

COX COMMUNICATIONS, INC. ROBOCALL MITIGATION PROGRAM

Pursuant to 47 C.F.R. § 64.6305(a), Cox Communications, Inc. (“Cox”), on behalf of itself and its affiliated voice service provider operating companies, details the specific “reasonable steps” it has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program and the type of extension it received under 47 C.F.R. § 64.6304.

Steps to Avoid Originating Illegal Robocall Traffic

Cox has adopted several practices to reduce the origination of illegal robocalls on its network.

STIR/SHAKEN Authentication. Cox has implemented the STIR/SHAKEN authentication protocol for voice traffic originating on its IP network platforms and authenticates calls consistent with the FCC’s STIR/SHAKEN rules and policies as delineated in C.F.R. § 64.6301. With respect to Cox business customers, Cox assigns STIR/SHAKEN Caller ID attestation levels for all calls originating on our network based on the attestation level definitions in section 5.2.4 Attestation Indicator in ATIS-1000074.v003. Cox implements multiple checks to ensure that all of its customers are assigned an appropriate attestation level. Regarding its residential customers, Cox contracts with its vendors to assign STIR/SHAKEN attestation levels.

Know Your Customer - Vetting. Cox uses a multi-layer Know Your Customer approach. As an initial matter, Cox does not sell services to international call originators. Cox conducts internal checks to determine whether a prospective customer is a known bad actor based on prior Cox experience. In addition, for Cox residential customers, Cox uses an integrated passive identity and fraud scoring solution during the account opening (buy-flow) process that includes checks against multiple external and internal databases to evaluate identities and assess fraud risk prior to all account openings. Prospective residential customers must provide phone number, email, address, date of birth, and other information. This information is then used to query external, nationally recognized databases to assess the validity of the customer-provided information and produce a digital risk assessment. Cox also uses a solution that consumes the applicant information and queries a list of historical bad actor accounts and high balance bad debt accounts to identify matches or commonalities of the applicant to former fraud.

Cox also vets the identity of its commercial customers by, among other things, collecting information, confirming the physical service address during the installation process, and requiring the email address associated with the account to sign relevant contracts. Additional measures for Cox business customers include vetting of commercial customers at account opening by conducting a comparison of the customer’s business and personal identification information to former account Business and Account Owner information. Cox applies an additional vetting process for all small business customers because, in Cox’s experience, these smaller enterprises account for the vast majority of fraud by former Cox business accounts. Specifically, after new account opening orders are submitted, a back-end process queries the personal and business information against known fraud former accounts and high bad debt balance former accounts. If there is a match to the former fraud/bad debt information, the account and order are sent to the Fraud Operations team for investigation into the customer identity and association to former account fraud. If the investigation results in a confirmed fraud, the account opening, and service order are rejected and the sales and operations teams are notified. If the investigation results in an “all clear,” the account opening and order proceeds. In addition, for prospective small business customers at new account opening, the customer address is checked for serviceability blocks tied to fraud and/or bad debt. If there is a block on the address, the customer is hard stopped and required to verify their identity before completing their order via the Fraud Operations team. The contract signature process is another check for the validity of the email address supplied by large, enterprise customers.

In addition, as part of the onboarding process, Cox salespeople discuss with business customers their general communications needs—for example, if the customer needs a toll-free number so that it can receive inbound customer service calls or has a particular number of employees who make large numbers of outbound calls—to determine the appropriate product mix for an individual customer.

All prospective customers, including non-SIP customers, are provided with a Cox commercial services agreement during the sales onboarding process that they must accept to receive service. The commercial services agreement includes restrictions on use of auto-dialers and other prohibited practices, such as illegal number spoofing. All Cox customers are contractually bound to adhere to Cox's commercial services agreement. Cox's commercial service agreements require customers to comply with all applicable laws, including TCPA requirements, and prohibit misuse of services. Misuse includes, but is not limited to, engaging in "robocalling" or continuous or extensive call forwarding or long-distance abuse; and use of auto dialers, power dialers, any type of automatic outbound dialing or predictive calling/dialing system, or the functional equivalent of any of these systems. Cox's commercial service agreements also prohibit use of services to commit acts of fraud. Cox may terminate any customer for violation of its commercial service agreements. Likewise, Cox residential customers are bound by our residential customer services agreement.

