

# The Machine Era of Spam Calls

How Automated Fraud Scaled Globally in 2025

## MOST SPAMMED COUNTRIES

-  Indonesia
-  Chile
-  Vietnam

**68 Billion**

spam and fraud calls  
identified globally in 2025



**79%**

of all unknown calls were  
spam or fraud in Indonesia



**500M+**

users protecting each other  
in real time



# The Machine Era of Spam Calls: How Automated Fraud Scaled Globally in 2025

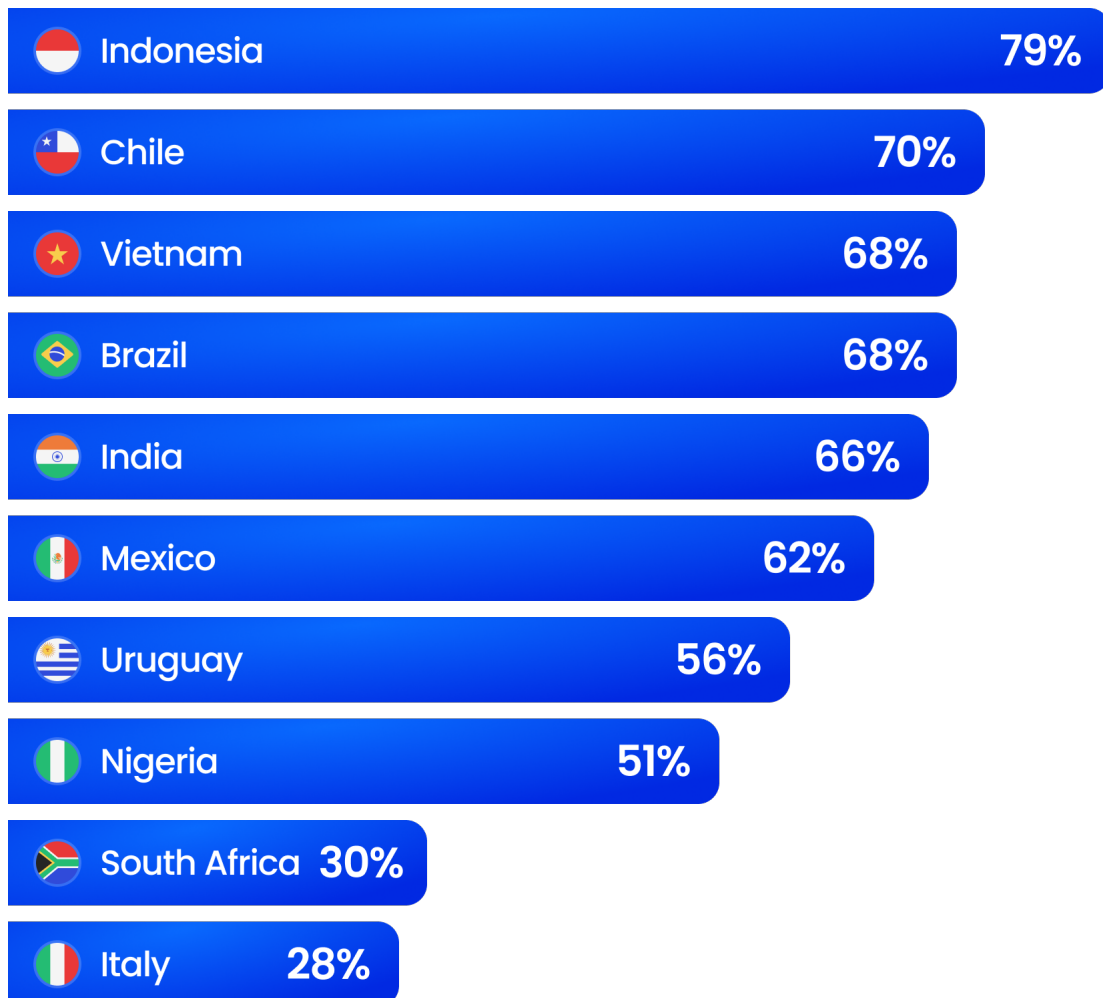
A Truecaller Analysis of Communication Fraud and the Rise of the Machine Era

A phone call used to mean a person on the other end. That's no longer a safe assumption.

