

When your customer no longer answers

How caller ID spoofing not only enables fraud, but also undermines trust in legitimate bank contact. And why guaranteed number identity is the key to accessibility, cost reduction, and compliance

For directors, compliance officers and risk managers in the financial sector

Trusted Voice is a trademark of Trusted B.V.

Stadhuisplein 10, Eindhoven • www.trustedvoice.eu

July 2026

The double threat: when your number is no longer trusted

Imagine: a customer receives a phone call. The number on his screen is identical to the number on his debit card. A friendly voice asks him to confirm a suspicious transaction. The customer trusts the number and follows the instructions. Within minutes he has lost thousands of euros. Your bank has not called anyone. It was a fraud.

Now imagine the opposite: your own employee calls that same customer, this time for real, to verify an unusual transaction. The customer sees the number, hesitates, and does not answer. The employee tries again. And again. After three attempts, he registers the contact as 'not reached' and moves on to the next one. The customer later calls back via the general line, frustrated and suspicious. The transaction has now gone through.

These are two sides of the same coin, and both are caused by caller ID spoofing: the act of forging the phone number that appears on the recipient's display. It is not a future scenario. It happens today, every day, all over Europe. And it hits the financial sector the hardest. Not only due to direct fraud damage, but also due to a growing inaccessibility that drives up operational costs and undermines customer contact.

Criminals misuse numbers of banks, hospitals and government agencies to deceive people. The result is no longer just direct financial damage. It is a fundamental erosion of trust in the telephone channel. When customers no longer dare to answer when their bank calls, the institution loses its most important instrument for personal customer contact, with all the consequences that this entails for accessibility, customer satisfaction and operational efficiency.

The size: figures that don't lie

Europol published an alarming position paper on caller ID spoofing in October 2025, based on information from police forces from 23 EU member states. The conclusions are not bad:

- The global annual damage caused by caller ID spoofing is estimated at €850 million.
- In 64% of all reported fraud cases, phone or text message is the primary attack channel.
- Some 400 million Europeans remain vulnerable to spoofing-related fraud.
- Criminal networks now offer 'spoofing-as-a-service'. Ready-made services that allow anyone to pretend to be a bank or government agency.
- In the Netherlands, the Fraud Help Desk registered more than 44,500 fraud reports in the first half of 2025 with a damage of €26.8 million; The number of reports of telephone fraud increased by 250% compared to a year earlier.
- The Dutch Central Bank reported a 30% increase in the number of fraud cases in the payment system in 2025, to approximately 658,000 cases with €198 million in damage. In European credit transfers, the category that includes bank helpdesk and investment fraud, the number of fraud cases increased by 55% to 129,000, amounting to €148 million (compared to €121 million in 2024).
- In bank helpdesk fraud, in which criminals pretend to be bank employees with a spoofed bank number, scammers stole almost €26 million in 2025. €3 Million more than in 2024 while the number of victims fell to almost 5,900. The damage per victim is therefore increasing.
- According to the AFM (report 'From pyramid to iceberg', December 2025), the damage caused by investment fraud is estimated at €150 to €750 million per year, while only €75 million was reported to the police. It is estimated that only 5 to 17% of the victims come forward.
- According to the Dutch Banking Association, almost 70% of all online fraud nowadays starts on social media, after which the telephone channel and spoofing are used to build trust.

Behind each of these figures are thousands of individual stories of people who have lost confidence in their own phone, and in their bank.

The invisible cost: when your own employees can no longer make it through

The direct damage of spoofing fraud is visible in the figures. But there is a second, less visible but at least as drastic consequence: the growing distrust of customers makes it increasingly difficult for banks to reach their own customers by telephone.

Bank employees experience this on a daily basis. Customers answer less and less often when they are called. Even when the conversation is legitimate and urgent. And even when a customer does answer, it takes more and more time and effort to gain trust. 'How do I know that you are really from my bank?' is no longer an exception, but the standard response. Employees have to work through a wall of mistrust before the actual conversation can begin.

The asymmetry that distorts the image

An underexposed part of this problem is the skewed relationship between how often a bank actually calls and how often criminals pretend to be that bank. Banks call their customers sparingly and with a concrete reason, a suspicious transaction, an expired document, an outstanding action. Spoofers do the opposite: they call on a scale, repeatedly, and often with a compelling urgency to put pressure on victims.

As a result, the telephone contact that a customer attributes to "the bank" is statistically more and more likely to be fraud than a legitimate conversation. Every spoofed call, regardless of whether the fraud ultimately succeeds, thus colors the customer's image of the bank. The bank is associated with intrusive, manipulative telephone approaches, through no fault of its own, while it hardly makes any calls itself. This is a form of image damage that is separate from direct fraud damage: it affects confidence in the bank's telephone channel, even among customers who have never been victims themselves. Purely because the "number of the bank" has now become synonymous with a well-known fraud pattern.

