



Someone Is Spoofing Your Business Number: What to Do

Get a business phone number with a simple auto attendant menu from Auto Attendant. A caller picks who they need and the call rings that person's own mobile, so nobody on your team has to publish a personal number.

Published by Auto Attendant · 2026-10-29 · someone is using my phone number to call people · my number is being spoofed · business number spoofed what to do · report spoofed number

Original article: <https://autoattendant.io/articles/someone-spoofing-my-business-phone-number>



In this article

1. [The short version](#)
2. [What "someone is using my number" usually means](#)
3. [Why you cannot stop it at the source](#)
4. [Is spoofing illegal?](#)
5. [Step 1: Confirm it is spoofing, not your own traffic](#)
6. [Step 2: Report it](#)
7. [Step 3: Tell your carrier and your callers](#)
8. [Step 4: Protect the number's reputation](#)
9. [What the regulators will and will not do](#)
10. [Should you change your number?](#)
11. [One-page checklist](#)
12. [FAQ](#)

The short version

If strangers keep calling your business to ask "why did you call me?", your number is most likely being **spoofed**: someone else is placing calls and faking your number in the caller ID. They do not need access to your phone, your account or your office. You usually cannot stop it at the source, but you can confirm it, report it, warn the people who call back, and protect the number's reputation while it lasts.

This guide covers the United States and Canada as of October 2026. It is educational, not legal advice.

What "someone is using my number" usually means

Caller ID normally shows the number and name of the line a call came from. Spoofing is changing what the person receiving the call sees. The FCC defines it as a caller deliberately falsifying "the information transmitted to your caller ID display to disguise their identity" ([FCC, Caller ID Spoofing](#)).

The CRTC describes three common patterns ([CRTC, Caller ID Spoofing](#)):

Pattern	What the recipient sees	Why scammers use it
Neighbouring	A number matching the first 6 digits of their own number	Looks like a local call, so more people answer
Mirroring	Their own number	Curiosity; confusion
Impersonation	The number of another person or organization, such as a known brand or a government office	Borrowed trust

Your business is usually caught in the first or third pattern. A robocaller picks numbers that look local to the people it targets, or picks a real business number because a real business is more believable. Some of the people who get those calls then call the number back, and that number is yours.

Signs that this is what is happening:

- Several unknown people call within hours or days, all saying they missed a call from you.
- Callers describe a recorded message, a "warranty" pitch, a bank alert or something else your business does not do.
- Your own call history shows no outbound calls to those people.
- Some callers are angry; some ask to be removed from "your" list.

Why you cannot stop it at the source

Caller ID is data that the calling side sends along with the call. Whoever originates the call can, technically, put another number in that field. Your number being spoofed does not mean your line was hacked. It means someone typed your digits into their calling system.

Two industry measures reduce spoofing but do not end it:

- **STIR/SHAKEN caller ID authentication.** The FCC required US voice providers to implement STIR/SHAKEN in the IP portions of their networks by June 30, 2021, and has since extended the obligation to more providers ([FCC, Call Authentication](#)). The CRTC directed Canadian providers to implement the same framework for IP-based calls, but says that "not all calls received will be authenticated," for example when a call is not carried entirely over IP or the phone cannot display the result ([CRTC](#)). Our explainer on [STIR/SHAKEN call authentication](#) goes deeper.
- **Traceback.** In Canada, an industry working group built a call traceback process, at the CRTC's request, to find the origin of unwanted calls "regardless of the type of technology used by the caller" ([CRTC](#)). In 2026 the CRTC made participation in call traceback mandatory for all voice service providers ([Telecom Decision CRTC 2026-52](#), [CRTC 2026 decisions list](#)). In the US, the Industry Traceback Group, established in 2015 by USTelecom, plays a similar role for the industry ([Industry Traceback Group](#)).

So the realistic goal is not "make it stop today." It is: show that the calls are not yours, help the people who call back, feed the reports that drive enforcement, and keep your number usable.

The FCC's own expectation is reassuring: "Usually, scammers switch numbers frequently. It is likely that within hours they will no longer be using your number" ([FCC](#)). That is a general observation, not a promise; some campaigns last longer.

Is spoofing illegal?

