



CINCINNATI BELL INC.

On Behalf of

CINCINNATI BELL TELEPHONE COMPANY LLC

CINCINNATI BELL EXTENDED TERRITORIES LLC

CBTS TECHNOLOGY SOLUTIONS LLC

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Cincinnati Bell Telephone Company (“CBT”), Cincinnati Bell Extended Territories (“CBET”) and CBTS Technology Solutions (“CBTS”) (collectively, “Cincinnati Bell”) submit this report, as of June 30, 2021, on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. Cincinnati Bell reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

Company Background

CBT is an incumbent local exchange carrier providing voice, data and broadband Internet access services to residential and business customers in the greater Cincinnati, Ohio area, as well as northern Kentucky and a small portion of southeastern Indiana. CBET is a competitive local exchange carrier (“CLEC”) offering local telephone service and broadband Internet access in portions of Ohio and video service in portions of Ohio, Kentucky and Indiana. CBTS is a CLEC and long distance provider authorized to provide service in 49 states and the District of Columbia. CBTS provides long distance service to residential and business customers and offers a variety of technology solutions to business and enterprise customers, including solutions that incorporate interconnected VoIP and cloud services.

Cincinnati Bell utilizes both TDM and IP networks. It has implemented the STIR/SHAKEN framework on the IP portions of its network. The non-IP portions of its network qualify for the non-IP exception for implementation of STIR/SHAKEN. As described below, Cincinnati Bell has implemented a Robocall Mitigation Program for its entire operation and Cincinnati Bell has deployed protections designed to ensure that it remains free of illegal robocalls on its network.

STIR/SHAKEN Implementation

Cincinnati Bell will comply fully with all conditions set forth in the FCC’s orders, rules, and policies regarding the implementation of the STIR/SHAKEN framework for intermediate

providers, including the First Call Authentication Report and Order and Second Call Authentication Report and Order.¹

Cincinnati Bell is subject to the continuing extension provided in 47 C.F.R. § 64.6304(d) for non-IP networks and therefore is exempt from the requirements of § 64.6301 for the TDM portions of its network. 47 C.F.R. § 64.6304(d). Cincinnati Bell complies with § 64.6303(b) through its participation in the ATIS Non-IP Call Authentication Task Force, which is working in the industry to develop a non-internet Protocol caller identification authentication solution. 47 C.F.R. § 64.6303.

Cincinnati Bell has fully implemented STIR/SHAKEN in the IP portions of its network. Cincinnati Bell is implementing STIR/SHAKEN through use of the TNS Call Guardian Authentication Hub. This is a managed end-to-end call authentication solution that fully satisfies the FCC's STIR/SHAKEN requirements. It provides a standardized approach to call authentication and verification (STIR – RFC 8224, RFC 8225, RFC 8226 and SHAKEN – ATIS-1000074-E, ATIS-1000080, ATIS-1000082).

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Cincinnati Bell has implemented to detect and prevent illegal robocalls from originating on its network as of June 30, 2021. Cincinnati Bell is not a significant source of illegal robocalls at this time and has tailored its robocall mitigation practices to address the areas most at risk of - originating illegal robocalls. The measures described below explain how Cincinnati Bell mitigates and addresses the risk it experiences. Cincinnati Bell will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should it determine that changes are appropriate, its practices may differ from those described below.

Customer Due Diligence

- Cincinnati Bell conducts a comprehensive due diligence and credit review before establishing a contractual relationship with customers. Cincinnati Bell's Security Team will review information about new and renewing customers including, but not limited to type of business, state and country of incorporation as contracts are entered into or renewed. The Security Team will identify customers it believes warrant further investigation based on factors that indicate they may be capable of originating illegal robocalls, such as having been subject to a traceback request or previous robocall enforcement action. This review will be aided by external sources and internet searches as are useful in the process. If the investigation raises a concern, the Security Team, in cooperation with Cincinnati Bell's account team, will discuss the concerns with the

¹ *Call Authentication Trust Anchor; Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, FCC 20-42 (rel. Mar. 31, 2020); *Call Authentication Trust Anchor*, WC Docket Nos. 17-97, Second Report and Order, FCC 20-136 (rel. Oct. 1, 2020).

customer and take steps to ensure the customer is aware of and will abide by the restrictions. The Security Team will monitor these customers on a “watch list” to determine if additional actions are necessary. Customers who do not engage in problematic practices after a period of time will be removed from the watch list.

- Cincinnati Bell monitors all of its services for violations of its Acceptable Use Policy (AUP), including excessive use.
- Cincinnati Bell will terminate or suspend service to customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service.

