



SENTRY® Call Blocking for Finance

How Banks, Lenders, and Financial Institutions Stop Fraudsters From Spoofing Their Phone Numbers

SENTRY® Call Blocking for Finance

Why Financial Services' Phone Numbers Are the Most Frequently Spoofed in the United States

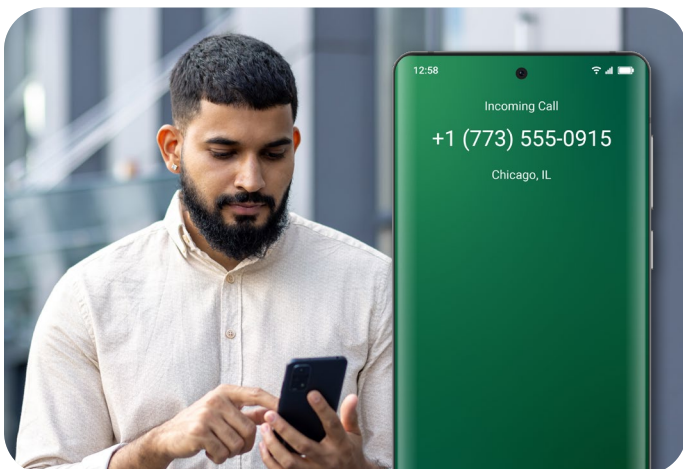
Fraudsters choose numbers consumers trust, and financial institution numbers top that list: fraud hotlines, main contact numbers, and payment reminder lines all carry authority over accounts and funds. These numbers are spoofed more often, cause disproportionate consumer harm per incident, and accumulate carrier reputation penalties faster than most other industries.

Imposter scams were the FTC's most reported fraud category for the fifth straight year in 2025, with business impersonators¹ — led by bank impersonators — **accounting for roughly \$1 billion in reported losses.**

The fallout hits your institution: reduced answer rates, customer service calls about incidents you never initiated, regulatory inquiries, and "Scam Likely" labels on numbers. [SENTRY® Call Blocking](#) tops spoofed calls before they reach consumers, before complaints build, and before your outbound program is penalized for fraud you did not commit.



How Phone Number Spoofing Works in Financial Services Fraud



[Spoofing](#) lets a caller insert any number into the caller ID field of an outbound call, with no requirement that the displayed number matches the true origin. [Caller ID \(CNAM\)](#) was designed for convenience, not verification, and fraud operations exploit this by using numbers consumers recognize and trust.

The call appears to come from your institution, the consumer complies, and your number absorbs the complaint and reputation damage.

SENTRY® Call Blocking for Finance

What Is the Cost of Spoofing to a Financial Institution's Outbound Calling Program?



Call Answer Rates

Complaint volume pushes analytics platforms to score your number as suspicious, triggering "Spam Risk" or "Scam Likely" labels and suppressing response to legitimate calls.

Customer Service Burden

Consumers call in to report incidents your team has no record of, consuming agent time without generating value.

Long-term Brand Damage

Customers who believe your number was responsible for fraud may reduce activity or close accounts, weakening hard-earned trust.

Regulatory Exposure

Spoofing victims may file with the CFPB, FTC, or state regulators, drawing inquiries to your institution even when you were only the impersonated party.

How Does SENTRY Protect Financial Institution Phone Numbers

SENTRY prevents scammers from using your business phone numbers to make fraudulent calls. Before your call is placed, First Orion generates a time-limited key and shares it with the carrier network. When the call reaches the carrier, it checks for that key — legitimate calls are delivered, and anything without a valid key is blocked before it ever reaches your customer.



SENTRY® Call Blocking for Finance

Why Should You Choose SENTRY Over Other Solutions?

First Orion's SENTRY

- Flexible integration options, including a REST API and patented SIP call routing configuration, with implementation guides to streamline onboarding.
- End-to-end call authentication that confirms a call's legitimacy in real time, from origination to delivery.
- A standalone offering that also complements [INFORM® Branded Calling](#) for more advanced configurations.

Typical Competitor Solutions

- Limited integration options.
- Heavy reliance on STIR/SHAKEN alone, which simply expresses a level of confidence of the call's origination but is not designed as a complete spoofing prevention solution.
- Limited customization, with blocking embedded in broader product bundles instead of offered as a focused capability.

Why Do Legitimate Financial Service Calls Get Labeled as Scam Likely?

Two main mechanisms drive "Scam Likely" or "Spam Risk" labels, and each requires a different fix.

Spoofing-driven complaints: For compliant institutions, spoofing-generated complaints are usually the primary driver. Some analytics systems cannot distinguish your legitimate calls from spoofed calls using your number, so your outbound traffic inherits negative scores. If your practices are compliant, STIR/SHAKEN is configured, and CNAM registration is current but labels persist, active spoofing is the likely cause — and SENTRY addresses this by stopping the spoofed calls that generate complaints.

Behavioral flags: Analytics systems also look for patterns that resemble high-risk robocall behavior: short-interval repeat calls, high unanswered or short-duration rates, and calls to National DNC Registry numbers. These require a review of dialing practices, not spoofing protection.



SENTRY® Call Blocking for Finance

What Financial Services Operations Are Covered Under SENTRY?



**Payment
reminder and
collections
programs**



**Customer
service and
relationship
management**



**Automated
notification
systems**



**Fraud alert
and account
security calls**

How Does SENTRY Work with INFORM® Branded Calling?

SENTRY blocks spoofed calls that use your business numbers, while INFORM brands your authenticated calls with your business name, logo, and call reason. Together, spoofed calls never reach your customers, and legitimate calls arrive fully identified, increasing the likelihood that consumers answer instead of dismissing them as suspicious.

You can choose which programs receive INFORM branding, SENTRY protection, or both, depending on risk profile and business goals.



SENTRY® Call Blocking for Finance

Frequently Asked Questions for Financial Services Teams

Does SENTRY require changes to existing telephony infrastructure?

No. It operates at the network level through First Orion's carrier integrations, so there are no changes to CRMs, dialers, or STIR/SHAKEN configurations. Number registration is the only step.

How does it handle numbers shared across departments or multiple telephony/VoIP providers?

Protection is tied to the registered number itself, not to a specific department, system, carrier, or platform.

How does it interact with TCPA, FDCPA, or state calling regulations?

SENTRY blocks fraudulent calls displaying your number that do not originate from your systems and does not change your compliance obligations for calls you place.

Can it help recover a number that already has a Scam Likely label?

Yes. SENTRY includes our end-to-end security feature, Call Authentication, that verifies the call in real-time. This verification signals to carriers that your call is legitimate and should not be labeled as scam.

How do we know if our numbers are being actively spoofed?

Watch for customer service reports about calls consumers did not initiate, answer rate declines without practice changes, "Scam Likely" labels despite compliant practices, and FTC or carrier complaints. AFFIRM Reputation Monitoring gives insight into how your outbound calls show up on your customers' phones and makes sure you're not being flagged as spam or scam.

**Start Spoof-Proofing
Your Numbers Today.**

