

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

**REVISED CERTIFICATION OF COMPLIANCE FOR
ROBOCALL MITIGATION DATABASE**

Twilio Robocall Mitigation Plan

Twilio¹ hereby submits this Revised Certification of Compliance for Robocall Mitigation Database (RMD) and its Robocall Mitigation Plan (Plan) to the Federal Communications Commission (FCC or Commission). This Plan replaces and supersedes Twilio's previous Plans, which were filed with the Commission on February 24, 2024, and January 27, 2025.

Twilio is dedicated to combating illegal robocalls and fraudulent traffic. Twilio certifies that all calls originated on its network are subject to the Plan as set forth herein, which meet the requirements the of the *Sixth Caller ID Authentication Report and Order*,² including additions of and revisions to the Commission's rules³. Twilio further certifies that no prior Twilio robocall mitigation certification has been removed by FCC action, and Twilio is therefore not prohibited from filing this Plan in the RMD.

¹ In this filing Twilio is used to refer to two entities, Twilio Inc. (FRN 0020-2373-43) and its wholly owned subsidiary Twilio US Technology Inc. (FRN 0028-8448-92). Both entities are listed in the RMD.

² *Call Authentication Trust Anchor*; Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573 (2023) (*Sixth Caller ID Authentication Report and Order*).

³ See, 47 CFR §§ 64.6303(c), 64.6305(d) - (g).

Twilio takes reasonable steps to avoid originating, carrying, and processing illegal robocall traffic, as detailed below. Twilio takes affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, as detailed below. Twilio also has “know-your-upstream provider” procedures in place designed to mitigate illegal robocalls. These practices can reasonably be expected to significantly reduce the origination, carrying, and processing of illegal robocalls.

Mitigation Practices

STIR/SHAKEN: Twilio has fully implemented the STIR/SHAKEN authentication framework on its network and was one of the first service providers to do so, ahead of the mandatory deadline. Twilio’s policies are informed by the “Best Practices for the Implementation of Call Authentication Frameworks” report, released in September 2020 by the North American Numbering Council (NANC) Call Authentication Trust Anchor (CATA) Working Group and the Wireline Competition Bureau’s December 2020 Caller ID Authentication Best Practices. Twilio complies with the STIR/SHAKEN requirements and uses the framework to authenticate and verify calls.

Do-Not-Originate (“DNO”): Twilio blocks calls outbound to the public switched telephone network (PSTN) from phone numbers on DNO lists circulated by USTelecom’s Industry Traceback Group (“ITG”). Twilio also incorporates the SOMOS DNO number list within its network. Twilio blocks the numbers on this list which include numbers reported as inbound only by providers, numbers unused by customers as reported by providers, and numbers designated as inbound only by customers. Twilio regularly queries and updates these lists to ensure the information is accurate and up-to-date.

Analytics and Know Your Traffic (“KYT”): Twilio uses automated detection methods, manual reviews and a combination of manual and automated enforcements to stop and prevent unwanted and fraudulent calls on its platform. Twilio monitors its network for spikes in calls to high-risk routes and uses machine learning models to detect voice fraud. In particular, Twilio developed a machine learning (“ML”) powered system called Tollmaster that automatically detects and alerts Twilio’s operations team of possible fraudulent voice calls. It also triggers automated enforcement actions such as account suspension or call blocking. The system provides interfaces for Twilio’s operations team to manually review and investigate alerts and mitigate traffic via customer outreach and manual enforcement.

Twilio has built its in-house advanced analytical signals to catch bad actors that make fraudulent calls. These signals, among other things, such as change in billing behavior, access patterns and fast ramp up of calling activity together help identify bad actors or when a verified customer’s account has been taken over to make fraudulent calls.

Twilio leverages YouMail's “Watch” service, which actively monitors US phone numbers for illegal robocall activity and provides downloadable details that include evidence of illegal robocalls made with that number. YouMail is known within the industry for its analytics offerings and partners closely with the Industry Traceback Group (ITG), the FCC, and State AG offices who use their services to protect consumers from illegal robocalls.

