Stolen Bank Identity, Millions of Fraud Calls

How a top five global banking institution shut down a mass spoofing campaign and restored trust in its outbound calls

CUSTOMER STORY #1034

SecureLogix®

Call Spoofing Protection & Outbound Call Trust

Introduction

Summary

For a global financial institution managing tens of millions of customer interactions every month, the integrity of every phone call is not simply an operational concern — it is a matter of direct financial risk and customer trust. When fraudsters began systematically spoofing the bank's contact center and enterprise phone numbers to impersonate the institution and defraud its customers, the consequences extended far beyond nuisance. Customers lost money. Account takeovers mounted. And the bank's most recognizable customer-facing phone numbers — the numbers printed on the backs of credit cards and posted on every branch window — became tools of fraud in the hands of bad actors.

This is the story of how SecureLogix® and its industry-leading TrueCall™ Spoofing Protection Service delivered a decisive, data-backed solution to that threat — and what the results reveal about the scale and nature of phone number spoofing attacks targeting major financial institutions today.

Top 5
global banking and financial institution, serving millions of customers worldwide

13 Million
estimated outbound calls per month

900,000+
phone numbers under management by SecureLogix® Reputation Defense™ Service

30%
of outbound calls from the bank's key numbers were identified as spoofed prior to deployment

3.2 Million
spoofed call attempts blocked during initial deployment and protection period (Aug – Oct)

8.3 Million
legitimate calls authenticated from August through October for the initial 55-number deployment

5 Million
calls blocked in a single attack event

Enterprise Client Overview

About the Business

SecureLogix has served this top five global banking and financial institution as a trusted voice security partner since 2013, making this one of the deepest and longest-standing enterprise voice security engagements in the industry. The bank is among the largest financial institutions on the planet, employing hundreds of thousands of people worldwide and serving millions of customers across its retail, commercial, wealth management, and investment banking lines of business. Its U.S. operations alone represent a sprawling customer communications footprint — one that generates and receives call volumes few enterprises in any sector can match.

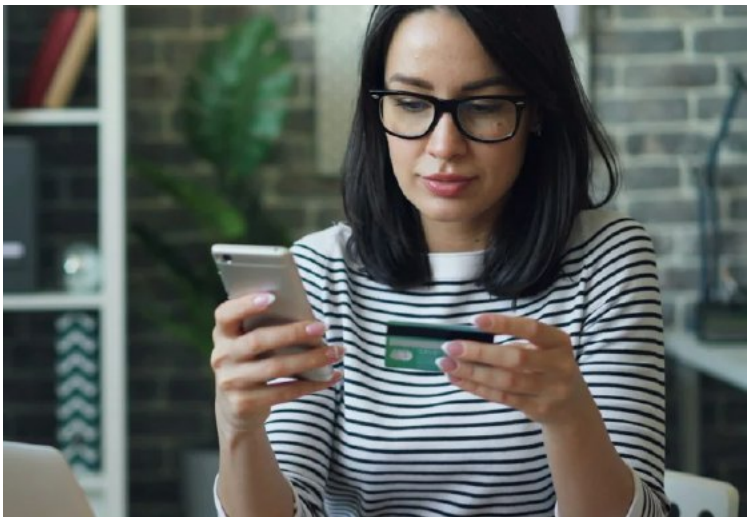
The bank's telecommunications environment operates along two primary axes: contact center and enterprise voice. SecureLogix's Call Defense™ System has been protecting the contact center environment since 2013, with enterprise voice protection added in 2023. SecureLogix servers are connected across a large data center infrastructure – providing unified call security coverage across all inbound traffic flows into both the contact center and enterprise environments.

The contact center handles eight to nine million inbound calls every week — translating to roughly 30–40 million calls per month. Enterprise voice, covering all administrative offices, regional headquarters, and branch banking locations, adds further substantial volume, estimated at approximately 70% of that contact center scale. The bank's outbound calling footprint is equally large, and the bank places approximately 13 million outbound calls per month to wireless subscribers across the major U.S. carriers.

A Remarkable Portfolio

The breadth of the bank's phone number portfolio is itself remarkable. Rather than retiring phone numbers as campaigns end or business units evolve — a policy risk given that any released number could appear in legacy materials and be reassigned to another party — the bank retains numbers indefinitely. As a result, its registered phone number portfolio under SecureLogix Reputation Defense management exceeds 900,000 numbers. Roughly 20% of those numbers generate 80% of the total outbound call volume, but the full portfolio represents both the breadth of the institution's customer-facing voice identity and the corresponding magnitude of its spoofing exposure.

