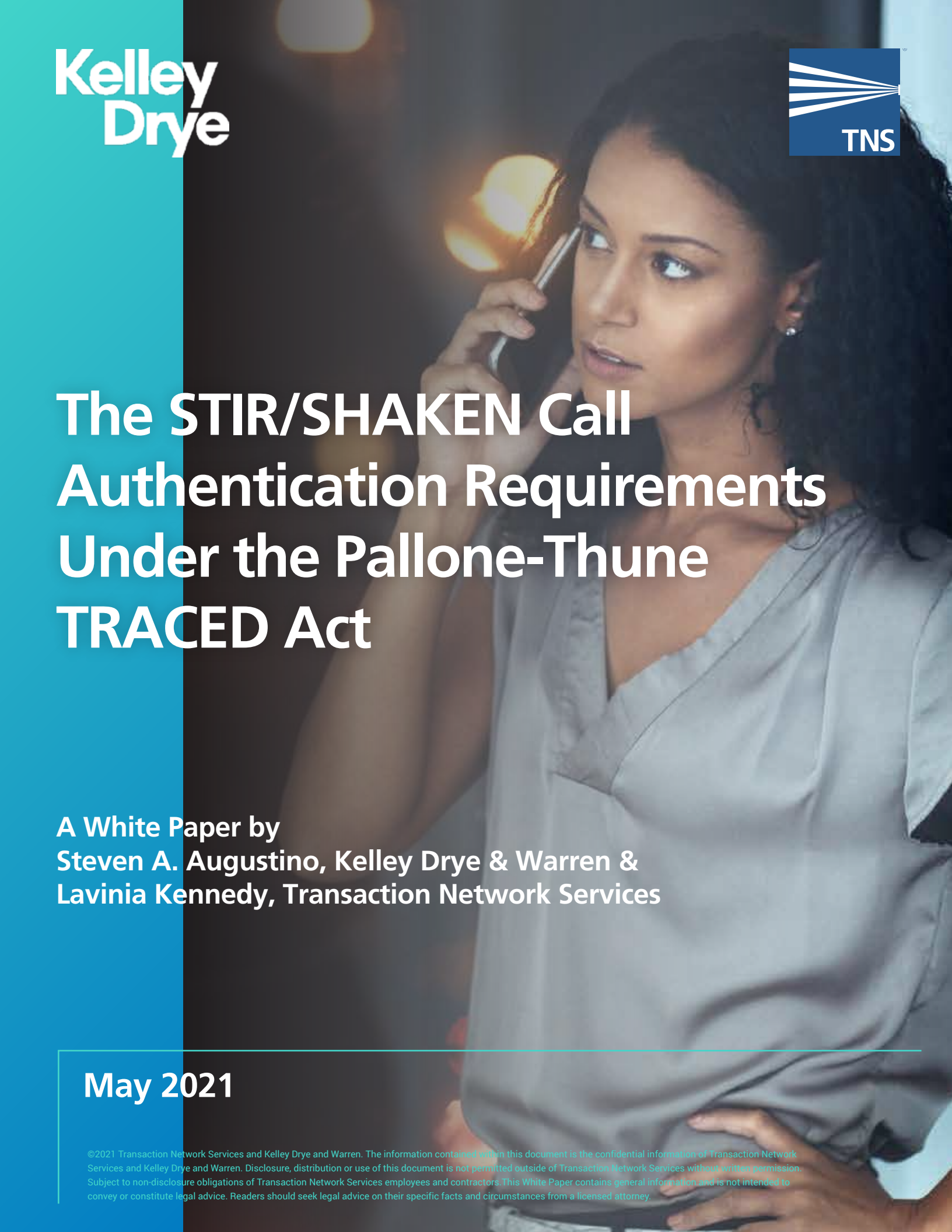


The STIR/SHAKEN Call Authentication Requirements Under the Pallone-Thune TRACED Act

A White Paper by
Steven A. Augustino, Kelley Drye & Warren &
Lavinia Kennedy, Transaction Network Services

May 2021

Contents

Introduction

In 2020, the Federal Communications Commission ("FCC" or "Commission") issued rules requiring that certain communications service providers implement the STIR/SHAKEN call authentication framework and other robocall mitigation practices.

In addition to mandating STIR/SHAKEN to combat robocalls, the FCC issued orders that encourage voice service providers to block unwanted calls by giving them safe harbors for erroneous blocking when call analytics are used, when bad-actors are blocked per FCC orders and when network-based blocking techniques are used.