Twilio also subscribes to and receives RRAPTOR honeypot data, which is used to identify suspicious accounts and take appropriate corresponding action. Incorporating and analyzing this data expedites the process for suspending bad actors from Twilio’s platform and creates outreach opportunities for Twilio to further educate customers about compliance requirements.

Through its RRAPTOR and YouMail honeypot partnerships, Twilio is able to view the actions of its customers within the broader voice ecosystem. Honeypots operate as an early detection tool providing a view into a customer's calling activity and patterns. By analyzing the data these honeypots produce, Twilio is able to detect potentially non-compliant or unlawful activity on its platform, including potential violations related to the Telephone Consumer Protection Act (TCPA) and the Federal DNC Registry. Honeypot recordings provide definitive proof of non-compliant behavior, which allows for swift enforcement on these actors. Twilio investigates the flagged activity and can take a variety of actions to address this behavior including, but not limited to, placing an account in remediation and requiring the account holder to provide a remediation plan addressing the flagged concerns in order to get back in good standing. Twilio may also take enforcement action on the non-compliant account by either disabling voice traffic or suspending the account, which restricts all traffic on an account across both voice and messaging. By proactively monitoring the returns from various honeypot partners, Twilio is able to capture and address non-compliant traffic in its infancy, prior to the initiation of larger or persistent calling campaigns.

Twilio deploys data-driven analysis in its robocall mitigation efforts, using data created from usage of its platform to aid in detection of bad actors. Twilio's Voice Insights tool employs sophisticated anomaly detection capabilities for AI-assisted identification of accounts engaging in suspicious activity. Twilio monitors account specific data points across multiple dimensions and looks at a variety of metrics as indicators of a consumer's willingness to receive the call. These metrics include call completion rates, final SIP responses, and call duration. Twilio then investigates calls identified as suspicious. Twilio also monitors call duration on accounts, in

particular accounts placing a high volume of short duration calls, where the proportion of short calls to total calls rises above a healthy threshold. Accounts with legitimate use cases will be informed and educated to follow best practices for calling based on the data that was analyzed. Twilio conducts a holistic customer account review and includes other industry standard factors such as ASR (answer seizure rate), ALOC (average length of call), SIP errors, and other call and traffic usage anomalies that indicate the overall health of a customer.

Know Your Customer (“KYC”): Twilio’s KYC requirements serve as a gating factor to help prevent bad actors from using Twilio’s platform. Twilio takes a multi-tiered approach to its KYC policies that include customer vetting, restricting initial access to its network, and the use of contract terms that allow for immediate termination when Twilio’s services are abused by new, existing or renewing customers. Twilio built a KYC platform, Trust Hub, to ingest a variety of information about such customers, including the customer’s legal business name, physical address, business type, business industry, business registration number such as tax identification numbers, business regions of operation, website URL, social media profiles, and authorized representatives. Twilio verifies the information provided against public records and private databases and assesses KYC for fraud detection using common signals (e.g., email, phone number, IP addresses). In some instances, Twilio uses a third party service, e.g. Persona, that provides authentication via biometrics (selfies), device and geolocation fingerprinting and ID forgery/ replica detection. The KYC data collected by Twilio is utilized to prevent repeat offenses and mitigate risks associated with malicious actors.