The bank's wealth management division introduces additional complexity. It's traffic is tracked and reported separately each week, given its distinct calling patterns and customer base, including financial advisers operating out of branch locations. This layered telecom environment — millions of calls per week, across two major voice domains, with a phone number portfolio approaching seven figures — sets the stage for understanding both why this institution was a prime spoofing target and why getting protection right was a matter of urgent priority.



The Problem

Fraudsters Were Posing as Bank Agents

Phone number spoofing is not a new threat, but when wielded against a globally recognized consumer bank, its consequences are acutely damaging. Fraudsters recognized that the bank's most prominent customer-facing numbers — the toll-free lines printed on credit cards and displayed prominently in advertising — carry an inherent authority that almost any consumer will recognize and trust. By spoofing those numbers and delivering fraudulent calls into the carrier networks, bad actors could place millions of calls per month with calling number displaying the bank's own identity.

The fraud playbook was straightforward and alarmingly effective: contact consumers displaying the bank's known number, open with a text message asking if the consumer had authorized a suspicious charge, and then — when the consumer replied 'no' — follow immediately with a call spoofed from the bank's number. With the number confirmed on screen and matching the bank's published contact information, consumers had little reason to question the caller's legitimacy. From there, fraudsters would assert that the consumer's account had been compromised and that funds needed to be moved immediately to a secure account to prevent loss. Account takeover attempts and fraudulent fund transfers followed, with documented financial losses attributable across the bank's telephony fraud channels reported to reach as much as $150 million per year in aggregate.

The bank became aware of the problem through a combination of direct customer reports and carrier-level data analysis. Customers would call the bank's actual contact center to report that 'you just called me,' only to discover that no such call had been placed.

Fraud Complaints Began to Rise

Post-incident reports began accumulating from customers who had suffered actual financial loss after engaging with spoofed calls they believed to be legitimate. The bank's fraud team moved to quantify the problem systematically.

Working with AT&T and Verizon, the bank's security leadership generated carrier-level reports showing all calls delivered to those carriers' wireless subscribers from the bank's registered phone numbers — along with STIR/SHAKEN attestation data for each call. The findings were striking. The bank makes outbound calls exclusively over AT&T and Verizon SIP trunks. Any call from a carrier other than AT&T or Verizon was, by definition, not a legitimate call from the bank. Even more concerning is that some of these calls from other carriers included an A-level or B-level STIR/SHAKEN attestation. The carrier reports documented that approximately 30% of calls reaching AT&T and Verizon wireless subscribers from the bank's numbers were being originated from other carriers — flagging them as spoofed.

The fraud picture was complicated further by the specific mechanics of STIR/SHAKEN in a multi-carrier environment. While STIR/SHAKEN theoretically provides authentication, fraudulent carriers were obtaining signing certificates from authorized certificate authorities and applying A-level and B-level attestations to some of the spoofed calls. The bank now had documented evidence of the problem's scale. The question was what to do about it.

