

Robocall Mitigation Plan

(Last updated April 1, 2024)

The Federal Communications Commission (“FCC”) has directed certain providers to upload a Robocall Mitigation Plan to the Robocall Mitigation Database portal that describes the specific reasonable steps the provider has taken to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic as part of its robocall mitigation plan. Specifically, the FCC requires the following to be included in robocall mitigation plans: (1) voice service providers must describe how they are meeting their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls; (2) non-gateway intermediate providers and voice service providers must, like gateway providers, describe any “know-your upstream provider” procedures in place designed to mitigate illegal robocalls; and (3) all providers must describe any call analytics systems they use to identify and block illegal traffic including whether they use a third-party vendor or vendors and the name of the vendor(s). This Robocall Mitigation Plan is being filed in accordance with the above-referenced requirements.

Entities Covered by Filing

Inmate Calling Solutions, LLC d/b/a ICSolutions

ICS Corrections, Inc. f/k/a/ Centurylink Public Communications, Inc.

These entities are collectively referred to as “ICSolutions” herein. ICSolutions is a “voice service provider” as defined by the FCC.¹ ICSolutions is not a “gateway provider” or an “intermediate provider” as defined by the FCC.²

¹ The term “voice service” means any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan, including, without limitation, any service that enables real-time, two-way voice communications, including any service that requires Internet Protocol-compatible customer premises equipment and permits outbound calling, whether or not the service is one-way or two-way voice over Internet Protocol. See 47 C.F.R. § 64.6300(o).

² See 47 C.F.R. § 64.6300(d) (defining “gateway provider” as “a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider”); id. § 64.6300(g) (defining “intermediate provider” as “any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point insofar as that entity neither originates nor terminates that traffic”).

Extension under FCC Rule 64.6304(b)

ICSolutions provides correctional calling services (“CCS”) to correctional facilities throughout the United States. Among other things, these services allow the incarcerated to initiate voice calls to their friends and families outside the correctional facility. ICSolutions voice calling services are outgoing only; the incarcerated are not permitted to receive incoming voice calls.

When receiving a voice call initiated by an incarcerated person, the called party is orally notified that the call is from a correctional facility prior to acceptance of the call, and the called party's caller ID display shows the ICSolutions name and/or the ICSolutions toll-free customer service number. ICSolutions does not provide a service to end user customers that receive caller ID information. Consumers (called parties) receiving calls initiated by incarcerated people may block the receipt of future calls by pressing a certain key when ICSolutions attempts to complete the call to the consumer's telephone number, or by contacting ICSolutions directly. The consumer may choose to block all calls from incarcerated people, or only specific calls.

ICSolutions is subject to an extension of the STIR/SHAKEN implementation requirements under FCC Rule 64.6304(b) as a voice service provider that is "incapable of obtaining a [Service Provider Code] token due to Governance Authority policy." Under the rule, the extension remains in place until ICSolutions is "capable of obtaining an [Service Provider Code] token."

Under the current Service Provider Code ("SPC") Token Policy issued by the Secure Telephone Identity Governance Authority in May 2021, a provider must have the following to receive an SPC token: (1) certification on file with the FCC regarding the provider's status of implementing STIR/SHAKEN or compliance with a robocall mitigation plan and a listing in the FCC's Robocall Mitigation Database; (2) an Operating Company Number ("OCN"); and (3) a current FCC Form 499-A report on file.

ICSolutions is a reseller and does not control the network infrastructure necessary to implement STIR/SHAKEN. ICSolutions has contracted with underlying third-party providers to originate, transmit, and terminate calls initiated by incarcerated people, as well as obtain telephone numbers on ICSolutions behalf. As such, ICSolutions does not need to obtain an OCN, and thus does not meet the requirements to receive an SPC token under the current SPC Token Policy. ICSolutions understands that its underlying third-party providers have obtained the necessary SPC token, and those providers have implemented the various STIR/SHAKEN attestation levels for voice calls initiated by incarcerated people that originate on the ICSolutions CCS system.

Robocall Mitigation Plan

Given the specialized nature of ICSolutions services, it is highly unlikely that illegal robocall traffic could be originated by incarcerated people via the ICSolutions CCS system. ICSolutions has not received information suggesting that robocalls were originated by incarcerated people. Therefore, ICSolutions does not consider its CCS system or its customers at high risk of originating illegal robocalls.

Nevertheless, ICSolutions works closely with its underlying third-party providers to prevent, detect, and mitigate the delivery of illegal robocall traffic. ICSolutions understands that each of its underlying third-party providers are listed in the FCC's Robocall Mitigation Database and that these providers have implemented technical and operational processes, including analytics software, to monitor all traffic on their networks. ICSolutions has completed the "know-your-customer" screening process for several of its underlying third-party providers and is subject to provisions in its contracts with its underlying third-party providers that require ICSolutions to take all necessary steps to prevent illegal robocalls on the ICSolutions CCS system.

ICSolutions also has implemented monitoring and reporting procedures designed to detect and prevent fraudulent traffic on its CCS system, which would include illegal robocalls to the extent they were to occur.

When illegal activity is detected on the ICSolutions CCS system, ICSolutions works with its correctional facility customers to stop unlawful activity as quickly as possible.

ICSolutions has taken steps to prevent “new and renewing customers” from originating illegal robocalls. CCS voice calls are subject to stringent safety and security measures and oversight by ICSolutions and its correctional facility customers. CCS calls are validated prior to connection, monitored, and recorded, and correctional facilities impose limits on the specific numbers that may be called by the incarcerated. These safety and security measures make it virtually impossible for the ICSolutions CCS system to be used to originate illegal robocalls.

Further, all ICSolutions customers are subject to enforceable terms of use and an acceptable use policy for use of all ICSolutions-provided services. These policies prohibit use of ICSolutions services for any purpose other than the intended purpose, including use of ICSolutions services for criminal activity or use in a manner inconsistent with applicable laws, rules, and regulations (including correctional facility policies).

Responding to Traceback Requests and Cooperation with State and Federal Regulators

ICSolutions commits to respond to traceback requests and to cooperate with investigating and stopping illegal robocalls as necessary. ICSolutions will respond to traceback requests received from the Industry Traceback Group, the FCC, or law enforcement within 24 hours as required under FCC rules.

ICSolutions also will cooperate with state and federal regulators to prevent, detect, and mitigate illegal robocalls as applicable. Specifically, ICSolutions will: (1) respond to valid law enforcement requests in a timely manner; (2) provide relevant information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and (3) fully implement mandated robocall mitigation procedures possible with the goal of maximizing the mitigation of illegal robocalls.