to use communication services without having to pay for them or in an unauthorized manner.

Organized crime groups

Toll fraud is linked to organized criminal groups in certain instances. It’s one tactic crime syndicates use as part of larger schemes to launder money or finance additional illegal activities.

Covert operations

It’s possible for individuals with malicious intent or state-sponsored actors to commit toll fraud for espionage. Intercepting calls, gathering sensitive information, and monitoring specific targets are all possible once they’ve gained unauthorized access to communication systems.

Phishing and social engineering

Toll fraud can also be a component of more comprehensive attacks, such as phishing or social engineering. Perpetrators may engage in social engineering tactics to coerce victims into providing access credentials or other information that enables them to commit their crimes.

02

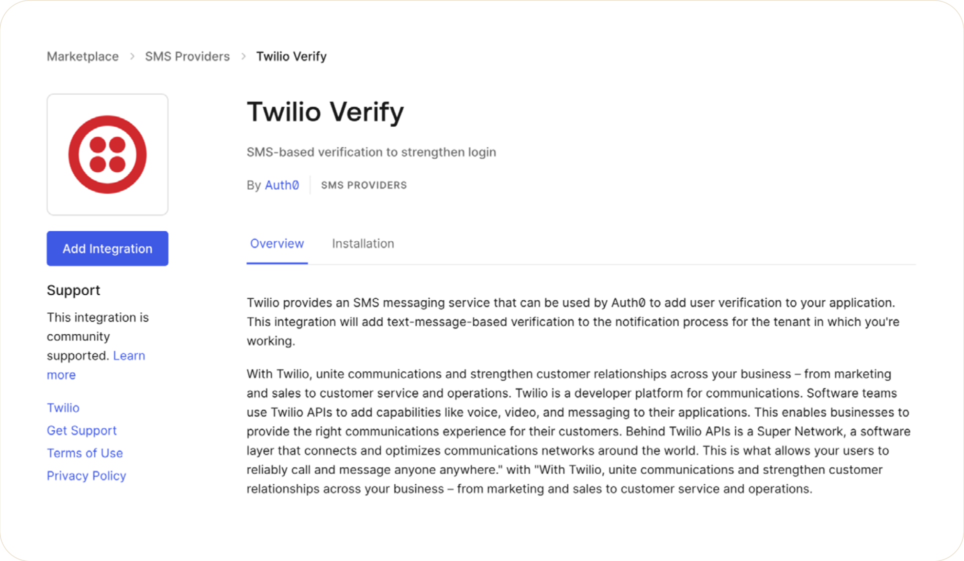
SMS pumping

SMS pumping occurs when fraudulent people take advantage of a phone number entry box to receive a one-time passcode or any other information via text message. Attackers can exaggerate traffic and abuse your application if this form doesn’t have sufficient safeguards.

The practice of pumping SMS is a unique hazard to mobile networks. Hackers take advantage of SMS system vulnerabilities to send a large volume of premium-rate SMS messages, often at the expense of customers who aren’t aware they’re being victimized. This behavior almost always involves automated methods, and it frequently causes people to suffer sizable financial losses.

How to use built-in integration with Twilio

The Okta Auth0 includes out-of-the-box integration with Twilio and comes pre-built. You can quickly connect the two platforms using this integration, which does not require you to install any code. Twilio provides security measures to prevent these types of fraud.



Marketplace > SMS Providers > Twilio Verify

Twilio Verify

SMS-based verification to strengthen login

By Auth0 | SMS PROVIDERS

Add Integration

Overview | Installation

Twilio provides an SMS messaging service that can be used by Auth0 to add user verification to your application. This integration will add text-message-based verification to the notification process for the tenant in which you're working.

With Twilio, unite communications and strengthen customer relationships across your business – from marketing and sales to customer service and operations. Twilio is a developer platform for communications. Software teams use Twilio APIs to add capabilities like voice, video, and messaging to their applications. This enables businesses to provide the right communications experience for their customers. Behind Twilio APIs is a Super Network, a software layer that connects and optimizes communications networks around the world. This is what allows your users to reliably call and message anyone anywhere." with "With Twilio, unite communications and strengthen customer relationships across your business – from marketing and sales to customer service and operations.