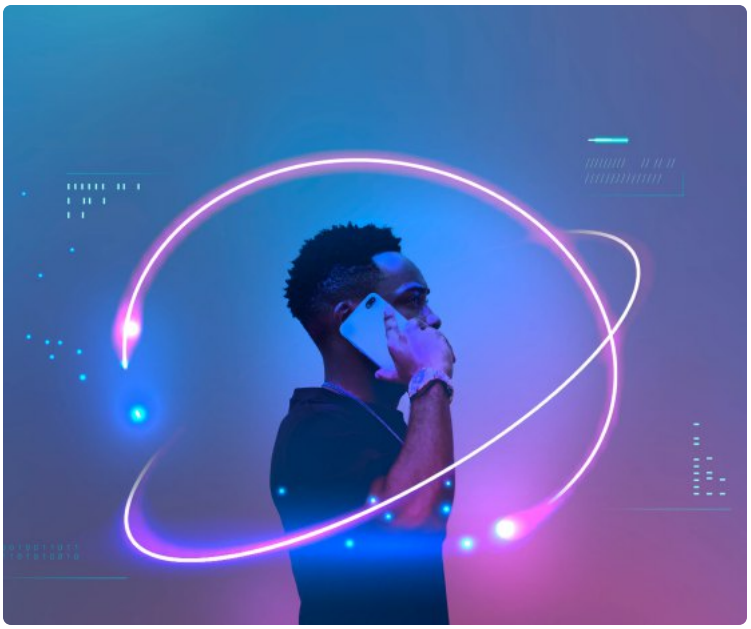
The Solution

TrueCall™ Spoofing Protection

SecureLogix deployed its TrueCall™ Outbound Call Spoofing Protection Service in partnership with the bank's security and telecom teams, going live on August 20th of the deployment year. The deployment began with protecting the bank's 55 highest-priority outbound phone numbers — its most prominent and heavily spoofed toll-free contact center numbers — against calls delivered to Verizon Wireless and T-Mobile subscribers. Coverage was extended to AT&T Wireless on October 6, completing three-carrier protection across all major U.S. wireless networks. Twenty-four additional toll-free numbers were added in the weeks following initial deployment, bringing the protected set to 75 numbers. Additional phased rollouts are planned to systematically expand coverage to numbers responsible for virtually all of the bank's outbound toll-free calling volume, before extending protection to the bank's 300,000-plus active Direct Inward Dial (DID) numbers.

The TrueCall Service operates by integrating directly with the major wireless carriers through their call analytics engines to authenticate outbound calls from the bank in real time. When a call leaves the bank over an AT&T or Verizon SIP trunk, the SecureLogix platform signals the appropriate analytics engine that the call is legitimate. Any call using the bank's registered numbers that does not carry this authentication signal is identified as spoofed and blocked at the carrier network level, before it ever reaches the consumer's device.

Critically, SecureLogix's unique 'line-of-sight' architecture ensures that authentication signals are generated and delivered to analytics engines before calls complete transmission — eliminating the race condition that can cause legitimate calls to be inadvertently blocked or mislabeled under less sophisticated implementations. This is achieved through SecureLogix's proprietary capabilities and its multiple interconnection methods with carrier networks, through on-premise equipment, cloud carrier integration, and/or SIP.



TrueCall™

spoofing protection servcie

Carrier-level filtering identifies and blocks spoofed calls using your corporate numbers in near real-time, before they reach customers.

- Prevent spoofing of outbound numbers
- Prevent fraud & spam labels
- Increase answer rate
- Industry's strongest spoofing protection

The Solution

continued

Numbers Vetting & Low Friction Deployment

In large deployments like this bank, moving a large quantity of phone numbers into active protection requires SecureLogix to work with each carrier to first verify that the submitting enterprise owns each number — a prerequisite designed to prevent enterprises from inadvertently enrolling numbers they no longer control. For any bank with a large portfolio of phone numbers, manual verification is just not feasible at scale. SecureLogix can uniquely address this with its proprietary Automated Vetting Solution. Manual number vetting is painful enough when performed once, but many carriers require monthly reverification. The SecureLogix automated vetting process innovation — with no parallel in any competing solution — enables financial institutions to scale their protection programs across their full number portfolios without the bottleneck of manual verification at each renewal cycle. The deployment process itself at the bank was notable for its low friction. The SecureLogix team handled all carrier coordination, onboarding, and monthly reporting. The bank's telecom and security teams were engaged to confirm ownership and escalate as needed, but the operational burden on the enterprise was minimal. Within weeks of go-live, the system was processing millions of calls per week and generating the alert and reporting data the bank's security team needed to monitor the program's impact in real time.

Business Results & Impact

Numbers

8.3 million

legitimate calls authenticated

3.2 million +

spoofed calls blocked

~ 5 million

calls blocked in single attack

75 numbers

numbers now protected

Millions of Fraudulent Calls Blocked

From August through mid-November of the deployment year — covering the initial protection set of 55 phone numbers before expanding to 75 — SecureLogix authenticated 8.3 million legitimate outbound calls from the bank's numbers while blocking 3.2 million spoofed call attempts (measured through late October for the initial 55-number set). These figures represent only the calls addressed during the initial deployment window and will grow substantially as the program expands in scope.

