



AUTO ATTENDANT / RESEARCH & PRACTICAL GUIDANCE

Phone Toll Fraud: How to Protect a Small Business Line

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 · toll fraud · international revenue share fraud · pbx hacking · call forwarding fraud · wangiri one ring scam

Original article: <https://autoattendant.io/articles/phone-toll-fraud-business-how-to-prevent>



In this article

1. [What toll fraud is](#)
2. [Three ways it reaches a small business](#)
3. [How Canadian carriers block Wangiri and other fraud](#)
4. [Who pays when it happens](#)
5. [Controls that work](#)
6. [Staff script for missed calls and odd voicemails](#)
7. [If you think it is happening now](#)
8. [Monthly 10-minute checklist](#)
9. [FAQ](#)

What toll fraud is

Toll fraud is someone running up call charges on your account so that they, or a partner, get paid. One carrier's policy puts it in a single line: "Toll fraud is the theft of long-distance service" ([Summit Broadband, Toll Fraud Policy](#)).

The money usually comes from **international revenue share fraud (IRSF)**. Some international and premium number ranges earn a share of every minute of traffic that reaches them. A fraudster gets hold of such numbers, then pushes as many long calls as possible to them, from your phone system, your voicemail, your forwarding settings, or your staff calling back a "missed call." The number holder collects the termination revenue; you get the bill. The New Zealand Telecommunications Forum's industry guideline describes the fraudster as receiving "a share of the revenue from termination charges obtained by the number range holder" ([NZ TCF IRSF Prevention Guidelines, 2016](#)). Twilio's documentation says the owners of the targeted numbers "receive revenue for every minute" of calls placed to them ([Twilio, Voice Dialing Geographic Permissions](#)).

The same guideline groups several attacks under "revenue share fraud": PABX (phone system) hacking, IRSF, Wangiri fraud, VoIP hacking and voicemail hacking ([NZ TCF](#)).

How big is it? The Communications Fraud Control Association (CFCA) estimated telecom fraud losses of \$38.95 billion in 2023, about 2.5% of telecom revenues, and listed "PBX Fraud" among the top five fraud methods ([CFCA, November 13, 2023](#)). That number covers all telecom fraud worldwide, mostly losses borne by carriers, so treat it as a sign of scale, not of your personal risk.

This guide is for small businesses in the US and Canada, as of October 2026. It is educational, not legal advice.

Three ways it reaches a small business

1. A hacked phone system or VoIP account

The classic case is an on-premises phone system (PBX) or a hosted VoIP account whose credentials are guessed or stolen. Attackers then place international calls through it, often outside business hours. One US carrier's guidance warns that criminals "often will direct their heaviest assaults on your network when vigilance is at its lowest", meaning nights, weekends and holidays, and lists remote access features such as Direct Inward System Access (DISA) and the remote maintenance port as entry points ([FirstLight Fiber, Mitigating International Toll Fraud](#)).

For a cloud phone account, the equivalent is a stolen login or API key. Twilio's advice to its own customers is to "Use 2FA to protect against account-takeovers and keep API keys private" ([Twilio](#)).

2. Voicemail, auto-attendant and forwarding features used as a dial-out

Features that can send a call outward are the weak points. FirstLight says "Voicemail and Auto Attendants are common vulnerability points" and tells customers to "Ensure outbound access is not enabled on your auto attendant" and to delete inactive voicemail accounts ([FirstLight](#)). The NZ guideline's customer checklist includes "Disabling PABX ports and features that are not used (e.g. remote call-forwarding)" and making sure voicemail PINs are secure ([NZ TCF](#)).

Why forwarding matters: when a hosted system forwards a call to another phone, it typically creates a second, outbound call. Twilio's billing note describes "An inbound leg from the caller to your Twilio number" and "An outbound leg from Twilio to the number you are forwarding the call to," each billed per minute ([Twilio Support, call forwarding charges](#)). So if someone can change where your line forwards (for example, to an international premium number), every inbound call becomes a paid outbound call. (*Editorial note: this is the general billing structure; whether your plan charges for the forwarded leg depends on your provider.*)

3. Wangiri (one-ring) callbacks

Wangiri, the one-ring scam, needs no hacking at all. An automated dialer calls huge numbers of phones, lets them ring once, and hangs up, hoping someone calls back ([Trend Micro with Europol](#)). The FCC's guide explains the trap: "If you call back, you risk being connected to a phone number outside the U.S.," and "you may wind up being charged a fee for connecting, along with significant per-minute fees for as long as they can keep you on the phone," shown on the bill as "premium services, international calling, or toll-calling" ([FCC, 'One Ring' Phone Scam](#)).

The numbers can look domestic. The FCC notes that "232" goes to Sierra Leone and "809" goes to the Dominican Republic, and that scammers may also spoof caller ID ([FCC](#)). FirstLight makes the same point for business phone systems: "Calls that do not start with 011 can also be international and are often overlooked in security arrangements" ([FirstLight](#)).

