identidad

Real data in Action: A Case Study on Telecom Fraud Prevention.

2025

identidadtech.com

Real data in Action:

A Case Study on Telecom Fraud Prevention.

Fraud remains a global challenge in the telecom industry, with evolving tactics threatening network integrity and profitability. Like many operators, one of our partners faced the usual difficulties of maintaining a secure, high-quality network. As part of a managed services agreement, Identidad integrated its proprietary Anti-Fraud Suite—an added benefit that provided real-time visibility into fraudulent patterns and enabled swift action against emerging threats.

The insights presented in this case study are based on 2024 performance results, demonstrating how an effective fraud prevention strategy enhances security and helps create a healthier traffic flow. At Identidad, we recognize that tackling fraud is not just about blocking threats—it's about enabling better business outcomes. Through collaboration, data-driven decision-making, and continuous communication, operators can refine their fraud prevention strategies while ensuring higher-quality traffic and optimizing revenue potential.

Beyond individual implementations, fraud intelligence gathered through our Anti-Fraud Suite is shared within industry forums and associations, contributing to a broader effort to combat fraud globally. By exchanging insights and best practices with industry leaders, we help strengthen the global telecom ecosystem, ensuring that fraud prevention strategies evolve in step with emerging threats. This collaborative approach benefits the industry by fostering more secure and efficient networks worldwide.

The Financial Impact of Telecom Fraud and the Need for Prevention

Telecom fraud continues to be a **major global challenge**, impacting businesses, operators, and consumers. As fraud tactics evolve, they pose significant risks to **network integrity, financial stability, and service reliability**. Fraudsters are shifting to more **complex and deceptive schemes**, making real-time detection and prevention essential for mitigating losses and maintaining a secure telecom ecosystem.

Key Industry Insights: The Cost of Fraud and Revenue Protection

The following statistics highlight the scale of telecom fraud and its financial impact:

- According to the Global Telecom Outlook 2024–2028 by PwC (PricewaterhouseCoopers), global telecom service revenue (fixed and mobile) reached **US$1.14 trillion** in 2023.
- Revenue is projected to grow at a **2.9% compound annual growth rate (CAGR)**, reaching approximately **US$1.3 trillion by 2028**.
- **US$28.5 billion** was lost to telecom fraud in 2023, representing **2.5% of global telecom revenue** – cfca.org, pwc.com.
- If no additional countermeasures are implemented, **fraud losses could increase to US$32.5 billion annually by 2028** – pwc.com.
- 12% increase in 2023 in fraud activity compared to previous years – cfca.org

Leveraging Fraud Prevention to Protect and Grow Revenue

With the **telecom industry's total revenue projected to reach US$1.3 trillion by 2028** (pwc.com), preventing fraud is more than just a security measure—it's a **business strategy for protecting and maximizing revenue**. As competition and infrastructure costs rise, operators must **optimize existing revenue streams** and prevent unnecessary financial losses.

By prioritizing **real-time fraud detection and adaptive security solutions**, telecom companies can:

- **Reduce financial losses** and reinvest savings into innovation and network expansion.
- **Enhance service reliability**, leading to improved customer trust and retention.
- **Ensure compliance with industry regulations**, avoiding legal and reputational risks.

Fraud will remain an evolving threat, but with proactive, data-driven prevention strategies, telecom operators can safeguard revenue, strengthen market position, and create sustainable growth in a rapidly changing industry.

Our Approach to Fraud Prevention

Proprietary Fraud Prevention Tools

Identidad has developed a suite of proprietary fraud prevention tools that provide real-time detection, immediate blocking, and continuous analysis of fraudulent activity. These tools work together to **safeguard telecom networks, enhance traffic quality, and prevent financial losses**.

International Anti-Fraud System

The International Anti-Fraud System continuously monitors global traffic patterns, analyzing key parameters such as B-Number, A-Number, ASR (Answer-Seizure Ratio), and ACD (Average Call Duration) to identify anomalies. This system ensures immediate action against fraudulent sources and alerts the fraud prevention unit for further investigation.

Fraud Prevention Process: How it works

1. Detection – The system continuously scans traffic using advanced algorithms to identify Wangiri fraud, International Revenue Share Fraud (IRSF), call spoofing, and other fraudulent activities. An alarm is triggered when suspicious patterns are detected, signaling potential fraud.
2. Blocking – Once the alarm is activated, the system automatically blocks suspicious traffic in real time, preventing robocalls, PBX hacking, scam calls, and other threats before they cause financial harm.
3. Analysis – The fraud prevention team investigates triggered alarms, examining fraud patterns to determine the legitimacy of the threat. Findings are shared with partners to verify and refine detection methods.
4. Categorization & Collaboration – Confirmed fraud cases are categorized and stored to prevent future attacks. Identidad shares insights within industry forums and with partners, contributing to a stronger global fraud prevention network. Additionally, partners can report emerging fraud trends, ensuring the system continuously adapts to new threats.

