

BICS ROBOCALL MITIGATION PROGRAM

This document aims to describe the different activities and actions that BICS takes to detect and block robocalls and spam traffic from its network.

1. ABSTRACT

As a leading global International Carrier operating in the voice, messaging and roaming connectivity markets, BICS naturally collaborates with operators and communications service providers around the globe to fight telecom frauds and security breaches.

In this respect, BICS is constantly monitoring all the traffic that transits through its network searching for fraudulent activity so as to mitigate the impact of it both on BICS' network as well on BICS' customers.

BICS supports the FCC efforts to mitigate the impact of Robocalls on any international traffic that enters the U.S. through BICS' Gateway. As a result, BICS has strengthened measures to improve the detection and protection against spam and robocalling activity.

BICS authenticates calls as per the FCC STIR/SHAKEN requirements for all traffic originated by BICS' customers and using U.S. Numbering Plan resources that are duly allocated to BICS by a BICS supplier.

For the rest of the traffic that is carried by BICS in its role as a transit carrier (i.e., an intermediate service provider) and that is not originated by BICS' customers using U.S. Numbering Plan resources, BICS passes on any authentication certificate received from the sending party. As noted below, BICS also cooperatively participates with the industry traceback consortium and fully and promptly responds to all traceback requests it receives from the FCC, law enforcement, and the industry traceback consortium regarding calls for which it acts as an intermediate provider. Additionally, where BICS acts as a foreign service provider, its traffic is subject to a Robocall Mitigation Program.

As described below, BICS has implemented a Robocall Mitigation Program that includes reasonable steps to avoid originating illegal robocall traffic.

2. CUSTOMER VETTING

BICS vets its customer base with whom BICS does business with as part of customer signature process. As part of this process, BICS seeks to ensure that its customer base does not engage in illegal robocalls.

3. MONITORING OF TRAFFIC ORIGINATED BY U.S. NUMBERING PLAN RESOURCES ALLOCATED TO BICS (BICS AS A SERVICE PROVIDER)

3.1. STIR/SHAKEN

BICS supports the FCC efforts to implement the STIR/SHAKEN requirements for all IP traffic and passes unaltered to the subsequent intermediate provider or voice service provider in the call path any authenticated caller identification information it receives with a SIP call that passes through BICS' gateway.

Additionally, BICS has implemented the STIR/SHAKEN authentication framework for its IP traffic where the caller ID is in the range of the U.S. numbering plan resources duly allocated to BICS. BICS authenticates caller identification information for all SIP calls that it originates and transmits those calls with authenticated caller identification information to the next voice service provider or intermediate provider in the call path.

3.2. Controls on traffic terminated into U.S.

BICS monitors behaviours that show illegal, spam and robocalling activity based on several key parameters. These controls are built to work on all BICS' traffic, independently of the technology used, be it IP or TDM.

The behaviours monitored are as follows:

- caller IDs that generate an abnormally high amount of calls to a wide amount of B numbers within a given timeframe (several timeframes are monitored)
- caller IDs that generate an abnormally high amount of short calls to a wide amount of B numbers within a given timeframe (several timeframes are monitored)
- caller IDs that have an abnormal or wrong format and that generate material traffic volumes
- Traffic burst from a given traffic source (sending party with respect to BICS)
- caller IDs generating material traffic volumes while they should not generate traffic (eg. Roaming ranges MSRN, closed ranges, etc)

BICS has also implemented analytics and advanced Machine Learning models to detect robocalls. These models consider a wide range of the call traffic record parameters to determine outliers and possible robocall and spam events.

Based on the results from these controls and analysis, BICS may enhance the mitigation of robocalls and spam calls by blocking the traffic proactively, informing the unwanted traffic senders and receivers.

Additionally, any notification on abnormal traffic received from any customer or supplier is investigated accordingly and the necessary actions taken as per BICS internal process (eg. traffic block, request traffic removal by the sending party, inform receiving party, etc).

4. MONITORING OF BICS TRANSIT TRAFFIC (BICS AS AN INTERMEDIATE PROVIDER)

4.1. STIR/SHAKEN

BICS supports the FCC efforts to implement the STIR/SHAKEN requirements for all IP traffic and passes unaltered to the subsequent intermediate provider or voice service provider in the call path any authenticated caller identification information it receives with a SIP call that passes through BICS' Gateway.

4.2. Controls on traffic terminated into U.S.

BICS monitors all traffic transiting through its network with regards to behaviours that show illegal, spam and robocalling activity based on several key parameters. These controls are built to work on all BICS' traffic, including the traffic originated and terminated into U.S., independently of the technology used, be it IP or TDM.

The behaviours monitored are as follows:

- caller IDs that generate an abnormally high amount of calls to a wide amount of B numbers within a given timeframe (several timeframes are monitored)
- caller IDs that generate an abnormally high amount of short calls to a wide amount of B numbers within a given timeframe (several timeframes are monitored)
- caller IDs that have an abnormal or wrong format and that generate material traffic volumes
- Traffic burst from a given traffic source (sending party with respect to BICS)
- caller IDs generating material traffic volumes while they should not generate traffic (eg. Roaming ranges MSRN, closed ranges, etc)

BICS has also implemented analytics and advanced Machine Learning models to detect robocalls. These models consider a wide range of the call traffic record parameters to determine outliers and possible robocall and spam events.

Based on the results from these controls and analysis, BICS may enhance the mitigation of robocalls and spam calls by blocking the traffic proactively, informing the unwanted traffic senders and receivers.

Additionally, any notification on abnormal traffic received from any customer or supplier is investigated accordingly and the necessary actions taken as per BICS internal process (eg. traffic block, request traffic removal by the sending party, inform receiving party, etc).

5. COLLABORATION

BICS takes an active role at the Industry level to define the best approach and guidelines for the international wholesale carrier community to fight against fraud in general and robocalls in particular by chairing the i3Forum Fight Fraud workgroup.

BICS commits to continue to respond fully and in a timely manner to all traceback requests from the FCC, 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 calls.