Support

This integration is community supported. Learn more

Twilio
Get Support
Terms of Use
Privacy Policy

After establishing Twilio as your service provider and integrating with Okta's Auth0, you may be able to use features offered by Twillio to protect your business from fraudulent activity.

Find out more about how Okta Auth0 works w ith Twilio.

Best practices you can follow with Twilio to safeguard your business

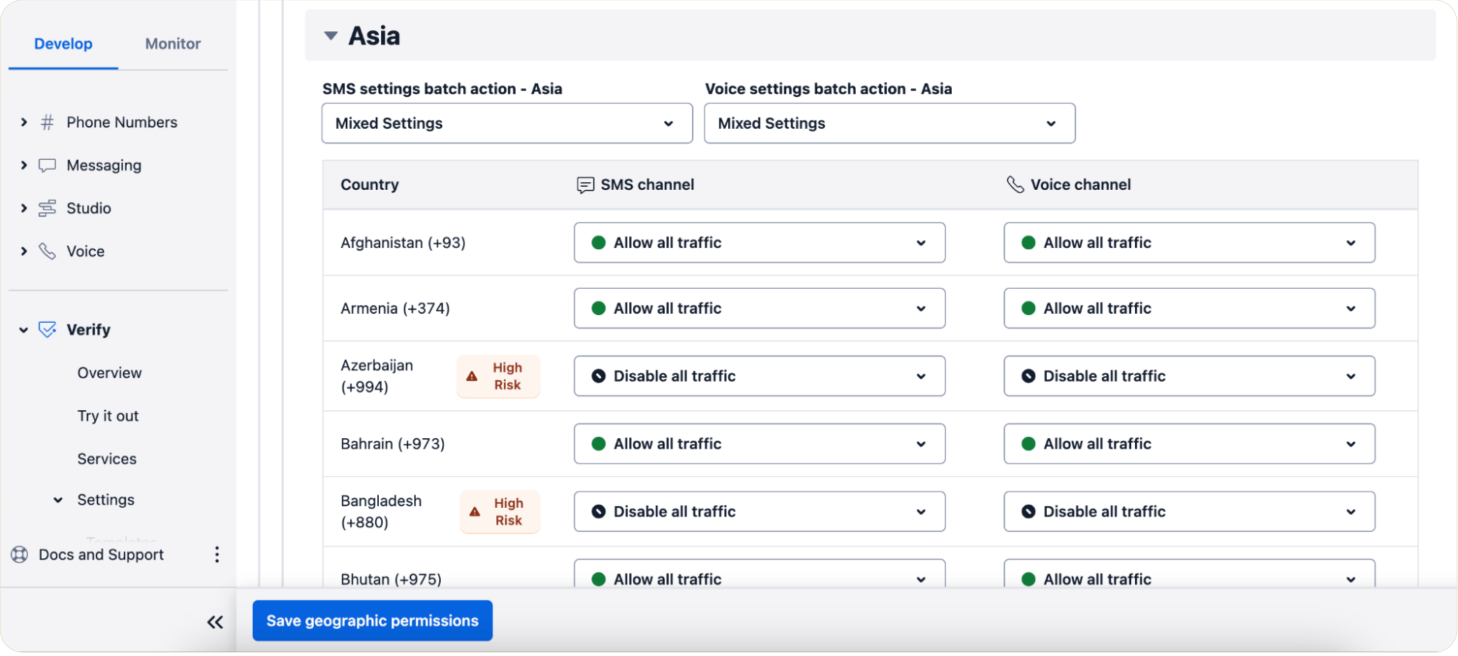
Manage geo channels

Create network channels and classify them geographically based on your user information to determine where traffic is likely to come from. Additionally, you can establish allow and block lists and apply network safelisting. You can also track channel usage and compare projected versus actual usage.

