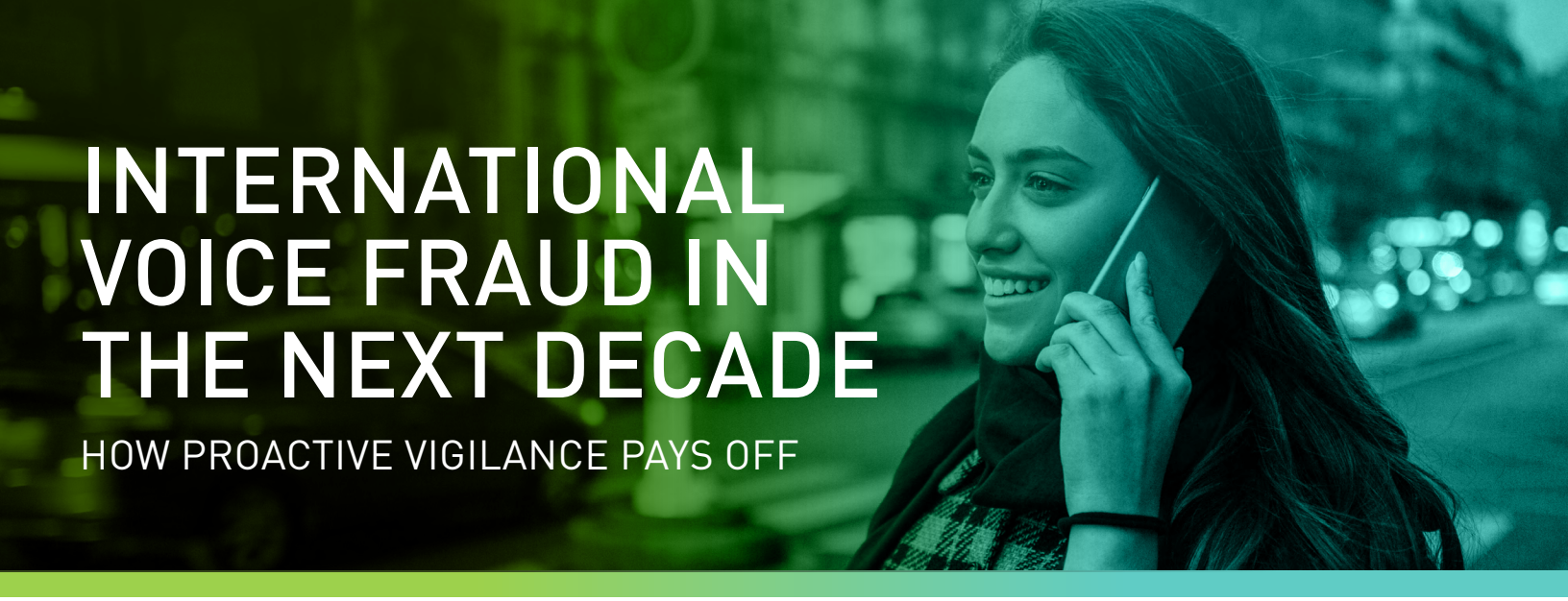

INTERNATIONAL VOICE FRAUD IN THE NEXT DECADE

HOW PROACTIVE VIGILANCE PAYS OFF

Telecommunications providers are combatting fraud — and winning — by adopting a more sophisticated, proactive approach.

High-tech crimes like telecom fraud can be profitable, global operations. In fact, annual losses due to international voice fraud attacks amount to billions of dollars every year. It's a costly challenge, made even more difficult by its constantly evolving nature. Fraud isn't limited to any region, it's both automated and perpetrated by live actors, and it happens to providers of any size. It hurts the bottom line of business, certainly; but it also hurts individual consumers whose own communications, information, and funds can be compromised.

As a large-scale provider, we are always looking for ways to protect against voice fraud. To defend against attacks, we implement a specialized solution of tactics and techniques that are now being made available to our own clients in order to build a more unified front line against these increasing threats. Voice fraud is a constantly evolving criminal activity. To protect against it requires an approach that can evolve to meet an ever-changing threat.

There are a multitude of fraud types that span voice, SMS, wireless roaming, and more. Though not an exhaustive list, below are some specific fraud cases — and how our Fraud Mitigation service protected customers and revenue by fighting back.

