STIR/SHAKEN Implementation & Robocall Mitigation Checklist

MARCH 2021

BACKGROUND

In 2020, the Federal Communications Commission (FCC) issued rules requiring that certain communications service providers implement the STIR/SHAKEN call authentication framework and other robocall mitigation practices, generally by June 2021. A key element of the FCC rules is a requirement for all voice service providers to certify as to the status of their implementation of STIR/SHAKEN and, if the provider has not fully implemented the framework (including providers excused due to an extension), the provider must implement a robocall mitigation program on the exempted portions of its network.

There are three required elements of a robocall mitigation program:

(1) the provider must take reasonable steps to avoid originating illegal robocall traffic;

(2) the provider must commit to respond to requests from the Industry Traceback Group to trace suspect calls for mitigation efforts; and

(3) the provider must cooperate in investigating and stopping any illegal robocallers.

These plans should be customized and should reflect the service provider's customer base, services and the risk that illegal robocalls may be originated on its network. To assist providers in developing these robocall mitigation plans, we suggest the service provider consider the following questions:

ROBOCALL MITIGATION PROGRAM QUESTIONS

Customer Due Diligence:

New and Renewing Customers:

- What information do you collect about new customers? Do you verify information when contracts are renewed or services are added?
- Do you offer any services that enable large volumes of outbound calls?
- How do you determine the customer's identity and their right to use the telephone number for STIR/SHAKEN purposes?

Enterprise and Small Business Customers:

- Do you research the customer's reputation and assess the accuracy of all reported information? This includes history of enforcement actions, lawsuits, civil investigative demands, etc.
- Do you review public complaint data or other business reputational data regarding the customer?
- Do you have a policy that defines the circumstances by which you deny, suspend or terminate service to a customer?

Measures to Prevent or Avoid the Origination of Illegal Robocalls

- Do you have enforceable terms of use and/or an acceptable use policy?
- Do you use any analytics technologies or services to monitor traffic on your networks and identify potentially unlawful call origination activity?
- What anti-fraud policies do you have?
- Are there any calls that you block by default, such as calls originating from invalid numbers?

Responding to Traceback Requests

- Do you participate in the Industry Traceback Group?
- What penalties do you have in place if a customer originates a call that is the subject of a traceback request or a large volume of traceback requests?
- Do you have a process in place for investigating and stopping customers that the FCC identifies as originating illegal calls?

Kelley Drye Contacts

STEVEN A. AUGUSTINO
Partner
saugustino@kelleydrye.com
(202) 342-8612

CHRIS M. LAUGHLIN
Associate
claughlin@kelleydrye.com
(202) 342-8635

Follow Us

Kelley Drye provides a number of timely and topical communications, including our TCPA Tracker.

Sign up here to receive Kelley Drye email communications tailored to your interests.

Kelley Drye's Full Spectrum Podcast
www.kelleydryefullspectrum.com

COMMLAW MONITOR BLOG
www.commlawmonitor.com

Twitter
@KelleyDryeComm
www.twitter.com/KelleyDryeComm