The data also revealed several mass-attack events that underscore the severity of the threat the bank was facing. In the week of November 7 alone, SecureLogix blocked nearly 5 million calls in a single coordinated attack — a volume that would have deliveredmillions of fraudulent calls to consumers displaying the bank's caller ID had the protection not been in place. Carriers provide real-time alerts to the SecureLogix team when these attack spikes begin, enabling prompt notification and documentation for the bank's security team.

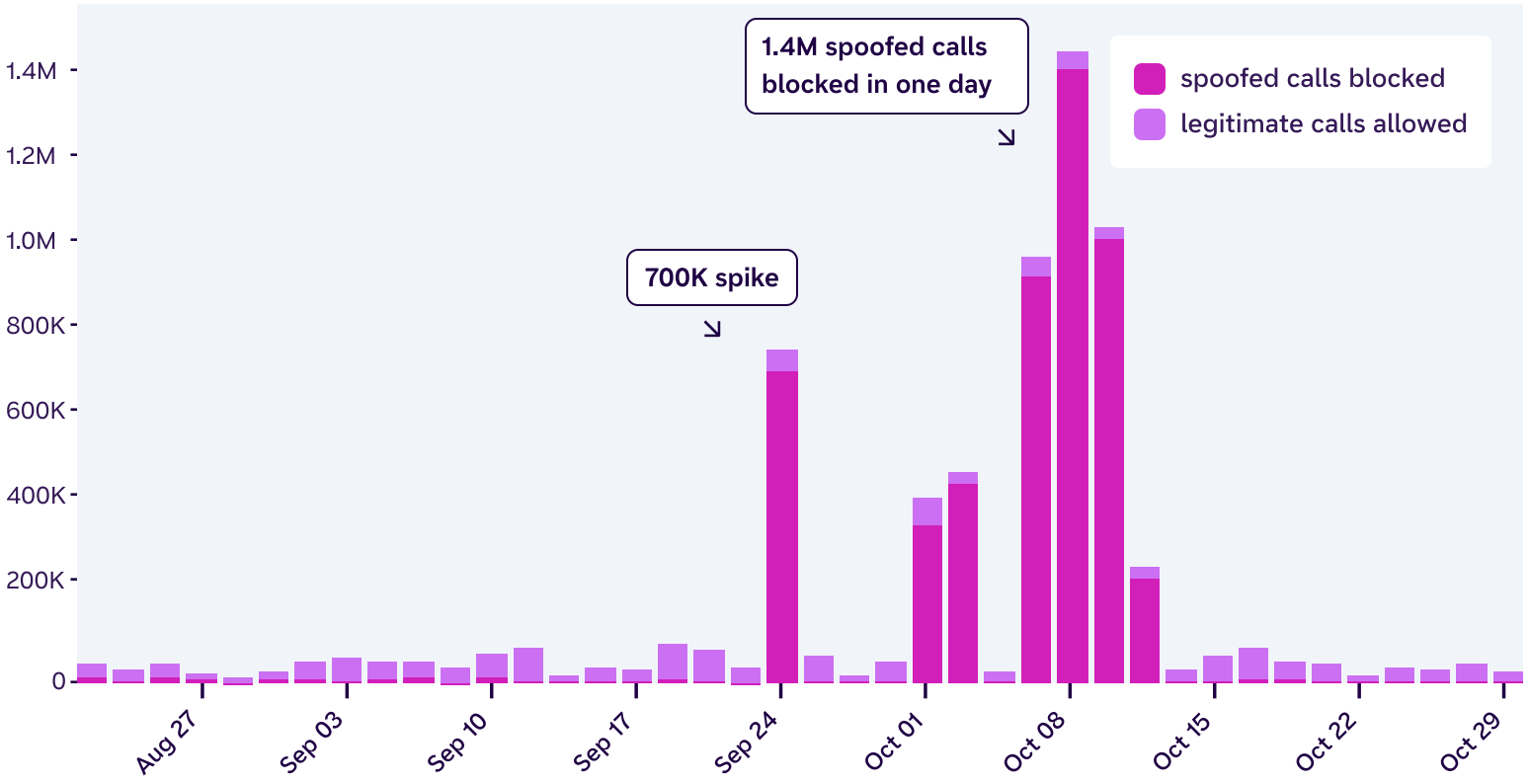
Carrier level reports confirmed that the SecureLogix protection was not only stopping these spoofing attacks, but these reports also revealed a displacement effect: fraudsters who had been targeting the bank began shifting their spoofing activity toward other major financial institutions, notably another large national bank. This outcome — while concerning from an industry perspective — validates the effectiveness of the TrueCall Service in making this bank a materially harder target than its unprotected peers.