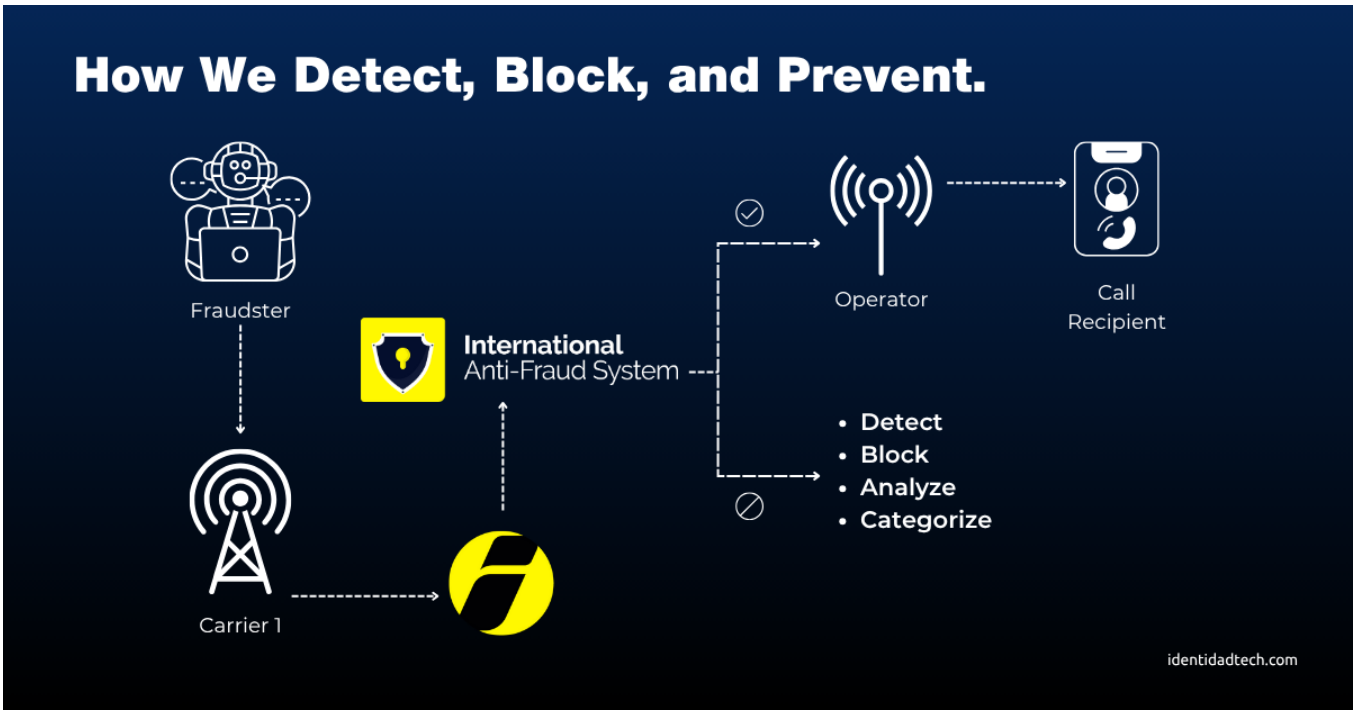

Image 1: How Identidad;s International Anti-Fraud System works.

Falcon Eye 360: Intelligent Fraud Detection & Network Security.

Falcon Eye 360 is a **penetration testing tool** that **performs** automated and manual test calls to **identify bypass voice traffic patterns and points of entry**. It is actively used across **14 markets for voice fraud prevention**.

Results: Measuring the Impact of Fraud Prevention.

Enhanced Call Quality & Network Integrity

The deployment of Identidads' International Anti-Fraud System has led to significant improvements in network performance, directly affecting key telecom metrics:

- **+71% increase in Average Call Duration (ACD)** – This increase is a direct result of **blocking fraudulent robocalls**, which are typically very short in duration. By preventing these calls, the system **allows legitimate calls to be completed properly**, improving overall call quality.
- **+29% increase in Answer-Seizure Ratio (ASR)** – Fraudulent traffic often distorts ASR by introducing unanswered or manipulated calls. By filtering out fraudulent patterns, the system ensures that **more real calls connect successfully**.
- **+24% increase in Answer-Bid Ratio (ABR)** – A higher ABR indicates that more legitimate calls **reach their intended recipients**, reflecting improved traffic quality and revenue protection.

- **Blocked traffic decreased by 14% in 2024 compared to 2023** – This reduction highlights the system's ability to **differentiate between fraudulent and legitimate traffic**, ensuring that **only necessary blocks are enforced**, optimizing network efficiency.

Fraud Prevention Process: How it works

These improvements translate into better traffic quality, reduced revenue leakage, and increased operational efficiency. By eliminating fraudulent robocalls, improving call completion rates, and ensuring legitimate traffic flows uninterrupted, telecom operators using Identidad' Anti-Fraud System can recover a significant portion of lost revenue.

Beyond revenue protection, higher-quality traffic also reduces the number of disputes, minimizing the time and resources spent on dispute resolution. With fewer billing conflicts and stronger communication between partners, operators can streamline operations, improve trust, and focus on growth and innovation rather than fraud mitigation.