The FCC also has recognized concerns that legitimate calls will be impacted. To protect such calls, the FCC mandates that each carrier implement a redress process that includes a point-of-contact for blocking complaints and a rapid turn-around for initial response to blocking concerns. The FCC also will require voice service providers to provide notification of blocking via industry standard notification codes.

The obligations adopted for voice service providers in the Order are discussed in this white paper. These requirements are in addition to the obligations previously summarized and this information should be added to the prior advice.

Section One - Pallone-Thune TRACED Act Summary

The compliance deadline for call authentication under the Pallone-Thune TRACED Act is June 30, 2021.

It mandates STIR/SHAKEN for IP-based networks and a robocall mitigation program for non-IP networks, and applies to originating, terminating and intermediate voice service providers.

Only four automatic extensions for STIR/SHAKEN implementation have been granted :

1 | Small voice service providers with under 100,000 subscriber lines now have until June 30, 2023.

2 | Voice service providers unable to obtain SPC tokens have an indefinite extension until such time that they become capable of receiving tokens.

3 | Those services subject to pending 214 discontinuance have been given until June 30, 2022 to comply.

4 | Non-IP networks have been given an indefinite extension, but must comply with 64.6303 (relating to development of call authentication for TDM)

The Wireline Competition Bureau (WCB) may issue other extensions on a case-by-case basis.

Mandatory Implementation of STIR/SHAKEN for IP-based Networks

Section 64.6301 requires voice providers to:

- Authenticate and verify SIP calls originated and terminated on-net
- Authenticate SIP calls it will exchange with other voice service providers
- Verify SIP calls it receives from others for termination to the end-user

Intermediate providers must:

- Pass authentication information unaltered
- Authenticate un-signed calls

Robocall Mitigation Program for Non-IP Networks

The FCC required a robocall mitigation program to demonstrate three key robocall mitigation elements:

1 | Evidence of reasonable steps to avoid originating illegal robocall traffic

2 | A commitment to respond fully and in a timely manner to Industry Traceback Group (ITG) requests

3 | Cooperation in investigating and stopping any illegal robocallers using its service

To aid effectiveness, the FCC recommends implementing reasonable call analytics and in its recent Fourth Report and Order has defined further mitigation obligations which this white paper will now explore.

Section Two - What are the Affirmative Obligations for Voice Service Providers to Reduce unwanted Robocalls?

Under the FCC's rules, voice service providers must do three things to mitigate unwanted robocalls.

1. Respond to traceback requests from the Commission, civil and criminal law enforcement, and the Consortium.

The Commission requires all voice service providers to respond to traceback requests from the Commission, civil and criminal law enforcement, and the FCC-designated Industry Traceback Group as the registered consortium for private-led traceback efforts (the "Consortium"). This requirement applies in addition to the requirement for providers adopted in the Second STIR/SHAKEN Order, which required originating and terminating voice service providers to commit to cooperate with traceback requests. The new requirement applies to all providers that are engaged in traceback response, regardless of their position in the network and their implementation of STIR/SHAKEN.

The FCC instructs the Consortium to notify it of identified patterns of provider non-compliance, although the Commission does not place any authority in the Consortium to address non-compliance. The Order clarifies that voice service providers are only required to respond to traceback requests from the FCC and law enforcement entities when these requests are made consistent with other legal and regulatory requirements.

2.Take steps to effectively mitigate illegal traffic when the provider receives actual written notice of illegal traffic from the Commission.

The Commission directs the Enforcement Bureau ("Bureau") to identify suspected illegal calls and provide written notice to voice service providers. This builds on the previous Call Blocking Order and Further Notice, which allows downstream voice service providers to block calls where an upstream voice service provider failed to effectively mitigate illegal traffic after being notified of that traffic.

The Commission's new requirement takes the additional step of holding the notified voice service provider liable for that failure.

When providing notice to voice service providers, the Bureau must: (1) identify with as much particularity as possible the suspected traffic; (2) cite the statutory or regulatory provisions the suspected traffic appears to violate; (3) provide the basis for the Bureau's reasonable belief that the identified traffic is unlawful, including any relevant non-confidential evidence from credible sources (like the Consortium or law enforcement agencies); and (4) direct the voice service provider receiving the notice that it must comply with Section 64.1200(n)(2) of the rules.

