Peruvian call center operator sentenced to 8 years over US government-impersonation fraud



A Peruvian call center operator received an eight-year sentence for a scheme that defrauded over 30,000 Spanish-speaking US residents of $15 million by impersonating officials and lawyers. The case shows how fear-based impersonation fraud works.

- Carla Magaly Alcedo Mendoza, 45, of Lima pleaded guilty to conspiracy to commit mail and wire fraud.
- She ran Peruvian call centers tied to fraud and extortion schemes between January 2013 and December 2018.
- Callers offered free services or products, then posed as US officials and lawyers and claimed payment was contractually owed.
- Victims were threatened with court action, arrest and immigration consequences; the Department

> of Justice put losses at $15 million across more than 30,000 people.
>
> - The FTC reported $3.5 billion in impersonation-scam losses for 2025, about $920 million of it to government impersonators.

A court in the United States has sentenced Carla Magaly Alcedo Mendoza, a 45-year-old from Lima, Peru, to eight years in prison. She pleaded guilty to conspiracy to commit mail and wire fraud after her arrest in March 2023 and extradition in April 2025.

What the scheme involved

According to court documents, she managed and operated call centers in Peru between January 2013 and December 2018. Callers contacted Spanish-speaking people in the US, telling them they qualified for free services or products. They then posed as government officials and lawyers and said the victims were contractually bound to pay large sums.

Victims were also threatened with court action, arrest and immigration consequences. The Department of Justice says the scheme defrauded more than 30,000 people of $15 million. She was the tenth defendant extradited from Peru and sentenced in this case, and other call center and distribution center operators have also been convicted.

Wider context

The source links the case to a June 2026 FTC warning that Americans lost $3.5 billion to impersonation scams in 2025, with reported losses nearly tripling since 2020 and about $920 million taken by government impersonators.

Relevance for Saudi institutions

The case is American, and the source does not mention Saudi Arabia. The tactics it describes are familiar, though: unsolicited calls, a false claim of official authority, and pressure built on fear of legal consequences. Institutions can use it as a reference point when reviewing how staff and customers are warned about this kind of social engineering.

What to do now

1. Include government and legal-authority impersonation scenarios in staff awareness training, especially for call center and customer service teams.
2. Remind customers through official channels that the institution and authorities do not demand payment or threaten arrest by unsolicited phone call.
3. Give front-line staff a clear process to escalate and record suspicious customer reports of payment demands.

4. Review fraud monitoring for unusual customer-initiated payments that follow a reported phone contact.
5. Check that fraud and social-engineering controls align with your applicable NCA and SAMA requirements.