Fraud prevention is not just about blocking threats—it is a proactive strategy to enhance call quality, protect network integrity, optimize operations, and maximize revenue potential.

Fraudulent Activity Breakdown

Identidad's tools successfully identified and mitigated various types of fraud. The chart below shows the percentage distribution of total blocked traffic – excluding scam calls, categorized by fraud type:

Type of fraud	% in 2024
IRSF	46%
Call Hijacking	28%
PBX Hacking	20%
Wangiri	6%

Table 1: Percentage distribution of total traffic blocked for fraudulent activity-excluding scams.

Scam Call Reduction

This cutting-edge fraud prevention solution is one of our latest developments, demonstrating our commitment to staying at the forefront of fraud prevention. **In the first two months of 2025, scam call patterns were already reduced by 95%, highlighting the effectiveness of our continuous innovations in securing telecom networks**.

At Identidad, we constantly evolve and develop new technologies to enhance security, protect revenues, and improve overall network integrity. This achievement exemplifies our ongoing efforts to lead the industry in fraud prevention.

Bypass Fraud Prevention

Results from the 2024 implementation of Falcon Eye 360 demonstrated a significant impact in the fight against telecom fraud:

- **512 bypass fraud routes were identified and blocked**, preventing fraudulent call rerouting.
- These detections ensured accurate billing by stopping international calls from being misclassified as local, safeguarding partner revenue.
- The implementation also strengthened network integrity by eliminating unauthorized call manipulation and ensuring that legitimate traffic flowed correctly.

These results highlight the effectiveness of Falcon Eye 360 as a proactive fraud prevention tool, reinforcing its value in protecting revenue and network integrity across global operations.

Financial Impact of Fraudulent IVR Blocking & CLI Integrity Monitoring

The implementation of Identidad's fraud prevention tools has led to cost savings and increased revenue protection by reducing fraudulent traffic and improving network integrity.

Fraudulent IVR Blocking

Through proactive monitoring and real-time intervention, it is possible to prevent significant revenue losses and protect networks from malicious traffic. The following key results from 2024 demonstrate the tangible impact of these efforts:

- **Over $165,000 saved in 2024** by preventing fraudulent call activity.
- **The market analysis of more than 37,000 completed calls** identified that **30% were linked to fraudulent IVR schemes**, highlighting the **effectiveness of proactive fraud detection**.
- **Fraudulent traffic was successfully blocked in 72 countries**, reducing **network congestion and revenue leakage**.
- The **combination of real-time fraud prevention and market analysis** strengthens fraud mitigation efforts, ensuring **immediate protection and long- term strategy development**.

Caller ID (CLI) Integrity Monitoring

By detecting anomalies in call traffic and Caller Line Identification, operators and anti- fraud solution providers like Identidad- can maintain billing accuracy, ensure compliance, and strengthen network integrity. The following results showcase the effectiveness of these joint efforts and the importance of continuous monitoring:

- **Over 263,000 calls were analyzed** to detect **CLI (Caller Line Identification) manipulation**, ensuring **billing accuracy and network integrity**.
- **5% of calls showed CLI discrepancies**, where the displayed number differed from the original A-number, potentially affecting pricing and revenue.
- **Market analysis provides a strategic advantage**, allowing operators to **anticipate fraud risks, adjust pricing strategies, and optimize traffic management**.
- **In certain countries, call pricing is influenced by origin-based rating (OBR)**— altering the origin can change call costs, leading to incorrect charges and potential revenue loss.
- **Continuous monitoring of route quality and traffic integrity** ensures compliance and **protects operators from financial risks associated with fraudulent call rerouting**.

Conclusion

This case study demonstrates that fraud prevention is not just a security measure—it is a critical strategy for revenue protection and growth. As fraud tactics evolve, telecom operators face increasing risks of revenue leakage, incorrect billing, and financial losses. Without proactive fraud management, these challenges directly impact profitability and operational efficiency.

By implementing Identidad's Anti-Fraud Suite, operators have successfully prevented revenue loss, ensured proper billing, and improved call quality, leading to higher legitimate traffic and fewer disputes. Fraud schemes such as IRSF, call hijacking, and CLI manipulation can distort call charges and reduce revenues. Still, real-time detection and automated blocking have effectively stopped these threats before they cause financial damage.

Additionally, accurate call routing and origin-based rating (OBR) compliance ensures operators receive the correct revenue for international traffic, avoiding losses caused by fraudulent call rerouting. The reduction of fraudulent robocalls and bypass fraud means higher monetization of real traffic, strengthening long-term revenue streams.

Beyond fraud mitigation, the collaborative sharing of fraud intelligence enhances the industry's ability to adapt, optimize pricing strategies, and protect revenues on a larger scale. By leveraging continuous market analysis and anti-fraud technologies, operators can maximize profitability, reduce financial risks, and build a more sustainable business model.

At Identidad, we remain committed to delivering innovative fraud prevention solutions that secure networks and directly impact the bottom line—protecting revenue, increasing operational efficiency, and driving long-term financial success.

To learn more, contact:

Santiago Sánchez VP of
Operations
ssanchez@identidadtech.com