In a business, the risk is the helpful employee who returns every missed call, or the voicemail that says "call us back about your delivery" at an unfamiliar number. The FCC mentions exactly that variation: fake voicemails urging a call back to "schedule a delivery" or about a "sick" relative ([FCC](#)).

How Canadian carriers block Wangiri and other fraud

In Canada, a carrier needs CRTC approval under section 36 of the Telecommunications Act to block calls. Two decisions show how this developed:

- **Telecom Decision CRTC 2020-125 (16 April 2020):** Bell Canada and its affiliates asked for urgent approval to block verified Wangiri calls during the early COVID-19 network surge. Bell explained that the calls go mostly to mobile subscribers, appear to come from overseas, and ring "only once or twice" in the hope of a callback; it recorded more than six million Wangiri calls on its networks between 16 and 20 March 2020 alone. The CRTC approved blocking verified Wangiri calls until 1 June 2020 ([CRTC 2020-125](#)).
- **Telecom Decision CRTC 2021-403 (9 December 2021):** The CRTC approved Bell's move from a trial to a permanent call-blocking mechanism for verified fraudulent calls. The system uses artificial intelligence to flag traffic anomalies; flagged activity is reviewed, and verified fraud is blocked at the network level. The decision records 1,120,372,443 calls blocked from 15 July 2020 to 16 October 2021, and keeps a redress process for wrongly blocked numbers ([CRTC 2021-403](#)).

Network blocking helps, but it targets known patterns. It does not protect a phone system whose own password has been guessed.

Who pays when it happens

Expect the bill to land on you unless your contract says otherwise. Carrier terms are blunt:

- Summit Broadband: "the customer is responsible for payment of any charges incurred due to fraud (including toll fraud)," "whether known or unknown to the customer" ([Summit Broadband](#)).
- FirstLight: "the security of your company's PBX and its internal processes are beyond FirstLight's scope," and "There is no limit to the potential loss and liability in the event of international toll fraud" ([FirstLight](#)). The same document says the FCC has ruled that the customer is responsible. Read that as the carrier's summary of tariff-era precedent. In *Chartways Technologies, Inc. v. AT&T Communications*, 8 FCC Rcd 5601 (1993), the FCC upheld a 1991 Common Carrier Bureau ruling that a business owed AT&T, under AT&T's tariff, for unauthorized calls that outsiders made through its PBX's remote access feature: the incoming 800 calls because it had subscribed to a service built to let unknown callers in, and the outgoing long-distance calls because the callers got dial tone from its premises, so the calls originated at its numbers. The FCC also found AT&T had no duty to warn the customer about toll fraud. In 2001 it applied the same tariff provisions to another hacked business and called Chartways "dispositive" ([FCC, Gerri Murphy Realty, Inc. v. AT&T Corp., FCC 01-310](#)). The FCC did open a toll fraud rulemaking in 1993 (CC Docket No. 93-292), but, as that 2001 order notes, it never adopted a rule on a carrier's duty to warn. No FCC rule allocates these losses today; your service contract does.

These are two smaller carriers' policies. Read your own provider's terms for "fraud," "unauthorized use" and "toll fraud" before you need them.

What rights you do have (US):

- **Dispute the charge.** Under the FCC's truth-in-billing rule, a carrier's bill must "prominently display" a toll-free number to "inquire or dispute any charges on the bill," and carriers "shall not place or cause to be placed on any telephone bill charges that have not been authorized by the subscriber" ([47 CFR 64.2401\(d\) and \(g\)](#)). Whether fraudulent calls through your own hacked equipment count as "unauthorized" is exactly what carriers dispute; call anyway, and fast.
- **Escalate.** For one-ring charges, the FCC says to "first try to resolve the matter with your telephone company," and if that fails, "file a complaint with the FCC at no cost"; victims of international phone scams can also complain to the FTC ([FCC](#)).

In Canada, start with your provider; if that fails, ask whether the service falls under the Commission for Complaints for Telecom-television Services (CCTS), the independent body that handles complaints about telecom services ([CCTS](#)).

Controls that work

Most of these take an afternoon. Work through them with whoever manages your phones.

Control	What to do	Source
Block international dialing you don't need	"If you do not make international calls, ask your phone company to block outgoing international calls on your line."	FCC
Allow only the countries you call	On cloud platforms, enable only needed countries and only low-risk ranges; Twilio: "Only turn on calling to countries you need to call."	Twilio
Block premium and high-risk ranges	Clearing a high-risk range blocks calls to it.	Twilio
Strong, unique PINs and passwords	Change defaults; no "1234", "1111" or extension numbers; change when staff leave.	FirstLight; NZ TCF
Two-factor authentication on portals	Protects against account takeover.	Twilio
Turn off what you don't use	Remote call forwarding, DISA, remote maintenance access, outbound access from the auto attendant, unused mailboxes.	FirstLight; NZ TCF
After-hours restrictions	Prohibit toll calling at night, weekends and holidays.	FirstLight
Usage alerts	Set alerts on calls or minutes per day; Twilio's example of an anomaly is "5 times more usage on a weekday compared to average usage over the last 3 weeks."	Twilio
Don't return unknown missed calls	Check whether an area code is international before calling back.	FCC

Two more points that are easy to miss:

- **Know who can change forwarding.** Anyone who can edit where calls forward can, in effect, dial out on your account. Keep that permission to one or two people. Our guide to [business phone call routing permissions](#) covers how to set that up.
- **Protect the account itself.** The same weak portal password that enables toll fraud can enable a number hijack. See our research note on [port-out fraud and SIM swaps](#).

