

How First Orion's **SENTRY®** Call Blocking Protects Healthcare Organizations from Number Spoofing



How First Orion's SENTRY® Call Blocking Protects Healthcare Organizations from Number Spoofing

Healthcare organizations face a serious call [spoofing](#) threat. Patients trust calls that appear to come from doctors' offices, hospitals, or pharmacies, and scammers use that trust to steal information.

When attackers spoof numbers, they can expose patient data, damage trust, and disrupt legitimate communications. First Orion's [SENTRY® Call Blocking](#) helps stop spoofed calls before they reach patients.



Call Spoofing in Healthcare

Healthcare fraud remains costly, and voice phishing keeps rising. Spoofed calls can look convincing because attackers often use stolen data, AI voice tools, and familiar caller ID tactics to impersonate healthcare teams.



How Call Spoofing Hurts Healthcare Organizations

Call spoofing can affect healthcare organizations in several ways:

- Patients may share insurance details, Medicare information, Social Security numbers, or payment data with a scammer.
- Brands may lose trust if patients believe its number was involved in a fraud attempt.
- Legitimate calls may get mislabeled as spam after complaints tied to spoofed activity.
- Staff may spend time handling fraud fallout instead of supporting patients.

How First Orion's SENTRY® Call Blocking Protects Healthcare Organizations from Number Spoofing

Why SENTRY Helps

SENTRY Call Blocking helps protect organizations at the carrier level before spoofed calls reach patients. That matters because prevention works better than reacting after the damage is done. SENTRY helps:



Block spoofed calls before they reach patients.



Preserve answer rates by protecting numbers from spam labeling.



Support your patient trust and communication efforts.



Reduce operational strain on your team.



Protect vulnerable populations, including seniors and patients managing chronic conditions.

How SENTRY Works

When organizations place an outbound call, systems send the caller and recipient information to First Orion via a REST API. First Orion generates a unique, time-limited authentication key for that specific call and delivers it to the recipient's carrier. When the call hits the carrier network, the carrier checks for that key. If it matches, the call goes through. If there's no match, the call never reaches the recipient.

The entire process runs in real time with no disruption to your legitimate call flow. Spoofed calls get blocked. Your real calls get through.

SENTRY works across all major U.S. carriers, integrates through a simple REST API or SIP configuration in a matter of days, and requires no app download from your customers. Protection happens inside the carrier network.



How First Orion's SENTRY® Call Blocking Protects Healthcare Organizations from Number Spoofing



SENTRY and INFORM

SENTRY works with First Orion's INFORM® Branded Calling to strengthen trust in your outbound communications. SENTRY blocks spoofed calls, while INFORM helps identify legitimate calls with the organization's name, logo (available with [INFORM® with Logo](#)), and reason for calling.

That combination helps patients recognize calls quickly. It can improve pickup rates, reduce missed appointments, and support better patient engagement.

Protect Numbers, Protect Patients

A healthcare organization's responsibility to protect patients does not stop at the firewall. When scammers use legitimate numbers, patients face fraud and organizations absorb the fallout.

First Orion SENTRY Call Blocking integrates with existing infrastructure, works across major U.S. carriers, and helps stop spoofed calls before they reach your patients. It protects your patients, your reputation, and your communications.

[Learn More about SENTRY](#)