Contractual Provisions with Customers: Twilio’s customers must adhere to the terms of Twilio’s Acceptable Use Policy (AUP)⁴ in order to operate on its platform. The AUP outlines specific prohibited conduct, although this list is not exhaustive. This provides Twilio the

⁴ <https://www.twilio.com/en-us/legal/aup>.

flexibility to apply the AUP to a variety of suspicious behaviors. The AUP also states that customers are responsible for their end users' compliance with the policy. The AUP is part of Twilio's Terms of Service and Twilio Platform Agreements (TPA). In particular, the AUP calls out the following prohibited activities including but not limited to:

- The *Violations of Laws or Standards* paragraph outlines that violating laws, regulations and provider requirements, including ones that impose consent requirements, is not allowed.
- The *Interference with the Services* section prohibits any activity that would negatively impact Twilio's platform/network or third-party networks that are linked to its platform/network (e.g., carrier networks).
- The *Country Specific Terms* section includes obligations for voice service provider customers to register with the FCC's Robocall Mitigation Database and cooperate with Twilio in determining the origin of suspected illegal robocalls.

Twilio maintains a dedicated compliance team to evaluate suspected violations of its AUP or other contractual provisions and take appropriate enforcement action. This includes suspending or terminating services for any customer using its platform to generate illegal robocalls. If a suspension occurs, the customer is notified via email and loses the ability to send any communications, though they may appeal the decision for a formal review by Twilio's operations team.

These policies, together with Twilio's KYC practices, have the effect of restricting the ability of new, existing, or/and renewing customers to originate illegal traffic.

Know Your Upstream Providers: As a non-gateway intermediate provider, Twilio has processes in place intended to ensure that its immediate upstream providers are not using Twilio's network to carry or process illegal traffic. In cases where Twilio serves as the intermediate provider to our customers who identify as a voice service provider (VSP), the customer must be registered in the RMD and sign originated calls using their assigned token.

Twilio collects information from such providers, the same as it does for any of its customers, including their physical business location, authorized contact person, state of incorporation, tax identification number, and business model. These providers are considered Twilio's customers and are contractually bound by the AUP, which prohibits the use of Twilio's services to transmit illegal communications, and obligates them to cooperate with illegal robocall tracebacks, and requires registration in the RMDe.

Collaboration with Industry Efforts: Twilio has sought to be a collaborative partner in the fight against illegal robocalls, as evidenced by its extensive engagement in industry-wide initiatives and participation, such as the Communications Fraud Control Association (CFCA) and similarly-situated industry associations. Twilio participates as a member of the ITG and as a member of the Alliance for Telecommunications Industry Solutions (ATIS), and it has collaborated with industry partners to implement additional upstream customer vetting by requiring more thorough mitigation plans. Twilio continuously evaluates and investigates provider concerns regarding suspicious calling patterns and lack of consent issues.

Robocall Mitigation Database and FCC Enforcement Actions: Twilio does not accept traffic directly from providers not listed in the FCC's RMD. It also monitors the FCC's enforcement actions against companies suspected of illegal robocalls to ensure that those companies are not using Twilio's network. When enforcement notices are released, Twilio checks to ensure that targeted companies are not Twilio customers, or if they are, as permitted by the FCC's rules, it takes steps to ensure that such companies are not originating illegal calls on Twilio's network.

Traceback Commitment

Twilio commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate, carry, or process illegal robocalls.

Attachment A

Information Regarding Twilio Principals

State of Incorporation: Delaware

Headquarters: San Francisco, California⁵

Company Type: Twilio is a publicly traded corporation, trading on the New York Stock Exchange, symbol TWLO.

Twilio Management:

Khozema Shipchandler, Chief Executive Officer
Aidan Viggiano, Chief Financial Officer
Christy Lake, Chief Administrative Officer
Thomas Wyatt, Chief Operating Officer
Inbal Shani, Chief Product & Technology Officer
Chris Koehler, Chief Marketing Officer

Board of Directors⁶:

Jeff Epstein, Chair of the Board
Khozema Shipchandler
Charlie Bell
Donna Dubinsky
Jeff Immelt
Deval Patrick
Erika Rottenberg
Miyuki Suzuki
Andy Stafman
Doug Robinson

⁵ Full address is: 101 Spear Street, 5th Floor, San Francisco, CA 94105.

⁶ Further information on Twilio's Board of Directors: <https://www.twilio.com/en-us/company#board-of-directors>