Staff script for missed calls and odd voicemails

Put this next to the front-desk phone:

"We don't call back unknown numbers from a single ring. If a voicemail asks us to call an unfamiliar number about a delivery, a prize or a relative, we look up the company's real number instead. If an area code is one we don't recognize, we check it before dialing. Numbers starting 011, and some three-digit codes that look like US area codes (809 is the Dominican Republic), are international."

FirstLight also suggests teaching staff to flag warning signs such as "Excessive hang-ups," "Dead air," and "Frequent calls requesting nonexistent extensions" ([FirstLight](#)).

If you think it is happening now

1. **Call your carrier's fraud or business support line immediately.** Ask them to block international and premium calling on the account. Summit Broadband, for example, asks customers to be ready to explain how the fraud occurred and what equipment changes were made ([Summit Broadband](#)).
2. **Change every password and PIN:** portal, voicemail, phone system admin, SIP credentials.
3. **Check and reset forwarding** on every line and mailbox.
4. **Call your phone system vendor**, if you have one.
5. **Write down timings and amounts**, and ask for the call detail records.
6. **Report it.** FirstLight advises notifying state police, the FBI and your insurer ([FirstLight](#)). In Canada, fraud can be reported to local police or the Canadian Anti-Fraud Centre ([CAFC](#)).
7. **Dispute the charges in writing** using the number on your bill ([47 CFR 64.2401\(d\)](#)).

Monthly 10-minute checklist

- ☐ Scan last month's bill or call log for international, premium or after-hours outbound calls
- ☐ Confirm international and premium calling are still blocked (or limited to the countries you need)
- ☐ Check forwarding destinations on every line and mailbox
- ☐ Remove users, mailboxes and extensions for people who have left
- ☐ Confirm 2FA is on for every admin login
- ☐ Check that usage or spend alerts are still going to a monitored inbox
- ☐ Remind front-desk staff about one-ring callbacks (see the [spam call guide](#) for blocking options)

FAQ

Is toll fraud covered by insurance? It depends on your policy; some cyber or crime policies mention telecom fraud, others exclude it. No general rule applies, so ask your broker. FirstLight's guidance lists notifying your insurance carrier as one of the first steps ([FirstLight](#)).

Should I call back a number that rang once? Not if you don't recognize it. The FCC's advice is: "Don't answer or return any calls from numbers you don't recognize" ([FCC](#)).

Who do I report to? In the US, your carrier first, then the FCC (billing) or the FTC (scams), per the FCC guide ([FCC](#)). In Canada, your carrier, then local police or the CAFC ([CAFC](#)).

Does a cloud phone service remove the risk? No. It removes the on-site PBX ports, but the account login, voicemail PINs and forwarding settings are still targets, and forwarded calls can still create outbound charges ([Twilio Support](#)).

Is it only an international problem? Mostly, because the revenue comes from international and premium ranges, but some of those ranges sit behind codes that look like ordinary North American area codes ([FCC](#)).

For what it's worth, Auto Attendant forwards calls only to US and Canadian numbers and places no outbound calls of its own, as a guard against this kind of fraud.

Source links

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

1. <https://summit-broadband.com/privacy-terms/toll-fraud-policy>
2. <https://www.tcf.org.nz/wp-content/uploads/Documents-Telecommunications-International-Revenue-Share-Fraud-Prevention-Guidelines.pdf>
3. <https://www.twilio.com/docs/voice/tutorials/voice-dialing-geographic-permissions>
4. <https://cfca.org/telecommunications-fraud-increased-12-in-2023-equating-to-an-estimated-38-95-billion-lost-to-fraud>
5. https://www.firstlight.net/wp-content/uploads/2021/04/Mitigating_International_Toll_Fraud.pdf
6. <https://support.twilio.com/hc/en-us/articles/223132367-How-Much-am-I-Charged-for-Call-Forwarding-with-Twilio>
7. <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/toll-fraud-irsf-criminals-monetize-hacked-phones-iot-devices-telecom-fraud>
8. <https://www.fcc.gov/consumers/guides/one-ring-phone-scam>
9. <https://crtc.gc.ca/eng/archive/2020/2020-125.htm>
10. <https://www.crtc.gc.ca/eng/archive/2021/2021-403.htm>
11. <https://docs.fcc.gov/public/attachments/FCC-01-310A1.txt>
12. <https://www.ecfr.gov/current/title-47/section-64.2401>
13. <https://www.ccts-cprst.ca>
14. <https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm>

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.