Globally, Truecaller identified over 68 billion calls as spam or fraud. In markets like Indonesia and Chile, more than 7 in 10 unknown calls are identified as spam. Spam and fraud have moved from human callers to automated systems running at a scale no person could match. The machine era of spam calls is officially here.

## The Global Landscape: Top 10 Most Spammed Countries











The following ranking identifies the countries where users experience the highest percentage of spam calls relative to their total unknown calls. This metric reflects the spam intensity of a market. In other words, if a user receives 10 calls from numbers outside their contacts and 7 of them are spam, that market has a spam intensity of 70%.



# Who is Calling?

## The 2025 Category Breakdown

While spam intensity tells us how often the phone rings, the category breakdown reveals the intent behind the calls. In 2025, we saw a clear divide between markets driven by sales and those dominated by high-stakes fraud.

 <b>Indonesia</b>	Financial services <b>42%</b>	Scams <b>21%</b>	Sales/Telemarketing <b>16%</b>
 <b>Chile</b>	Debt collection <b>38%</b>	Financial services <b>22%</b>	Scams <b>10%</b>
 <b>Vietnam</b>	Sales/Telemarketing <b>45%</b>	Financial services <b>13%</b>	Scams <b>10%</b>
 <b>Brazil</b>	Telecom <b>48%</b>	Financial services <b>10%</b>	Scams <b>10%</b>
 <b>India</b>	Sales/Telemarketing <b>36%</b>	Financial services <b>18%</b>	Scams <b>12%</b>
 <b>Mexico</b>	Financial services <b>41%</b>	Debt collection <b>11%</b>	Scams <b>10%</b>
 <b>Uruguay</b>	Scams <b>33%</b>	Financial services <b>13%</b>	Sales/Telemarketing <b>10%</b>
 <b>Nigeria</b>	Telecom <b>35%</b>	Sales/Telemarketing <b>10%</b>	Scams <b>6%</b>
 <b>South Africa</b>	Insurance <b>14%</b>	Financial services <b>10%</b>	Debt collection <b>6%</b>
 <b>Italy</b>	Telecom <b>13%</b>	Sales/Telemarketing <b>10%</b>	Financial services <b>5%</b>

## How Fraud Adapts Locally

The same automation, different tactics. Where financial systems are accessible, spam follows the money. Where debt culture runs high, automated dialers become collection tools. Where carrier trust is built-in, operators become cover.



### Indonesia & Mexico

Financial services top 40% of all spam. Automated systems target users with banking and loan-related lures at high frequency.



### Brazil & Nigeria

Calls from Telcos dominate. Automated outreach from both legitimate carriers and unverified third parties has become the primary source of spam for the user.



### Chile

Debt Collection accounts for 38% of all spam – higher than any other market globally. Automated dialers here are built for financial pressure, not sales.

# The Global Centres of Spam Intensity

South America and Southeast Asia are now among the most targeted regions on earth. In late 2025, Indonesia reached a peak where nearly 80% of all unknown calls were identified as spam, the highest density recorded globally. Taken together, these findings point to a broader global shift – as automated spam scales, trust in unknown calls continues to decline.

## The Americas

Chile



Brazil



Mexico



Uruguay



Peru



## Asia

Indonesia



Vietnam



India



Malaysia



Singapore



## Africa

Nigeria



South Africa



Kenya



Ghana



Ethiopia



## MENA

Egypt



Jordan



Morocco



Saudi Arabia



UAE



## Europe

Italy



France



Spain



United Kingdom



Poland



# Migration to the Southern Cone



In South America, the data shows a shift in activity toward the Southern Cone - specifically Chile and Uruguay. Chile's spam intensity jumped from 51% to 70% in only six months, while Uruguay emerged as a late-year outlier with a sudden 11% spike in the final quarter. This trend highlights how quickly automated calling infrastructure can pivot between regional markets.

