

Trusted Voice for the Help Desk

*You call to help, but no one believes you anymore.
How guaranteed number identity restores trust in your helpdesk.*

For IT managers, service directors and compliance managers in helpdesk and service organizations

Published by
Trusted Voice a trademark of Trusted B.V.
Stadhuisplein 10, Eindhoven • www.trustedvoice.eu
May 2026

The helpdesk dilemma: you call to help, but no one believes you anymore

Your helpdesk calls a customer about a critical software update. An end user calls back after a password reset. A service agent contacts you about an open ticket. Each and every one of these are legitimate, day-to-day actions of any professional helpdesk.

But more and more often, something worrying happens: the customer does not answer. The end user hangs up as soon as he hears 'helpdesk'. The employee doesn't trust the conversation — and does exactly what security experts taught him: hang up on unexpected calls.

That is not a fault of the customer. This is the direct result of years of telephone fraud in which criminals pretend to be helpdesks — and where the phone number on the display no longer offers any guarantee.

The 'Microsoft employee' — the face of helpdesk fraud

It started in 2008 and it doesn't stop. The most notorious variant of helpdesk fraud is the so-called 'Microsoft scam': a caller pretends to be a Microsoft employee, warns of viruses or security problems, and asks the victim to install software that allows the criminal to access the computer remotely. What follows is theft of bank details, personal information and not infrequently direct financial damage.

But the Microsoft scam is no longer the only variant. Criminals nowadays call on behalf of internet providers, software suppliers, cloud platforms and — increasingly — on behalf of the internal IT helpdesk of the company where the victim himself works. They use urgency ('your account has been hacked'), authority ('I am calling on behalf of IT security') and familiar terminology to gain the trust of the recipient.

The tactics have been refined. In 2023, attackers from the hacker group Scattered Spider managed to gain access to the network of MGM Resorts — a company with thousands of employees and advanced security systems — through a fake helpdesk call. The damage: hundreds of millions of dollars. The point of attack: a single phone call to the IT helpdesk.

The two-sided problem: fraud to and from the helpdesk

Helpdesk fraud has two faces, both of which affect the sector:

Customer fraud — Criminals call your customers and pretend to be your help desk. They use your organization's real phone number on the recipient's display (caller ID spoofing). The customer sees the trusted number, answers, and follows instructions that lead to data or money theft. Your organization hasn't called anyone — but it's bearing the reputational damage.

Help desk fraud — Criminals call your help desk pretending to be an employee or customer. They ask for a password reset, an MFA adjustment, or access to a system. They know names, ticket numbers and internal terminology. Your helpdesk agent helps — as he is trained — and unknowingly opens the door for the attacker.

In both cases, the result is identical: the word 'helpdesk' is associated with fraud. And that affects every organization that provides service over the phone.

The crisis of confidence in numbers

The extent of helpdesk fraud is not abstract — it is concrete figures that affect the daily reality of service organizations:

€ 26 million	stolen via helpdesk fraud in the Netherlands in 2025 — up from €23 million in 2024 (source: Dutch Banking Association)
5.900	victims of helpdesk fraud in the Netherlands in 2025, despite growing awareness (source: NVB)
€ 850 million	estimated global annual damage from caller ID spoofing (source: Europol, 2025)
90%	of incoming international calls to Finnish telecom operator Elisa were found to be fraudulent – before the introduction of anti-spoofing measures (source: Europol)
87%	of Americans refuse to answer if they don't recognize the caller (source: Truecaller)

What this means for your helpdesk

The consequences of helpdesk fraud extend beyond the direct victims. They go to the heart of any help desk operation: the ability to communicate effectively with customers and end-users.

Customers no longer answer. The advice from the police, banks and consumer organizations is unequivocal: do not answer when an unknown or unexpected number calls. That advice is understandable — but it also affects your legitimate help desk. Proactive service calls, callbacks, and escalation calls aren't answered. Your first-call resolution drops; Your costs increase.

Customers distrust your employees. Even when a customer does answer, trust is fragile. 'Are you really calling from the helpdesk?' is a question your employees hear more and more often. Every second spent convincing the customer that the conversation is legitimate is at the expense of the actual service.

Employees are targeted. Help desk agents are trained to help. Criminals take advantage of this by calling the helpdesk themselves and pretending to be a colleague or end user. A password reset, an MFA change — the helpdesk performs it in good faith. The attacker is in.

Reputational damage is structural. 'Your number was used to scam me' — that complaint cannot be solved once with a letter of apology. The trust that a customer had in your organization has been damaged. And on social media, one negative experience is shared with hundreds.

Question for your organization: How many customers did you not reach in the past quarter — not because they were unreachable, but because they no longer trusted your number?

Why this doesn't go away on its own

The core of the problem is not the behavior of criminals — that's a given. The core lies in the architecture of the telephony network itself. The public telephone network (PSTN) was built decades ago with one goal: to make calls. Authenticating the caller was not a design requirement.