Know Your Customer - Monitoring. Cox monitors voice traffic on the Cox network for anomalies, fraud and abuse, and suspicious traffic patterns. For example, Cox monitors its network traffic for unusual spikes of large numbers of outbound calls and reaches out to impacted customers as warranted. Cox investigates all complaints or inquiries relating to potential illegal spoofing or robocalling. Most such complaints involve spoofing of a Cox customer number by a third party rather than calls originating from the Cox network. Cox may conduct profiling on a per-telephone number basis, looking for patterns, or changes of patterns, of call volume, duration and call destination that may indicate illegal robocalling activity. Cox investigates suspected robocall patterns and acts as necessary, including through suspension and termination of the customer account as permitted by its service terms, contracts, and Acceptable Use Policies.

Know Your Upstream Providers. Cox verifies the registration of potential peering partners in the FCC's Robocall Mitigation Database. Cox does not peer with entities without current registrations.

Analytics-Based Inbound Robocall Blocking

Cox's commitment to mitigating illegal robocalls is further demonstrated in its use of STIR/SHAKEN verification of terminating calls and analytics-based call blocking. Cox provides opt-out call blocking based on reasonable analytics to all residential and business voice customers at no charge. The analytics-based call blocking services incorporate caller ID verification information and are designed to identify calls and call patterns that are highly likely to be illegal. TransUnion (Neustar) and TNS provide these call analytics services. Cox complies with the redress requirements of C.F.R. § 64.1200(k) (8-10).

Do Not Originate ("DNO") and Invalid Numbers

Cox proactively blocks certain calls from telephone numbers that either cannot or would not be used for originating calls. This helps avoid potential annoying, costly, and/or dangerous calls. First, the Cox voice network actively identifies and blocks calls appearing to originate from DNO telephone numbers. These numbers are typically identified by Cox's participation in an industry-led DNO call blocking process whereby telephone numbers are identified by valid sources as receiving inbound calls only.

Cox also blocks inbound calls purportedly originating from 10-digit numbers that are not valid NANP numbers (e.g., a number with an area code beginning with "0") as authorized by the FCC's 2017 Call Blocking Order.¹

Traceback Commitment

Cox commits to respond 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

¹ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, GC Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 ¶ 19 (2017).

any illegal robocallers that use its service to originate calls. Consistent with that commitment, Cox actively participates in industry traceback efforts and has served on the Industry Traceback Group Executive Committee since becoming a contributing member at the Gold Level in 2020.

COX COMMUNICATIONS, INC. – PARENT COMPANY, PRINCIPALS, AND AFFILIATES

Parent Company: Cox Communications, Inc. is a wholly owned subsidiary of CoxCom, LLC

Principals (Cox Communications, Inc.)

Dallas S. Clement – Director

Mark J. Greatrex – Director and President

R. Perley McBride – Director and Executive Vice President and Chief Financial Officer

Jennifer Hightower –Secretary

Charles L. Odom – Vice President and Treasurer

Rebecca L. Siegel – Vice President and Assistant Treasurer

Gregory L. Spick – Assistant Treasurer

Deborah M. Lucy – Assistant Secretary

Sonya Middleton – Senior Vice President and General Counsel, Law and Policy

Amber N. Hall – Vice President & Chief Compliance Officer

Affiliates/Subsidiaries

FRN	Name
0004330296	Cox Virginia Telcom, LLC
0004330239	Cox Nevada Telcom, LLC
0004330197	Cox Arkansas Telecom, LLC
0004329991	Cox Arizona Telcom, LLC
0004330262	Cox Rhode Island Telcom, LLC
0004330015	Cox California Telcom, LLC
0004330189	Cox Kansas Telcom, LLC
0004330148	Cox Georgia Telcom, LLC
0004330221	Cox Nebraska Telcom, LLC
0004330064	Cox Connecticut Telcom, LLC
0004330213	Cox Louisiana Telcom, LLC
0013870241	Cox Ohio Telecom LLC
0004330247	Cox Oklahoma Telcom, LLC
0004330106	Cox Florida Telcom, LP
0014799217	Cox Idaho Telcom
0004330163	Cox Iowa Telcom, LLC
0022616452	Cox Strategic Services, LLC