

New Call Authentication Requirements Under the TRACED Act



The FCC has announced additional robocall mitigation rules for voice service providers in the Fourth Report and Order; what's new?

Three further actions that voice service providers must take to mitigate unwanted robocalls



1 All voice service providers must respond to traceback requests from the FCC, civil and criminal law enforcement, and the US Telecom Industry Traceback Group.

2 Providers must take steps to effectively mitigate illegal traffic when written notice of illegal traffic from the Enforcement Bureau is received.

3 Providers must implement affirmative measures to prevent new and renewing customers from using their network to originate illegal calls by developing a robocall mitigation program.

Expanded safe harbor for call blocking

Safe harbor for call blocking has been expanded to also cover network-based blocking if caller ID authentication information is incorporated where available.



Terminating voice service providers must ensure network-based blocking targets only calls that are highly likely to be illegal, not calls that merely are unwanted.



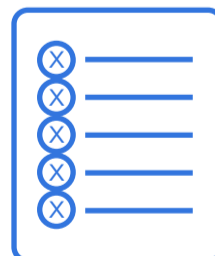
Specific steps are not prescribed for this process, but a combination of steps designated to identify legality are expected.



Providers must also ensure that call originators can effectively address redress mechanisms for errantly blocked calls.



Immediately notify callers of blocking



Disclose a blocked calls list to consumers upon request



Provide status of call blocking dispute resolution



Establish a point of contact for verifying call authenticity

For a deeper dive into the FCC's Fourth Report and Order please read our whitepaper: Updated Factors to Consider When Implementing the STIR/SHAKEN Call Authentication Requirements Under the Pallone-Thune TRACED Act, available at tnsi.com

Find out more at tnsi.com