Measures to Prevent or Avoid Exchanging Illegal Robocalls

Cincinnati Bell will prevent the origination of illegal robocalls on its voice network and assist with tracing and stopping illegal robocalls originating on other service providers networks. This is achieved through:

- **Contractual Provisions** – Cincinnati Bell’s tariffs, service agreements, and Acceptable Use Policy prohibit unlawful uses of service and provide for suspension and/or disconnection for violations of these provisions. Subscribers have an obligation not to use the services for any unlawful purpose, not to engage in any fraudulent uses, and to cooperate with Cincinnati Bell in mitigating unlawful activities. In addition, Cincinnati Bell’s contracts require subscribers to cooperate with the Company to investigate reports of unlawful activity, including cooperating with traceback requests.
- **Robocall Monitoring Procedures.** Cincinnati Bell uses TNS Call Guardian analytics technologies and services to monitor traffic on its network and identify potentially unlawful call origination. TNS provides reputation monitoring of originating numbers of Cincinnati Bell customers and enables Cincinnati Bell to identify changes in the reputation score and suspicious activity. Cincinnati Bell has developed a process to investigate incidents identified by this process. The investigation will include determination if the calls are originating on the Cincinnati Bell network (or, for example, are the result of third parties spoofing numbers associated with Cincinnati Bell subscribers or have been the subject of previous traceback requests), and will conduct appropriate follow-up with subscribers to remedy any problems or mitigate the situation. If effective action is not taken, Cincinnati Bell can suspend and/or terminate service to the subscriber.
- **Call Center Solutions.** CBTS offers enterprise level services to call center customers offering inbound and outbound services. CBTS requires its call center customers, who serve well known, reputable national brands, to adhere to applicable legal requirements, including robocall restrictions. Upon receipt of any claim of violations of the robocalling restrictions, CBTS will address the complaint with the customer and require the customer to take appropriate remedial action if necessary.

- **Preventing Calling Line ID (CLID) “Spoofing.”** Cincinnati Bell does not assist or enable its customers to “spoof” telephone numbers on the services it provides. To the extent a subscriber has customer premises equipment that enable spoofing, Cincinnati Bell has no involvement in such activity. However, spoofing in violation of the Truth in Caller ID Act violates Cincinnati Bell’s terms of service and is grounds for suspension and/or termination of service.
- **Call Blocking.** At this time, Cincinnati Bell does not block traffic from invalid numbers by default, but is in the process of implementing analytics-based blocking service from a leading third party analytics provider. Cincinnati Bell currently blocks traffic that appears to be illegal or is flagged as suspicious by its Security Team. In addition, Cincinnati Bell subscribes to the National Do-Not-Originate (DNO) list and blocks calls originating from these numbers to certain subscribers.

Responding to Traceback Requests

- Cincinnati Bell follows the relevant ITG Best Practices to facilitate its response to traceback requests, including specifically:
 - **Dedicated Point of Contact** – Cincinnati Bell has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual, and has provided the ITG with the contact information and business hours for those individuals.
 - **Ongoing Coordination** – Cincinnati Bell will coordinate with the ITG and other voice service providers in relation to instances of suspicious traffic, including exchanging information related to such traffic and ad hoc follow-up as appropriate.
 - **Prompt Investigation and Response** – Upon receiving a traceback request from the ITG, Cincinnati Bell will endeavor to initiate investigation of the source of suspicious traffic within four (4) business hours after receiving a traceback request and strive to complete the investigation and response to the request through the traceback portal within 24 hours. In the event it Cincinnati Bell is unable to respond to a traceback request, it will provide sufficient information in the traceback portal as to why it is unable to respond.
 - **Privacy of Traceback Investigations** – Cincinnati Bell will not share information about traceback investigations, except with the ITG, with other providers involved in the traceback investigation, or when pursuant to a valid legal process.
- Cincinnati Bell maintains current and correct information about its upstream carrier customers so that it can provide accurate responses to traceback requests.

- Cincinnati Bell will periodically review records of traceback requests to identify customers that are the subject of a pattern of traceback inquiries. Cincinnati Bell will determine an appropriate action to take on a case-specific basis, which may include directing the customer to remedy the problem and, if effective action is not taken, temporary suspension of the customer and/or termination of the customer's service.
- Cincinnati Bell maintains records of any traceback request it receives and the customer involved in the request.

Cooperation with State and Federal Regulators

Cincinnati Bell will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, Cincinnati Bell will:

- Respond to request for information about illegal robocalls;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.