Block risky countries: Manage Geo Permissions

You have several different options available to you in Twilio for managing geographic permissions, and one of those options is through Geo Permissions. Verify Geographic (Geo) Permissions is designed to visually allow destination countries to be blocked or unblocked when sending SMS or voice OTP messages to those destinations. Defining your Geo Permissions can help prevent unexpectedly high SMS or voice costs brought on by malicious actors who create unwanted verification requests.

To enable a destination country, select it from the list (SMS, voice, or both) and then set it to "Allow all traffic" or "Disable all traffic" to block that country. After that, click the “Save geographic permissions” button. For the channel you have not enabled (SMS, voice, or both), any messages sent to countries with the "Disable all traffic" setting will be disallowed.



Asia

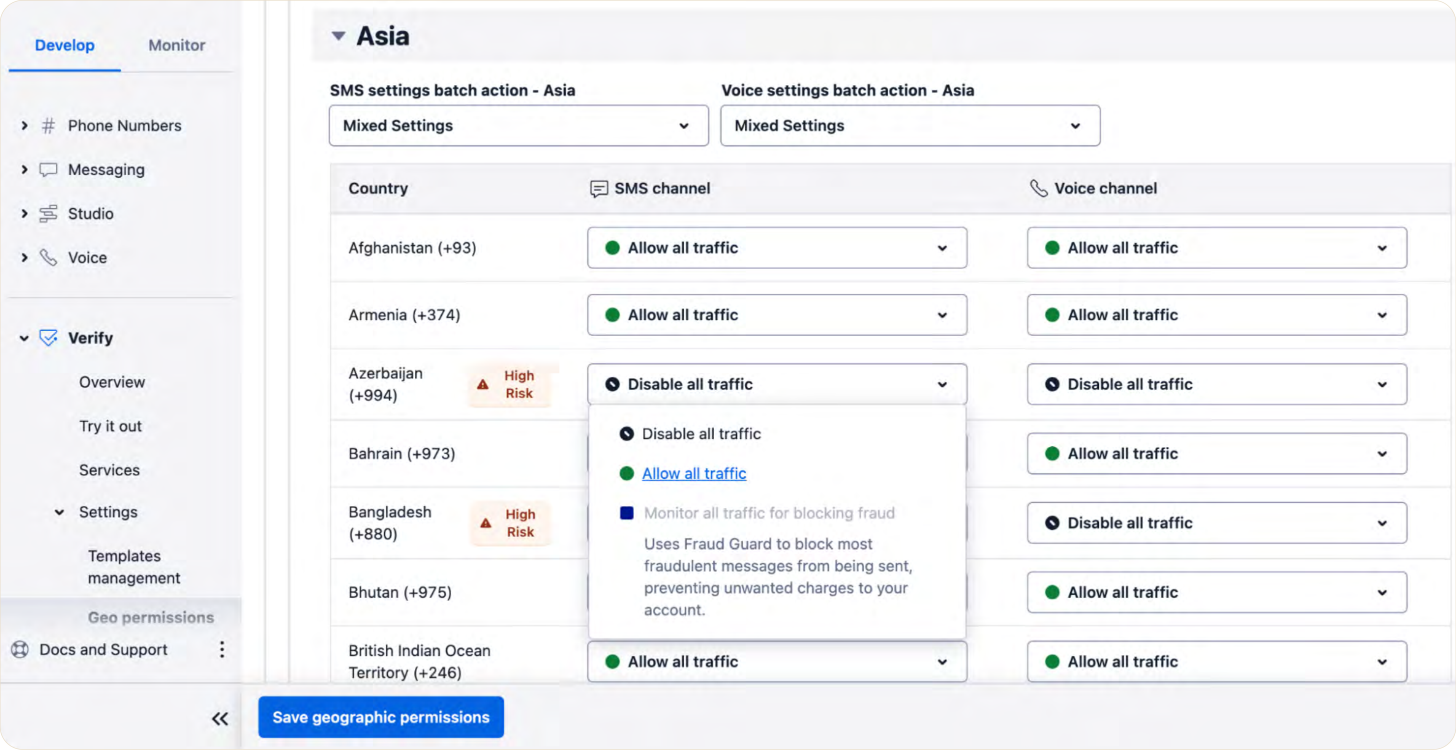
SMS settings batch action - Asia: Mixed Settings