United States

The Truth in Caller ID Act, in [47 U.S.C. 227\(e\)](#), makes it unlawful to "knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value." The FCC's rule, [47 CFR 64.1604\(a\)](#), repeats that standard and covers both voice and text messaging services, including callers outside the US when the recipient is in the US.

Key points:

- **Intent matters.** Displaying a different number is not illegal by itself. The FCC gives legitimate examples: a doctor calling from a personal mobile and showing the office number, or a business displaying its toll-free call-back number ([FCC](#)).
- **Blocking your own caller ID is not spoofing.** Showing "unknown" is legal ([47 CFR 64.1604\(c\)](#); [FCC](#)).
- **Penalties.** The statute sets an FCC forfeiture of up to \$10,000 per violation, or three times that for each day of a continuing violation, capped at \$1,000,000 for any single act or failure to act ([47 U.S.C. 227\(e\)\(5\)](#)). Adjusted for inflation, the amounts in force in October 2026 are \$14,432 per violation, \$43,296 per day, and up to \$1,443,275 ([47 CFR 1.80](#)). Willful violations can also lead to criminal fines of up to \$10,000 per violation ([47 U.S.C. 227\(e\)\(5\)](#)).
- **States can sue too.** A state attorney general can bring a civil action in federal court to enforce the spoofing provision on behalf of the state's residents ([47 U.S.C. 227\(e\)\(6\)](#)).

Canada

Telemarketers calling Canadians must identify themselves and their client accurately. The CRTC says that spoofing caller ID to show "inaccurate, false or misleading information" violates that requirement, and each violation of the Unsolicited Telecommunications Rules can bring a fine of up to \$1,500 for an individual and up to \$15,000 for a corporation ([CRTC](#)). The CRTC opened a review of those rules in 2026 (Compliance and Enforcement 2026-132); until it issues a decision, the current rules apply. The CRTC also lists legitimate uses, such as a call centre displaying its client's number, or a doctor showing the hospital's general call-back number ([CRTC](#)).

Fraud itself is a police matter in Canada (see Step 2).

Step 1: Confirm it is spoofing, not your own traffic

Before you tell anyone your number is being spoofed, rule out the boring explanations. Spend 20 minutes on this.

1. **Pull your outbound call log** for the dates callers mention, from your phone provider's portal or bill. Look for calls to the numbers that called you back.
2. **Check every system that can send calls with your number:** the desk phones, the mobile app of your phone service, any dialer or CRM, an appointment-reminder service, an answering service, a marketing agency. Any of these may be set to display your main number.
3. **Ask staff** whether anyone ran a call campaign or set up a new tool.
4. **Check the content.** If callers describe a pitch your business never makes (car warranty, tax debt, "your account is locked"), it is almost certainly not your traffic.
5. **Write it down.** Keep a simple log; you will need it for reports and for your carrier.

A log template:

Date and time of call-back	Caller's number	Where they are	What they say the call was about	Time they say they got the call
2026-10-27 10:14	(555) 010-xxxx	Ohio	Recorded "warranty" message	About 9:50

Screenshots of callers' texts or of your carrier's call log are useful evidence. Do not ask callers for more personal information than you need.

If your log shows outbound calls you cannot explain, the problem may be different: account compromise or toll fraud. Change passwords on your phone account and portal, and call your provider right away.

Step 2: Report it

Reports rarely produce an individual fix, but they are how regulators and carriers find campaigns. File once, with your log attached or summarized.

In the United States

- **FCC.** At the FCC Consumer Complaint Center, choose "unwanted calls/texts" as the Phone Issue, then "my own number is being spoofed" as the sub-issue. The same path covers a number that is "blocked, or labeled as potential spam" ([FCC Consumer Complaint Center](#)).
- **FTC.** The FTC takes reports at [ReportFraud.ftc.gov](#) when money was lost or someone has details about a scam, and at [DoNotCall.gov](#) for unwanted calls with no money lost ([FTC, Phone Scams](#)). If a customer was defrauded by a call that showed your number, point them there.
- **Your state attorney general** can enforce the spoofing law ([47 U.S.C. 227\(e\)\(6\)](#)). If a campaign is impersonating your business to defraud customers, a short report to the state consumer protection office is worth sending.