## The Rise of Telecom Outreach in Europe

In markets like Italy and the UK, calls from telcos moved into the top three most reported categories by the end of 2025. This is a clear sign that automated outreach from service providers has become a primary source of unknown calls across the region.

For businesses operating in Europe, this creates a direct problem. When calls from telcos dominate the spam landscape, legitimate companies lose the ability to reach customers with confidence. And calls go unanswered. This is where solutions like Truecaller for Business become critical. By giving verified companies a way to confirm their identity on every call, that unknown call turns into a trusted one, giving European businesses a way to reach customers with confidence.

## The MEA Spotlight

**+100 Million** Monthly Active Users in MEA

The MEA region represents one of Truecaller's most dynamic growth frontiers. In late 2025, the combined Middle East and Africa (MEA) region surpassed 100 million monthly active users.

Across the region, a new pattern of spam intensity is taking shape. Egypt leads with 22%, where nearly 1 in 4 unknown calls are now identified as spam. While Sales and Telemarketing remain the primary drivers, Financial services has emerged as a dominant force; users in Jordan and Saudi Arabia are experiencing a rising volume of automated outreach linked to banking and insurance lures.

# 2021 vs 2025

Spam calls identified

**+80%**

37.8 Billion → 68 Billion

User growth in 5 years

**1.5x**

300 Million → 500 Million

Debt collection calls in Chile

**5x**

7% → 38%

In 2021, Truecaller had 300 million users and helped identify 37.8 billion spam calls globally. By 2025, that community had grown to 450 million users and identified over 68 billion spam and fraud calls. Nearly double the volume. And on March 31, 2026, Truecaller crossed 500 million monthly active users, with more than 150 million of those outside of India.

That global shift shows in the data. In 2021, Truecaller was still primarily an India story. Today, the fastest growth is in Latin America, Southeast Asia, and Africa — exactly the regions that dominate the 2025 spam rankings. As the scale of spam has increased, more people are turning to Truecaller to manage it.

The category mix shifted too. In 2021, Sales calls dominated most markets. By 2025, two significant structural shifts emerged. Across Europe and Africa, Telecom-linked outreach has transitioned from a marginal category to a top-three dominance, where automated systems at the carrier level generate volumes that users struggle to distinguish from legitimate service updates. Meanwhile, in Chile, Debt Collection has eclipsed Sales as the primary category — surging from 7% in 2021 to 38% in 2025 — a definitive signal that automated dialers are now being utilized as instruments of financial pressure rather than mere sales outreach.

The machine didn't replace the spammer. It gave them reach they never had before.

## The Nordic Perspective

Sweden does not appear among Europe's most spammed markets — spam intensity sits at around 6% — but the nature of the threat is different, not smaller.

As a high-trust society, Sweden has historically been targeted by more sophisticated fraud. Rather than high-volume automated calls, scams often involve carefully crafted impersonation attempts that exploit trusted institutions and widely used systems like BankID.

What is changing is the convergence of these tactics with the global shift toward automation. Number manipulation — where calls appear to originate from trusted local contacts or organisations — is becoming more common, bringing industrial-scale techniques into a market previously defined by targeted fraud.

For legitimate businesses, this creates a new challenge. As trust in unknown calls declines, even genuine outreach risks being ignored. Solutions like Truecaller for Business and Secure Calls help address this by verifying identity at the point of contact, allowing organisations to reach customers with confidence.

# The Erosion of Trust

When most unknown calls are spam, people stop answering. The phone has become something to ignore rather than pick up.