When a provider receives this notice, it must promptly investigate the traffic identified in the notice and **either take steps to mitigate the traffic or respond that it has a reasonable basis for concluding that the identified calls are not illegal.** If a notified provider determines the traffic comes from an upstream voice service provider with direct access to the U.S. public switched telephone network ("PSTN"), the notified provider must inform the FCC and take lawful steps to mitigate this traffic (i.e., enforcing contract terms or blocking the calls from bad actor providers).

Each notified provider must promptly report the results of its investigation to the Bureau, including any steps it has taken to mitigate the identified traffic, or with an explanation as to why the provider reasonably concluded that the calls were not illegal. The Commission clarifies that a showing of a "reasonable basis for concluding that the calls are not illegal" requires sufficient due diligence on the part of the voice service provider making the determination. To "effectively mitigate" the identified traffic, it must first identify the traffic and next take steps to prevent the source of the call from continuing to originate that traffic. However, the Commission does not expect that originating voice service providers will need to block calls to comply with this requirement, although blocking may be necessary for gateway providers to comply with these requirements.

If a provider determines that the source of the call is another voice service provider with access to the PSTN, it must take any otherwise lawful steps to mitigate the traffic, but if a provider cannot take immediate action to mitigate traffic, the Commission encourages providers to use the safe harbor for provider-based blocking.

3. Implement affirmative measures to prevent new and renewing customers from using its network to original illegal calls.

The Order requires voice service providers to adopt affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls. The Commission requires that all originating voice service providers know their customers and exercise due diligence in ensuring that their services are not used to originate illegal traffic. It does not require any specific steps to accomplish this measure, but recommends that providers use caution in granting access to high-volume origination services. This obligation applies both to new customers and to "renewing" customers, suggesting that an evaluation also must be conducted when contracts are extended for an additional term, not simply when the customer first subscribes for service. Although not explicitly addressed in the Order, it is advisable for voice service providers to conduct an ongoing analysis of customer activity, not simply at service initiation or renewal.

Compliance Tips

To effectively mitigate illegal calls, providers should consider questions such as:

- What information do you collect about new customers? Do you verify information when contracts are renewed or services are added?
- Do you research the customer's reputation and assess the accuracy of all reported information? Do you check for a history of enforcement actions, lawsuits, civil investigative demands, etc.?
- Do you have a policy that defines the circumstances by which you deny, suspend or terminate service to a customer? Does it cover ITG traceback inquiries or an FCC notification?
- Do you use any analytics technologies or services to monitor traffic on your networks and identify potentially unlawful call origination activity?
- 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?

Section Three: Is There a Safe Harbor for Call Blocking?

The Commission expands the safe harbor adopted in the Call Blocking Order and Further Notice for blocking based on reasonable analytics to also cover network-based blocking if the network-based blocking incorporates caller ID authentication information where available and meets the requirements in the December 30 Order. To get the benefit of the safe harbor, a terminating voice service provider must ensure its network-based blocking targets only calls that are highly likely to be illegal, not calls that merely are unwanted. Providers must manage this blocking with network monitoring and oversight, which must include a process that "reasonably determines that the particular call pattern is highly likely to be illegal prior to blocking calls that are part of that pattern." The FCC expects voice service providers to demonstrate they have conducted an appropriate process, should the FCC inquire about specific blocking.

Critically, providers engaging in network blocking must include a process to reasonably determine that a particular call pattern is highly likely to be illegal prior to the call blocking. The FCC does not prescribe the specific steps for the process, but expects that it will include a combination of steps designated to identify illegality, such as dialing the telephone number from which the apparently illegal calls purportedly originate; reviewing complaint data about calls from the source; or contacting the originating voice service provider. The Commission clarifies that, because it is only authorizing blocking calls that are highly likely to be illegal, if the terminating provider finds that the calls in the pattern are likely lawful, that provider must immediately cease network-based blocking of the calls.

Section Four: Are There Any Additional Requirements for Providers?

The FCC adopts additional requirements for providers, imposing transparency obligations to ensure that call originators can effectively access redress mechanisms for erroneously blocked calls. Voice service providers are required to offer redress mechanisms for blocking engaged in by the provider or a third-party service providing services to the provider, but providers are not responsible for blocking done by a blocking service chosen by the consumer.