In Canada

- **Canadian Anti-Fraud Centre (CAFC) and local police.** The CRTC says suspected fraud can be reported to local police or the CAFC at 1-888-495-8501, a service run jointly by the RCMP, the Ontario Provincial Police and the Competition Bureau ([CRTC](#)). The CAFC also takes reports online at [reportcyberandfraud.canada.ca](#), including anonymously; its phone line answers Monday to Friday, 10 am to 4:45 pm Eastern ([CAFC, Report fraud and cybercrime](#)).
- **Telemarketing complaints.** If the calls are telemarketing, the CRTC's page links to its unwanted-telemarketing complaint process under the Unsolicited Telecommunications Rules ([CRTC](#)).

Step 3: Tell your carrier and your callers

Your carrier

Call your phone provider's business support and say exactly this: "Our number is being spoofed. People are calling us back about calls we never made. We have a log of dates and times. Can you confirm no outbound calls came from our account, and can you open a traceback or abuse report?" Ask for a ticket number. What each carrier does next varies and is not published consistently; at minimum you want written confirmation that the calls did not originate on your account.

People who call back

The FCC suggests explaining to callers that your number is being spoofed and that you did not make the calls, and placing a message on your voicemail saying so ([FCC](#)). Keep it short and calm.

Script for staff answering a call-back:

"Thanks for calling back. Someone is faking our number on robocalls this week. That call did not come from us, and we are not asking for any information or payment. If they asked you for money or personal details, please don't give any, and you can report it to the FTC (US) or the Canadian Anti-Fraud Centre. Sorry for the trouble."

Temporary greeting or menu message:

"Thanks for calling [Business name]. If you are returning a missed call from this number: we have not called you. Our number is being used by scam callers without our permission. We never ask for payment or personal details by phone. To reach us about something else, please stay on the line."

Website notice (top of the contact page):

"Scam calls are showing our phone number. [Business name] has not placed these calls and never asks for payment or account details by phone. If you received one, you can report it to [\[ReportFraud.ftc.gov / the Canadian Anti-Fraud Centre\]](#)."

Remove the notices a couple of weeks after call-backs stop.

Step 4: Protect the number's reputation

Spoofed robocalls can cause carriers and apps to label or block calls from your number, which hurts you if your business does call customers. The FCC notes that a number labeled "potential scam" or "spam" may have been spoofed, and that it has encouraged blocking providers to give callers a way to contact them and fix an incorrect block ([FCC](#)).

Practical steps:

1. **Register the numbers you call out from** at the Free Caller Registry, a free registration run by the call-analytics providers First Orion, Hiya and TNS. Registration is for businesses calling on their own behalf, and the site says plainly that registering "does not guarantee redress"; each provider still runs its own analysis ([Free Caller Registry](#)).
2. **Test how your number displays** by calling a few mobiles on different carriers. If a label appears, our guide on [why a business number shows up as spam](#) walks through the remediation steps.
3. **Keep your outbound caller ID consistent.** If you use several systems, make them all display numbers you actually own.
4. **Set a voicemail PIN.** The FCC warns that some voicemail services allow access when called from your own number, so a spoofer could reach your voicemail if no password is set ([FCC](#)).

What the regulators will and will not do

	FCC	FTC	CRTC	CAFC / police
Takes your report	Yes	Yes	Telemarketing complaints	Yes
Resolves your individual case	No: "We do not resolve individual unwanted call or text complaints" (FCC)	Not stated per report	Not stated per report	Police investigate; CAFC supports law enforcement (CAFC)
Uses reports for enforcement or policy	Yes (FCC)	Yes	Traceback and STIR/SHAKEN measures (CRTC)	Links crimes across reports (CAFC)

Set expectations accordingly. The report protects the record and helps the next business; it will not usually produce a phone call back telling you the culprit was caught.

Should you change your number?

Usually not. Your number is on your website, signage, listings and invoices, and the FCC's observation is that spoofers move on quickly (FCC). A new number does not stop anyone from spoofing it next. Consider a change only if a campaign persists for weeks, labels will not clear, and the call-backs are disrupting operations; and even then, keep the old number forwarding with a "we have moved" message for a long transition period.