Voice settings batch action - Asia: Mixed Settings

Country	SMS channel	Voice channel
Afghanistan (+93)	● Allow all traffic	● Allow all traffic
Armenia (+374)	● Allow all traffic	● Allow all traffic
Azerbaijan (+994) High Risk	Disable all traffic	Disable all traffic
Bahrain (+973)	● Allow all traffic	● Allow all traffic
Bangladesh (+880) High Risk	Disable all traffic	Disable all traffic
Bhutan (+975)	● Allow all traffic	● Allow all traffic

Verify Fraud Guard

The next way is through Verify Fraud Guard. By selecting "Monitor all traffic for blocking Fraud," the user can activate a country's Fraud Guard. If you don't wish to use Fraud Guard for any country, instead choose "Allow all traffic." When it comes to Verify Geo Permissions, Fraud Guard, also known as "Monitor all traffic for blocking fraud," is set by default for all countries, except certain countries, like the United States, where we observe negligible instances of fraud.



▾ Asia

SMS settings batch action - Asia: Mixed Settings

Voice settings batch action - Asia: Mixed Settings

Country	SMS channel	Voice channel
Afghanistan (+93)	● Allow all traffic	● Allow all traffic
Armenia (+374)	● Allow all traffic	● Allow all traffic
Azerbaijan (+994) ⚠ High Risk	Disable all traffic	Disable all traffic
Bahrain (+973)		● Allow all traffic
Bangladesh (+880) ⚠ High Risk		Disable all traffic
Bhutan (+975)		● Allow all traffic
British Indian Ocean Territory (+246)	● Allow all traffic	● Allow all traffic

- Disable all traffic
- ● Allow all traffic
- Monitor all traffic for blocking fraud
  Uses Fraud Guard to block most fraudulent messages from being sent, preventing unwanted charges to your account.

Learn more about Geo Permissions.

Alternatively, you can use the Twilio Lookup APIs to set the safe or block listing using code.

Understand real traffic vs. bots

Recognize the flow and incorporate a minimal adaptive barrier, such as CAPTCHA, to distinguish between a real user and a bot. Implementations like this will increase resource and user security while saving significant money. These days, bots are relatively common, and if the guardrails are implemented incorrectly, they can easily bring down the system. Many open-source libraries and tools offer these solutions, and they're simple to use.

With Twilio, you can use several libraries and MFA challenges to reduce bot attacks on your network.

Learn more about proper implementation.

Service Rate Limits

To limit the number of calls made in a specific amount of time, set up rate limiting. You should implement call-blocking policies should be to stop calls to known premium-rate numbers. Twilio has built a solution that may set caps or rate limits on several touchpoints, such as those based on user, device identifier, IP, geographical group, tenant, or organization. You can implement Service Rate Limits easily. Rate limits may not stop fraud; however, they'll slow down the attackers.

Learn more about Rate Limits with Twilio.