To this day, any connected carrier worldwide can send any phone number — and the network accepts this without verification.

Caller ID spoofing — the forgery of the number that appears on the recipient's display — is therefore not a security hole. It is a property of the network. And that property cannot be repaired with filters, blocklists or customer information.

The legislator moves — and expects you to move with it

The European and Dutch legislators leave no room for misunderstanding: secure communication will be a demonstrable obligation, not an obligation to make efforts. For helpdesks that provide service by telephone, three developments are directly relevant:

Digital Networks Act (DNA) — January 2026. The European Commission requires telecom providers to take harmonised measures against caller ID spoofing. As a Regulation, the DNA is directly applicable in all 27 EU Member States. BEREC will be tasked with providing guidance on technical measures to effectively protect end-users.

Cybersecurity Act (NIS2) – Spring 2026. The Dutch implementation of the European NIS2 Directive makes digital resilience a legal duty of care for organizations in vital sectors. Communication security is explicitly within the scope. Directors will be personally responsible.

DORA — Digital Operational Resilience Act. DORA sets requirements for the operational resilience of digital systems and communication processes, specifically for financial institutions. The reliability of outbound communication channels falls under the scope of DORA compliance.

In addition, Europol labels caller ID spoofing as a European security priority and calls for EU-wide technical standards and an international traceback system. The message is clear: the current situation is no longer tenable.

For helpdesks that operate in the financial sector, healthcare, government or ICT services, this means in concrete terms: you must be able to demonstrate that your outgoing communication is secure and verified. 'We are doing our best' will soon no longer be an answer.

The solution: guaranteed number identity for your helpdesk

Trusted Voice is designed with one belief in mind: every organization deserves the assurance that its callers are who they say they are — and so do its customers. Not by reducing the problem with filters or information, but by excluding it at the source.

How it works — help desk specific

Trusted Voice operates as a closed, telecom-grade network that is completely separate from the public telephony infrastructure. Every call your helpdesk makes via Trusted Voice is encrypted before it is forwarded. The identity of the caller — your agent, your system — is authenticated to the network. A call that fails this verification will not be accepted.

The result: when your helpdesk calls, it's arguably your helpdesk. Not because the customer has to believe it — but because the network guarantees it.

What this means for your day-to-day operations

Higher accessibility. Customers and end users record because they know the call is authenticated. Your proactive service calls, callbacks, and escalations are coming back on.

No 'are you really the helpdesk?' conversations more. Your employees spend their time on service, not on proving their identity. The average talk time decreases; customer satisfaction increases.

Protection against impersonation. Criminals will no longer be able to spoof your helpdesk number via the Trusted Voice network. Spoofing is technically excluded — not made difficult, but made impossible.

Compliance file out of the box. Every call is logged with full audit trail: who called, when, verified by the network. You can demonstrate that your communications are secure — to regulators, auditors and customers.

No adjustments at the customer's site. The recipient does not have to do anything. No installing an app, no creating an account, no change in behavior. The call arrives at a regular phone number, but verified.

Integration in weeks, not months. Trusted Voice connects to your existing call center software, CRM, and communications platform through a simple API integration. No infrastructural revision required.

Comparison: Without vs. with Trusted Voice

Characteristic	Helpdesk today	Helpdesk with Trusted Voice
Number identity	Unverified — anyone can spoof your number	Encrypted Verified Before Connection
Customer trust	Falling — 'is this really the helpdesk?'	Guaranteed — the network confirms identity
Spoofing risk	High — caller ID is easy to spoof	Excluded — technically impossible
Accessibility	Customers are recording less and less	Higher pickup rate through verified calling
Compliance	Not demonstrably safe	Audit trail per call — NIS2, DORA, GDPR-ready
Implementation	N/A	API integration — up and running in weeks

Conclusion: from distrust to trust

The distrust of calls from 'the helpdesk' is not irrational — it is learned. For years, consumers, employees and citizens have fallen victim to fraudsters posing as helpdesks. From the infamous Microsoft scam to sophisticated attacks on corporate networks via fake IT support: the word 'helpdesk' has become infected.

That problem cannot be solved with better training, stronger passwords or smarter filters. The problem is in the telephony network itself — and that network cannot be repaired.

Trusted Voice offers a fundamentally different approach: guaranteed number identity, verified at the source, within a closed network where spoofing is technically impossible. For your helpdesk, this means: higher accessibility, more trust, less risk of fraud and a demonstrable compliance file.

The choice in front of you
Keep calling through a network that can't guarantee your identity — and accept that customers trust you less and less. Or switch to authenticated calling now — and restore the trust your help desk deserves.
Contact us for a no-obligation consultation: www.trustedvoice.eu • Stadhuisplein 10, Eindhoven

© 2026 Trusted Voice B.V. — All rights reserved. This sector narrative is based on the white paper 'Trust on the line' and publicly available sources including Europol, the Dutch Banking Association, the Fraud Help Desk, the NCSC and the Digital Trust Center.