

SIP 603+

What the FCC's New Call-Blocking Rule Means for Telemarketing



For businesses that rely on outbound calling to reach consumers, an important regulatory change took full effect on March 25, 2026.

The Federal Communications Commission's mandate requiring the use of SIP code 603+ may sound like a technical footnote, but its implications for telemarketing operations are significant.

Understanding what this rule does (and what it doesn't do) is essential for organizations that depend on the phone to conduct business.

What is SIP 603+?

SIP stands for **Session Initiation Protocol**, the technology that governs how phone calls are set up, managed, and torn down on modern IP-based telephone networks. When a call fails to connect, the network returns a numeric response code explaining why. It's similar in concept to the HTTP error codes a web browser returns when a page fails to load.

For years, when a carrier's analytics system determined that an outbound call looked like spam or a robocall and then blocked it, the calling party could receive any one of several different SIP codes, none of which clearly communicated that a deliberate, analytics-driven block had taken place.

From the originating caller's perspective, any of these codes could just as easily mean a network error, a busy line, or a consumer manually rejecting the call. The lack of a standardized signal left legitimate businesses largely in the dark about whether their calls were actually reaching consumers or being silently intercepted.

The intent of SIP 603+ is to address and resolve this ambiguity. It is a modified version of the standard 603 response, distinguished in two key ways. First, it replaces the open-ended reason phrase "Decline" with "Network Blocked," making the intent unmistakable.

Second, it includes a structured Reason header containing machine-readable parameters: a cause code identifying why the call was blocked, a location code identifying where in the call path the block occurred, and contact information (a URL, email address, or phone number) for the blocking provider's redress process.

This last piece is significant, because it gives the caller a direct avenue to dispute the block.

The FCC's Order and the Road to Compliance

The rule was adopted by the FCC in February 2025 requiring all terminating providers that block calls based on analytics to immediately return a 603+ response and prohibited the use of the older 603, 607, and 608 codes for that purpose.

The order also requires every intermediate provider in the call path to pass the 603+ code back to the point of origination; it cannot be dropped or substituted along the way.

The compliance deadline was set at one year following publication in the Federal Register, landing on March 25, 2026. During the preceding transition period, carriers were permitted to begin adopting 603+ voluntarily while phasing out the legacy codes.

As of the deadline and publishing of this blog, use of 603+ is no longer optional. It is the mandatory and exclusive signal for analytics-based call blocking across IP networks.

Need assistance with customer contact compliance?

[Speak to an expert](#)

What This Means for Outbound Calling Businesses

Visibility is perhaps the more immediate benefit. With 603+ now standardized, organizations that pull call detail records (CDRs) from their telephony providers can begin filtering specifically for this code. A pattern of 603+ responses on a particular outbound number is a clear signal that the number has been flagged by carrier analytics as suspected spam, something that would previously have required guesswork to identify.

Redress is the longer-term operational benefit. Because the 603+ Reason header contains contact information for the blocking provider, legitimate businesses that find their numbers being incorrectly flagged now have a defined path to challenge the block.

This is a meaningful improvement over the previous environment, where even identifying which carrier was blocking calls often required significant investigative effort. The FCC designed this mechanism specifically to reduce the burden on legitimate callers who are caught up in analytics-based blocking despite operating within the law.

Important Limitations

Businesses should be careful not to overestimate the scope of 603+. The rule applies exclusively to voice calls blocked by carrier analytics on IP networks. It does not apply to text messages, to calls that are merely labeled as "Spam Risk" or "Scam Likely" on a consumer's caller ID display

Perhaps most importantly for businesses monitoring their call performance, 603+ provides no visibility into consumer-level blocking. Applications like Nomorobo, Robokiller, and similar smartphone spam-blocking tools operate at the device level, after the call has already traversed the carrier network.

These apps can silence, screen, or reject a call without generating any SIP response back to the originating party. A call intercepted by a consumer's spam-blocking app will typically appear in call records as a no-answer or a brief connect, indistinguishable from a genuine non-answer.

Similarly, 603+ does not address call labeling. If a number is being displayed to consumers as "Spam Likely," the call may still ring without any 603+ code ever being generated. Businesses experiencing low answer rates should not assume the absence of 603+ responses means their numbers are free of carrier or analytics flags.

What Businesses Should Do Now

With the compliance deadline now passed, organizations that conduct outbound calling should take several practical steps.

First, establish a process for regularly reviewing call records for 603+ responses, segmented by outbound number. Numbers generating repeated 603+ codes should be investigated and potentially retired or submitted for redress through the channel provided in the response header.

Second, consider proactive number reputation management. Services like Caller ID Reputation allow businesses to register outbound numbers directly with the major analytics providers that feed carrier blocking systems. This does not guarantee numbers will never be flagged, but it provides an additional layer of legitimacy that may reduce the likelihood of erroneous blocking.

SIP 603+ does not solve the broader challenge of operating a compliant outbound calling program in a regulatory environment that continues to tighten. Still, for organizations that take the time to understand and act on the data, it provides a clear signal when the network is working against you.

PossibleNOW is the pioneer and leader in customer contact compliance. From federal and state regulations to international laws, our platform **DNCSolution** consolidates everything a business needs to stay compliant with regulations such as Do Not Call, TCPA, CAN-SPAM, and Reassigned Numbers Database. We back our solutions with a 100% compliance guarantee and keep companies out of the crosshairs of professional litigators.

Our technology, processes, and services enable relevant, trusted, and compliant customer interactions.

PossibleNOW: Marketing Compliance Made Simple.

Request a Demo:



Contact Us

(800) 585-4888 or (770) 255-1020

email | info@possiblenow.com

visit | www.possiblenow.com