The Order requires providers to do the following:

1. Immediate Notification of Blocking.

Terminating voice service providers that block calls are required to immediately notify the caller that the call has been blocked by either sending a Session Initiation Protocol ("SIP") or ISDN User Part ("ISUP") response code, as appropriate, and all voice service providers in the call path are required to transmit these codes to the origination point. Providers that block calls are required to immediately notify callers of the blocking. All v service providers are directed to perform neces software upgrades to ensure the codes that the FCC requires for this blocked are appropriately mapped, and must ensure that calls transmitting over TDM and IP networks return an appropriate code. Providers must implement the blocking notification requirements by January 1, 2022.

2. Blocked Calls List (to Consumers).

The Order requires terminating voice service providers that block calls on an opt-in or opt-out basis to disclose to their subscribers a list of blocked calls upon request. Providers must provide this list within three (3) business days of receipt of the request, but the reporting requirement is limited to retaining records of calls blocked in the four weeks or 28 days prior to the request.

3. Status of Call Blocking Dispute Resolution.

When a calling party disputes whether blocking its calls is appropriate, the FCC requires terminating voice service providers to provide a status update to the party that filed the dispute within 24 hours.

4. Point of Contact for Verifying Call Authenticity.

The FCC requires that the point of contact established to handle blocking disputes for terminating providers also handle contacts from callers that are adversely affected by information provided by caller ID authentication seeking to verify the authenticity of their calls. A terminating provider that is not already blocking calls, but takes into account attestation information in call delivery, must provide a point of contact to receive caller complaints regarding caller ID authentication.

5. Summary

These measures are intended to balance the need to reduce illegal calls with protections for legitimate callers. The requirements only apply to carrier-controlled blocking activities.

The FCC declines to extend redress mechanisms to call labeling (AoR and similar) at this time, and instead encourages providers and their analytics partners to work in good faith with callers to avoid erroneous labeling. The Commission also declines to extend the safe harbor to cover the inadvertent or unintended misidentification of the level of trust for particular calls, and declines to take further action under Section 7 of the TRACED Act (protections from spoofed calls) at this time, although it may choose to do so in the future.

Section Five: TNS Solutions to Comply with the TRACED Act

TNS can assist with call authentication, safe harbor and implementing a robocall mitigation program.

Address Call Authentication Requirements

Implement a Call Authentication Framework using the TNS Call Guardian Authentication Hub on IP portions of the network, to deliver:

- STIR/SHAKEN compliance
- STI-CA approved certificates
- Universal call blocking
- Advanced call treatment and advice of risk
- Web portal access and custom reporting

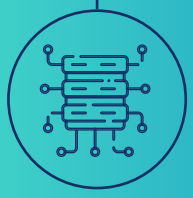
TNS enables accelerated SIP interconnections through the Call Guardian Authentication Hub via its Voice IPX solution.

Define a Robocall Mitigation Program

- Show progress upgrading to IP
- Show progress towards STIR/SHAKEN deployment
- Implement Robocall prevention measures (origination):
  - Know who is originating bad traffic on your network
  - Stop unlawful robocalls from originating on your network
- Implement Robocall Analytics measures (termination):
  - Protect subscribers from illegal robocalls terminating on your network by using reasonable analytics
- Show participation in the ATIS IPNNI Non-IP Call Authentication Working Group
- Show a commitment to respond to USTelecom ITG (Industry Traceback Group) requests
- Show cooperation with FCC and Law Enforcement investigations

Ensure Safe Harbor

Block high-risk traffic to protect subscribers implementing TNS industry leading reasonable analytics that includes use of authentication.



The TNS Call Guardian Authentication Hub provides the tools to comply with the FCC Robocall Mitigation Program. You can protect your subscribers against illegal/unwanted robocalls using TNS Call Guardian analytics and you can ensure bad actors do not initiate calls on your network by using reports, monitoring, alerts, and network traf-fic analysis.

The Call Guardian Authentication Hub lays the foundations for an easy transition, when ready, to STIR/SHAKEN. Contact us to learn more.

About the Authors

Steve Augustino

Chair, Communications Practice Group
Kelley Drye & Warren LLP

Office: (202) 342-8612
Mobile: (240) 305-2456
saugustino@kelleydrye.com

Lavinia Kennedy

Director, Product Management
Transaction Network Services

Office: (703) 453-8352
Mobile: (703) 929-4463
lkennedy@tnsi.com

Please contact us to find out more about how TNS can help you with a wide range of telecom solutions:

Asia Pacific **+61 2 9959 0800**
Europe **+44 (0)114 292 0200**
USA **+1 703 453 8300**
solution@tnsi.com
tnsi.com