One-page checklist

- ☐ Logged dates, times and caller numbers of call-backs
- ☐ Checked our outbound call log and every tool that can send calls with our number
- ☐ Changed portal and account passwords if anything looked odd
- ☐ Filed with the FCC ("my own number is being spoofed") or the CAFC
- ☐ Opened a ticket with our carrier and asked for confirmation that the calls were not ours
- ☐ Gave staff the call-back script
- ☐ Added a temporary greeting and website notice
- ☐ Set or changed the voicemail PIN
- ☐ Registered our outbound numbers at the Free Caller Registry
- ☐ Calendar reminder to remove notices two weeks after call-backs stop

FAQ

Can I sue the spoofer? Under the federal statute, enforcement of the spoofing provision is by the FCC, criminal prosecution, and state attorneys general (47 U.S.C. 227(e)). In practice, spoofers are hard to identify. Ask a lawyer if you have suffered real losses and know who is behind the calls.

Will my number be blocked because of this? It can be labeled or blocked by analytics, because blocking is based on call patterns and complaints (FCC). That is why Step 4 matters if you make outbound calls.

Is my phone or account hacked? Spoofing does not require access to your line. Check your outbound call log (Step 1). If it shows calls you did not make, treat it as an account security problem instead.

Does blocking our caller ID count as spoofing? No. Blocking your own number so it shows as "unknown" is allowed (FCC).

Someone called back angry and threatened to report us. What do we say? Use the script above, stay calm, and offer the reporting links. Your log and your carrier ticket show you took the right steps.

For a line that only receives calls, there is a simple tell: Auto Attendant numbers place no outbound calls at all, so any call showing one as caller ID did not come from the service.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. <https://www.fcc.gov/consumers/guides/spoofing>
2. <https://crtc.gc.ca/eng/phone/telemarketing/identit.htm>
3. <https://www.fcc.gov/call-authentication>
4. <https://crtc.gc.ca/eng/8045/d2026.htm>
5. <https://tracebacks.org>
6. <https://www.law.cornell.edu/uscode/text/47/227>
7. <https://www.ecfr.gov/current/title-47/part-64/section-64.1604>
8. <https://www.ecfr.gov/current/title-47/section-1.80>
9. <https://consumercomplaints.fcc.gov/hc/en-us/articles/115002234203-Unwanted-Calls-Phone>
10. <https://consumer.ftc.gov/articles/phone-scams>
11. <https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm>
12. <https://www.freecallerregistry.com/fcr>

THE PUBLISHER

About Auto Attendant

Auto Attendant gives a small business one phone number and a recorded menu that sends each caller to the right person. The call rings the mobile that person already carries, using their normal dialler and their normal mobile plan. Pricing is a single flat monthly fee for the whole company rather than a charge for each user, and there is no app, desk phone or hardware to install.

One number, one menu, the phones you already own

A caller dials the business number, hears a short greeting and chooses an option. Each option can ring one mobile, ring several at once so whoever is free answers first, or try people one after another in a set order. There is no limit on how many people sit on the receiving end, because nobody is billed per seat. Setup is done by the owner in a few minutes: pick a number, write the greeting, and point each option at a mobile.

What it deliberately is not

An auto attendant routes a call; it does not answer one. Nobody at Auto Attendant speaks to callers, and no AI stands in for a receptionist. A business that wants its calls handled, messages taken and appointments booked wants an answering service, which is a different product at a different price. A business that needs call recording, queues, agent dashboards or CRM integration wants a contact centre platform. Auto Attendant is for the case where the call should simply reach the right pocket.

Keeping personal numbers off the internet

The business number is the only number a caller ever sees. Personal mobile numbers are never displayed and never given out, which is what lets an owner put a number on a website, an invoice, a van or a Google Business Profile without handing a personal line to everyone who finds it. An existing advertised number can be ported across and kept, and the old line keeps working while the port is in progress.

Work with Auto Attendant

Visit [Auto Attendant](#) to see [how it works](#), [how it compares](#) to a personal mobile, Google Voice and a full phone platform, and the current [pricing](#).

Telephone number portability, emergency calling and caller-ID rules differ by country and change over time. Articles published here describe general practice and cite primary regulator and carrier sources; they are not a guarantee of any timeline, and they are not legal or regulatory advice for a specific business.

Website: <https://autoattendant.io>

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.