People are missing calls that matter. Doctors, schools, delivery drivers, banks – all fighting for attention on a phone that has been trained by experience to be ignored. For individuals, that means missed appointments and delayed information. For businesses, it means calls that go unanswered, drop in revenue, and customer relationships that quietly disappear.

As Telecom and carrier-linked calls become the dominant spam categories, it becomes increasingly difficult for users to distinguish between legitimate business outreach and unwanted noise.

## Looking Ahead to 2026

The data describes where spam and fraud calls are today. What comes next is already visible.

AI-generated voice calls are becoming harder to distinguish from real ones. Scam scripts are adapting faster than ever. The patterns observed in 2025 point to two clear shifts: people are seeing more information about who is calling them, and scam operations are becoming easier to run at scale through automation. For legitimate businesses, the unknown call has become a liability. A real company calling a real customer has to work harder than ever to be heard.

With 500 million users and over a decade of identity and reputation data, Truecaller holds one of the world's most comprehensive trust graphs – built from billions of real interactions across calls, messages, and community signals. In 2026, the focus is on using that base to reduce risk before users are forced to decide – by strengthening detection, context, and collective signals across calls and messages. That means expanding protection across four areas:

### **Reducing exposure at the household level.**

Spam and fraud rarely affect just one person. Family Protection is designed to extend safeguards across connected family members, particularly older users and first-time smartphone adopters, where the risk of harm is higher.

### **Real-time risk detection during calls.**

As scam scripts become more fluent and convincing, call-time warnings matter more than static labels. AI Call Scanner is being strengthened to surface risks during live interactions, helping users recognise high-risk situations as they unfold.

### **Faster identification of emerging fraud patterns.**

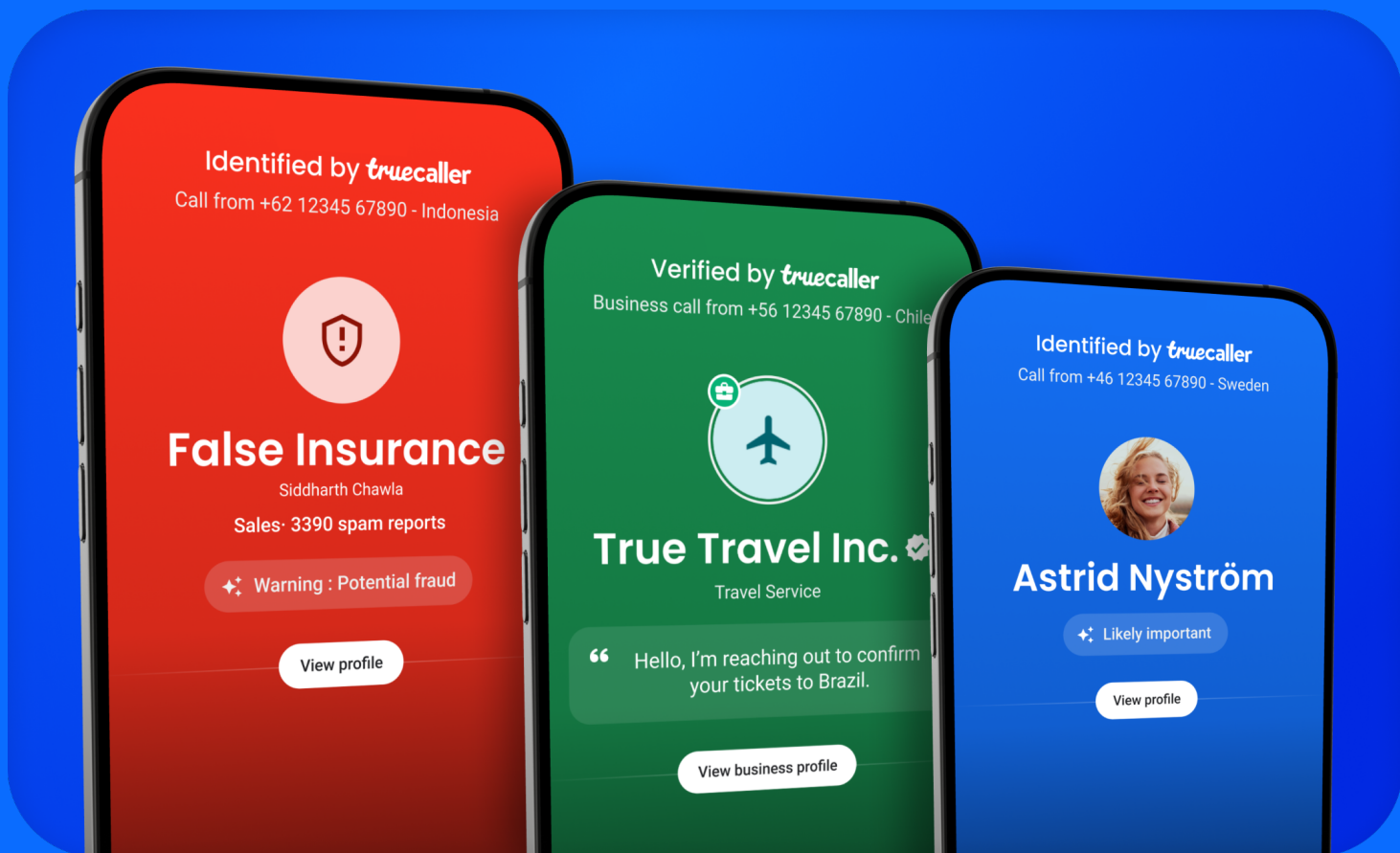
Scam campaigns adapt quickly across numbers, scripts, and channels. New detection systems focus on behavioural patterns over time, allowing fraud activity to be identified earlier – even when individual numbers change rapidly.