SAVE MILLIONS WITH PROACTIVE PROTECTION AGAINST:

- NUMBER SPOOFING
- IRSF
- PBX/IPBXHACKING
- CALL HIJACKING
- AND MORE

COMCAST TECHNOLOGY SOLUTIONS

#1: TELEPHONE NUMBER SPOOFING/PBX HACK

Issue: Account identification "spoofing," in simple terms, is a technique that fraudsters use to display a phone number that's different from the one that actually placed the call. In this case, a block of 34 Automatic Number Identifications (ANIs) originated in the U.S. to terminate traffic in Slovenia. Our Fraud Mitigation solution identified the issue quickly; however, the fraudsters tried to escape detection by only accepting calls from a certain range of U.S. calling numbers — making a positive fraud ID challenging.

Result: The team proactively blocked the 34 U.S.-originated numbers temporarily, as well as traffic to the terminating number in Slovenia. Out of a potential fraud exposure of almost $13,000, the team's work prevented over $11,500 in theft.

#2: INTERNATIONAL REVENUE SHARE FRAUD (IRSF)

Issue: IRSF is a popular method of generating voice fraud revenue. IRSF utilizes the practice of "pumping" traffic — generating calls to premium rate destinations. Fraudsters understand that a direct correlation exists between call volumes to high risk destinations and fraudulent voice revenue. During these high call volume events, fraudsters will utilize specific ANIs to generate the fraudulent call attempts to the premium rate numbers. In this case, a malicious ANI located within the U.S. generated an inordinate amount of calls to numbers located in both Jamaica and the United Kingdom. Fraud Mitigation picked up on this quickly and issued temporary blocks for the associated ANIs from the U.S. as well as dialed numbers from the U.K. and Jamaica.

Results: Multiple, unsuccessful call attempts were made by fraudsters after the blocks were implemented. The fraudsters realized that the fraud attack was identified and shut down by the carrier. They ultimately gave up. The Fraud Mitigation tactics proved their worth: Out of a total fraud exposure of almost $8,000, over $7,800 was thwarted.

#3: PBX HACK

Issue: Private Branch Exchange (PBX) fraud occurs when a criminal entity exploits a weakness in a company's firewall to gain access into a private phone system. Before they're detected, they generate traffic to a premium-rate number with a high per-minute charge on top of the call connection. In this case, Fraud Mitigation detected a high rate of call attempts (in excess of 400 per minute) to connect to 11 dialed numbers in Madagascar from a single ANI located in the U.S. Fortunately, Fraud Mitigation had already identified the terminating numbers in Madagascar and had them listed in their database; the calls were automatically blocked, resulting in zero fraud exposure.

Results: Although the attack was sophisticated and well-planned, the quick turnaround by Fraud Mitigation detected the activity and protected against approximately 30,000 attempts, and almost $7,000 in fraudulent activity, generated in just over an hour.

#4: CALL HIJACKING TO EXPLOIT PREMIUM RATE DESTINATION

Issue: Call hijacking is essentially self-explanatory: A nefarious actor gains unauthorized access to a phone number and uses it in any way they see fit — for robocalls, to intercept codes used for two-factor authentication, and to steal personal information. In this case, five ANIs located within the U.S. were engaged in a unique call pattern to suspicious numbers terminating in Liberia. There would be two calls made simultaneously, followed by a 10-15-minute delay, and then the process would repeat. Fraud Mitigation recognized the suspicious behavior and blocked the U.S. and Liberia numbers involved.

Results: After implementing the blocks, an additional 25 attempts were made by the fraudsters before this fraud event was abandoned. The rapid response of the Fraud Mitigation service shut down the attempt: With over $6,000 in potential fraud exposure, over $5,500 in theft was averted.

REAL-TIME PROTECTION AGAINST VOICE FRAUD

These real-world examples clearly show thousands of dollars in fraudulent activity can happen in mere minutes. It's easy to see how that adds up across accounts, and over days, weeks, and months. Comcast Technology Solutions is proud to now offer this proactive Fraud Mitigation service for operators who want a cost-effective way to minimize the impacts of IRSF and other voice fraud attacks. Our Fraud Mitigation service protects against:

- IRSF
- Wangiri — missed calls and spam SMS responses
- Artificial Inflation Of Traffic (AIT)
- Arbitrage exploitation
- Premium rate and high-priced destination exploitation
- PBX/iPBX hacking for the purpose of mentioned fraud types
- Malware originated calls for the purpose of mentioned fraud types
- Inbound roaming fraud for the purpose of mentioned fraud types

Fraud Mitigation is just one component of Comcast Technology Solutions' Communications Suite — wholesale data, voice, and long-distance services that deliver cost-effective quality and trusted performance. Our team of industry professionals work directly with you to create a tailored solution to meet your unique needs. Let us show you how we can help you exceed customer expectations while protecting and improving your bottom line.

FIND OUT MORE

800-824-1776 | ComcastTechnologySolutions@comcast.com
ComcastTechnologySolutions.com

COMCAST TECHNOLOGY SOLUTIONS