Business Results & Impact

continued

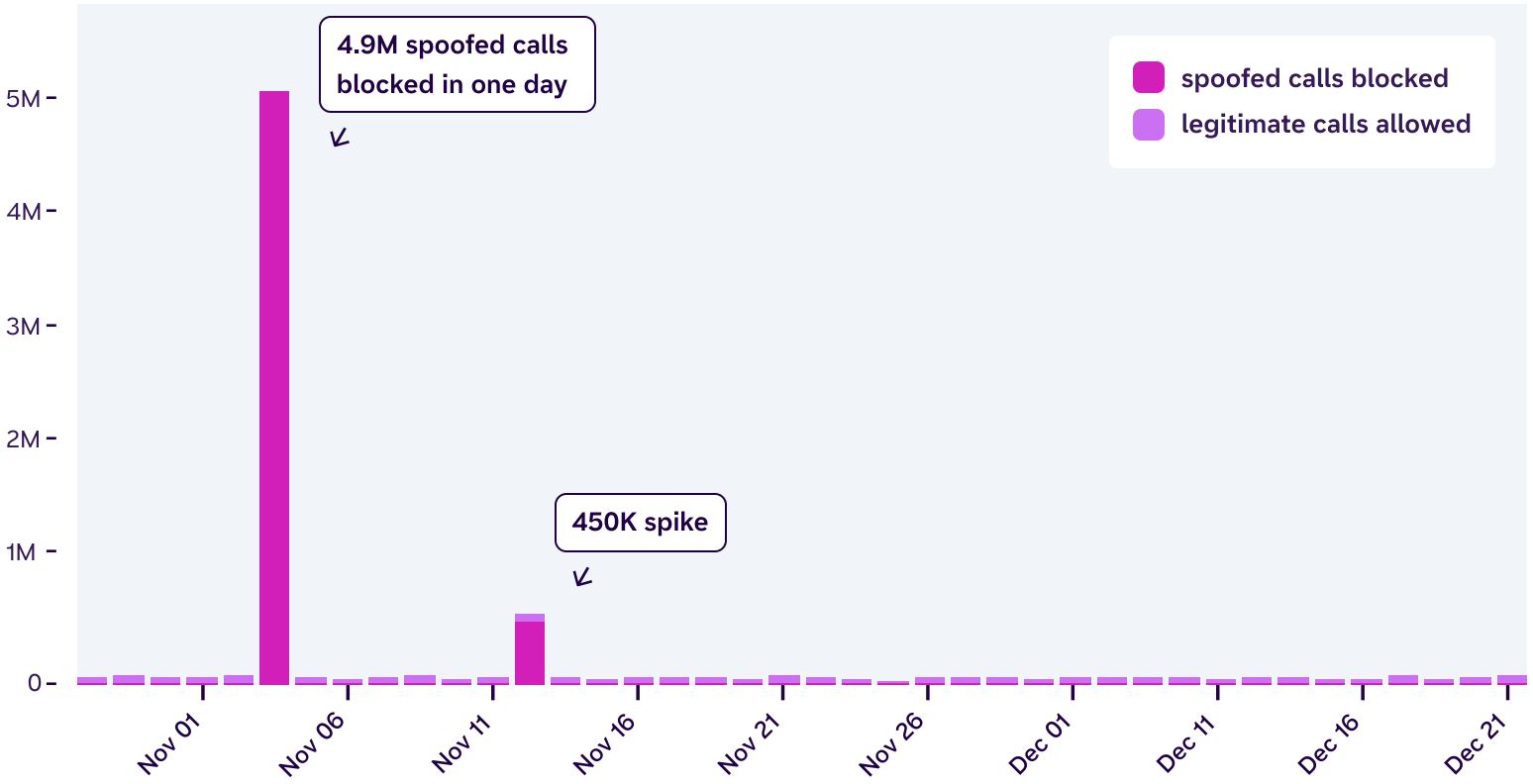
Spoofed Calls Identified & Blocked by Day