Smart delays between requests

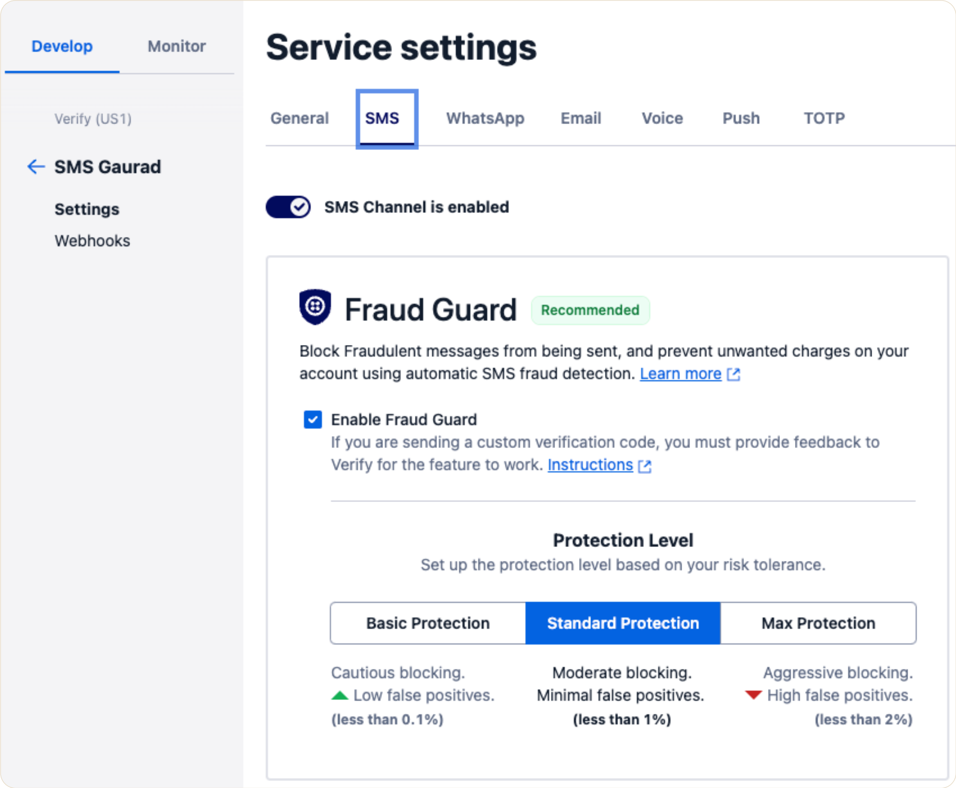
To implement retry logic, apply a smart or exponential delay based on category or number, depending on your user flow. This feature works similarly to Rate Limits, but it lets you and your authorized user continue to utilize the system. For instance, if more requests are generated from the same number, the delay may increase.

Learn more about how you can use retry logic effectively with Twilio.

SMS Fraud Guard

Through the monitoring of your current and historical SMS traffic, this feature of the Twilio Verify product will assist in preventing fraud linked to SMS. This feature will automatically block the prefix of the destination of the suspected fraudulent SMS message whenever there are unusual variations in the patterns of SMS traffic in a certain place.

You can enable this feature under “Service settings” and manage the protection level as per your requirement.



Service settings

SMS Channel is enabled

Fraud Guard

Block Fraudulent messages from being sent, and prevent unwanted charges on your account using automatic SMS fraud detection. Learn more

☑ Enable Fraud Guard
If you are sending a custom verification code, you must provide feedback to Verify for the feature to work. Instructions

Protection Level
Set up the protection level based on your risk tolerance.

Basic Protection	Standard Protection	Max Protection
Cautious blocking. ▲ Low false positives. (less than 0.1%)	Moderate blocking. Minimal false positives. (less than 1%)	Aggressive blocking. ▼ High false positives. (less than 2%)

Learn more about how you can use Twilio to prevent SMS pumping.

Conclusion

There's no question that using a phone number as an identifier provides a significant amount of convenience and speeds up the process of user adoption, allowing businesses to stay ahead of the competition and increase their value. Dangers lurk around every corner, but if companies are watchful about the circumstances in which they operate, they can reduce or even eliminate the associated risks.

SMS pumping and toll fraud are two major risks to the sector. It's crucial to apply the most advanced security controls to defend against these security concerns. The suggested solution combines

a. Monitoring

b. Segregation

c. Rate limitation

d. Bot detection

Out-of-the-box integration of Okta CIC and Twilio can help safeguard the business and keep these threat actors away.

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.