The consequences are tangible and measurable:

- Declining reachability: contact rates for outbound call attempts are structurally declining, requiring more attempts to reach the same customer.
- Rising call costs: Longer conversations due to trust building, more repeat attempts, and higher operational load per successful customer contact.
- Negative customer experience: Customers who do pick up experience the conversation as unpleasant due to the necessary verification steps — impacting customer satisfaction and NPS.
- Missed interventions: In the event of fraud alerts, late payments, or compliance-related verifications, failure to reach a customer can have direct financial and regulatory consequences.

And this problem will only get worse in the coming years. Increasing data breaches mean that more and more customer data is being exposed, allowing fraudsters to act more credibly. At the same time, the rapid development of AI, from voice cloning to real-time deepfakes, is making spoofing and social engineering increasingly sophisticated and difficult to recognise. The combination of these trends means that the trust problem is growing exponentially: the more convincing the fraud, the more suspicious the customer, the more difficult the legitimate contact.

What the healthcare sector teaches us about the urgency

The healthcare industry is the most striking example of why caller ID spoofing can no longer be considered a purely financial problem. In hospitals and GP practices, the telephone is not a sales channel, it is a healthcare channel. Doctors call patients with results. Pharmacists call about medication. District nurses call to confirm appointments.

When criminals spoof these numbers, something different happens than with a spoofed bank number. There is not only financial risk, but also direct risk to public health:

- Patients no longer answer the phone when the hospital calls, not even for critical results or appointments.
- Criminals pretend to be general practitioners or health insurers to extract medical data, social security numbers or bank accounts.
- Vulnerable elderly people, the largest group of care users, are also the most vulnerable target group for telephone fraud.
- Healthcare staff are spending more and more time convincing patients that they are actually an employee of the hospital.

This is a cautionary example for the financial sector. And the parallel goes beyond safety alone. Just as healthcare staff spend more and more time proving their identity, bank employees experience the same thing: longer calls, lower admission rates, higher costs per successful contact. The pattern we see in healthcare, declining trust in legitimate telephone contact, with direct consequences for accessibility and operational efficiency, is exactly the same pattern that is now unfolding in banks.

Europol warns that this will become the new normal: a society in which citizens no longer trust a single phone call, regardless of who is calling. The parallel between healthcare and finance makes one thing painfully clear: this is not a sector problem. It is a system problem. And it requires a system solution.

The regulatory landscape is shifting. And fast

For years, caller ID spoofing was a grey area in European regulations. That's over. A series of new and upcoming regulations make protection against spoofing a hard legal obligation — with direct consequences for financial institutions.

PSD3 and the Payment Services Regulation (PSR): liability shift

The new Payment Services Regulation (Article 59 PSR) introduces a compensation scheme for spoofing fraud for the first time. When a criminal pretends to be an employee of a bank, using the real phone number, email address or name of the institution, and the customer transfers money as a result, the bank is obliged to refund the full amount. Under the current PSD2, this type of fraud is not protected because the customer technically 'authorises' the payment himself. That gap is now being closed.

For banks, this means a fundamental shift: the financial risk of spoofing fraud shifts from the customer to the institution. The burden of proof to refuse repayment, the bank must prove that the customer acted with gross negligence, becomes considerably heavier. Prevention is no longer a service, but a financial necessity. Banks that can demonstrate that they technically exclude spoofed calls have a considerably stronger burden of proof.

NIS2 and DORA: communication security as a duty of care

The NIS2 Directive (Cybersecurity Act) requires organizations in vital sectors, including the financial sector, to demonstrably secure their communication channels. It is not an obligation to perform to the best of one's ability, but an obligation to achieve a result: you must be able to demonstrate that you have taken adequate measures to guarantee the integrity and authenticity of your communication.

The Digital Operational Resilience Act (DORA) also sets requirements for the operational resilience of financial institutions, including the reliability of communication processes with customers. A telephone channel that can be spoofed structurally does not meet this standard in all likelihood.

EU Digital Networks Act: anti-spoofing as a legal obligation

The proposed EU Digital Networks Act, expected in 2026, will make harmonised anti-spoofing measures mandatory for all EU member states. In combination with the ProtectEU strategy, in which Europol explicitly labels caller ID spoofing as a European security priority, a clear course is emerging: organizations that do not act now will soon be left behind.

The message is clear: the European legislator requires financial institutions to protect their telephone identity. Not as a best practice, but as a compliance obligation. The question is not whether you should act, but how quickly.

Why existing solutions fall short

Many organizations rely on reactive measures: spam filters, call analytics and awareness campaigns. These tools have value, but they all share the same fundamental limitation: they respond after a spoofed phone call has already reached the network.