### **Collective awareness through community signals.**

Scam activity often appears first as near-misses. Scamfeed allows users to share and surface suspicious experiences in real time, helping others recognise threats sooner. This collective awareness adds a layer of context that automated detection alone cannot provide.

The problem is getting harder. The tools to fight it are getting better.

# The Truecaller Way: Practical Steps to Reduce Risk



- » Be cautious with calls or messages that create urgency, especially those related to personal detail updates, account suspension, or law enforcement. Verify before responding.
- » Avoid responding to calls or messages that are flagged as spam or suspicious by community reporting or automated detection systems.
- » Do not click on unknown or unexpected links received via SMS or messaging apps, particularly when they involve financial actions. When in doubt, contact the organisation directly using official contact details.
- » Never share sensitive information such as OTPs, PINs, passwords, or bank information over a call or message. Banks, financial institutions, and government agencies do not request this information in this way.
- » Be cautious about requests to install apps or share screen access, especially if prompted during a call or via a message. Only install apps from official app stores.
- » Treat offers, refunds, or requests that arrive unexpectedly — especially from personal numbers claiming to represent organisations — with scepticism.

# Notes & Methodology

The data in this report was aggregated anonymously from metadata and spam classification signals for all Truecaller users globally from January 1st, 2025, to December 31, 2025.

The insights presented reflect patterns observed within this dataset and are intended to provide visibility into trends in spam and fraud activity at a global and national level. They should not be interpreted as precise measurements of all spam or fraud activity across the world, nor as assessments of individual users, organisations, or regions.

References to emerging scam patterns are indicative and forward-looking, based on observed behaviour and known adaptation trends. They do not constitute predictions or guarantees of future activity.

## About Truecaller

Truecaller is an essential part of everyday communication for over 500 million active users, with more than a billion downloads since its launch and 68 billion spam and fraud calls identified in 2025 alone. The company has been headquartered in Stockholm since 2009 and has been publicly listed on Nasdaq Stockholm since October 2021. For more information, please visit [www.truecaller.com](http://www.truecaller.com).

*truecaller* insights