The reason for this is structural. The Public Switched Telephone Network (PSTN), the global telephone network, was built decades ago without any form of identity verification. Any telecom provider can send any number, and the network shows this without control. Standards like STIR/SHAKEN, mandatory in the US, only work on specific IP-based segments and lose their authentication once a call crosses international borders or older equipment. The European Union and the United Kingdom have assessed this approach as insufficient.

Monitoring tools can flag suspicious patterns, but they can't authenticate the number itself. As long as the PSTN accepts unverified numbers, spoofed calls will continue to look legitimate the moment they come in. And it is precisely that moment, the first second that the number appears on the display, that determines whether the victim answers.

Trusted Voice: Guaranteed number identity at source

The problem of trust surrounding telephone customer contact has a structural cause and therefore requires a structural solution. Trusted Voice offers just that. Instead of detecting spoofed calls after they reach the network, Trusted Voice makes spoofing technically impossible. Even before the connection is established. But the value goes beyond fraud prevention: when customers see that an incoming call is verified and genuine, the doubt disappears. They record. Trust has been restored and with it the effectiveness of the entire outbound contact process.

The business case: concrete benefits for the financial sector

- **Elimination of spoofing fraud:** Criminals can no longer misuse your number to call customers. In combination with the PSD3/PSR liability shift, this prevents direct financial damage to your institution.
- **Higher reachability:** Customers see that the call is verified and pick up. The contact rate for outbound call attempts increases, which means fewer repeat attempts are needed and employees work more effectively.
- **Lower operational costs:** shorter calls because the trust threshold is removed, fewer repeat attempts, lower telephony and personnel costs per successful customer contact. The positive business case is directly measurable in the operational P&L.
- **Improved customer experience:** No more suspicious start to the conversation. Customers experience your outbound contact as professional and reliable, with a direct impact on customer satisfaction and NPS.
- **Brand protection:** Criminals can no longer borrow your bank's identity to deceive customers. Because every call from your institution is proven to be genuine, you prevent your own number

from becoming synonymous with fraud through no fault of your own, and you protect the trust that customers place in your brand.

- Compliance readiness: Trusted Voice meets the requirements of DORA, NIS2 and ISO 27001. Each verified call creates a complete audit trail, making audits easier and reducing regulatory risk.
- Future-proofing: As AI-driven fraud becomes more sophisticated and data breaches increase, the value of cryptographically proven number identity grows with it. An investment that pays for itself more and more.

The time to act is now

Caller ID spoofing is no longer a technical curiosity. It is an industrialized form of fraud that causes hundreds of millions of euros in damage every year. But the impact extends beyond fraud alone. The growing distrust in telephone contact is undermining the daily operations of financial institutions: customers who do not answer, employees who have to work their way through verification walls, rising costs per customer contact, and as the healthcare sector shows, entire communication channels that are losing their effectiveness. And this problem is only getting worse due to increasing data breaches and AI-driven fraud.

Regulations are shifting at a rapid pace. The PSD3/PSR shifts financial liability to the institution. NIS2 and DORA make communication security a duty of care. The EU Digital Networks Act will make anti-spoofing measures mandatory. Europol labels it as a European priority. Organizations that do not act now will soon have to explain why they did not do it.

Trusted Voice offers a proven, structural solution that addresses both problems at the same time: guaranteed number identity at the source, through a closed network that does not detect spoofing but eliminates it. The result is not only a safer channel, but also a more effective channel: higher reach, shorter calls, lower costs, better customer experience. No app for the receiver, no replacement of systems, no complexity for the end user. However, a complete audit trail, compliance with the strictest European standards, and a measurable positive business case. The choice is clear: will you continue to rely on a phone network that does not verify identity with rising fraud costs, declining accessibility, and growing compliance risks? Or are you taking the initiative to secure your customer communications, reduce your operational costs, and restore the trust that your customers, your regulator, and your reputation deserve?

Want to know more or schedule a meeting?

Contact Trusted Voice for a personalized explanation or a demonstration of guaranteed number identity for your organization.

www.trustedvoice.eu

References

- Europol – Position Paper on Caller ID Spoofing, October 2025
- Fraud Helpdesk Netherlands — Half-year results 2025
- De Nederlandsche Bank — Fraud in the payment system, figures 2025
- Dutch Banking Association – Bank helpdesk fraud figures 2025
- AFM — From pyramid to iceberg: the invisible extent of investment fraud in the Netherlands, December 2025
- European Commission – Payment Services Regulation (PSR), Article 59
- NIS2 Directive (Cybersecurity Act) and Digital Operational Resilience Act (DORA)
- EU Digital Networks Act – legislative proposal 2026
- Trusted Voice — www.trustedvoice.eu