Aug 2025 - Oct 2025



Spoofed Calls Identified & Blocked by Day

Nov 2025 - Dec 2025



Business Results & Impact

continued

Expanding Coverage Based on Security Team Intelligence

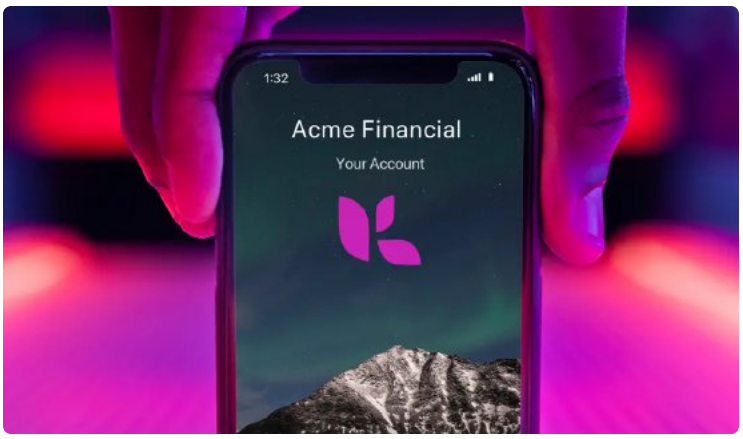
The bank's internal security team conducts ongoing analysis of customer-reported fraud events, tracking phone numbers cited in reports of fraudulent calls received by consumers who subsequently experienced account compromise or loss. This analysis has been instrumental in driving the program's expansion. As the security team identified additional bank numbers appearing in fraud reports from numbers outside the initial protected set, those numbers were added to the TrueCall program. The expansion from 55 to 75 numbers, and the planned additions in subsequent phases, are directly informed by this intelligence loop — creating a data-driven, continuously improving protection perimeter.

The financial losses attributable to phone channel fraud at major institutions are staggering. The bank's total telephony channel fraud losses — spanning inbound and outbound spoofing, social engineering, and related schemes — have been cited at figures approaching $150 million annually. While the TrueCall service addresses specifically the outbound spoofing vector, that vector is a significant contributor to total losses: it is the fraud mechanism that generates the false trust that enables successful account takeover and unauthorized fund transfer attempts. By cutting off fraudsters' ability to use the bank's own numbers as instruments of deception, the TrueCall Spoofing Protection Service directly attacks the trust infrastructure that makes these scams possible.

Protection of Brand, Reputation and Customer Trust

Beyond direct financial impact, the reputational damage to the bank's brand from unchecked number spoofing is difficult to quantify but real. Each consumer who receives a spoofed call bearing the bank's number — and each customer who is defrauded as a result — represents a potential permanent loss of trust in the institution's ability to protect its customers. By removing millions of spoofed calls from circulation, SecureLogix is directly protecting the bank's customer relationships and the integrity of its most fundamental customer touchpoint: the phone call.

The program's success has already reached senior leadership within the bank. Internal reporting on the program's results was included in executive briefings as early as October following deployment 2 months prior — at which point the program had blocked more than 3 million spoofed calls — and the data has been used in executive presentations highlighting the program's progress and value. This level of executive visibility reflects the program's direct connection to the bank's core fraud risk and customer trust priorities.



Summary & Key Takeaways

Summary

The deployment of SecureLogix TrueCall™ Spoofing Protection at this top five global banking institution demonstrates what is possible when carrier-level call authentication technology is applied with precision, speed, and scale. The results speak directly to the need — and to the opportunity that SecureLogix's approach uniquely addresses.

The engagement at this institution is also a clear illustration of a principle that SecureLogix consistently advocates to enterprise clients: outbound call trust must be built on a foundation of secured, authenticated, and spoofed-protected calling numbers before identity is amplified through branded calling. Deploying call branding on numbers that fraudsters are actively spoofing doesn't just fail to solve the problem — it potentially makes the problem worse by increasing consumer recognition of numbers that bad actors are simultaneously weaponizing. Protection first. Then you are safe to amplify caller identity.

Key Takeaways

- Fraudsters were spoofing approximately 30% of outbound calls from the bank's primary contact center numbers — a threat that carrier-level reporting and STIR/SHAKEN data analysis made visible and quantifiable.
- SecureLogix TrueCall services deployed rapidly, providing active protection across three major wireless carriers within weeks, with minimal operational burden on the bank's internal teams.
- Over 8.3 million legitimate calls have been authenticated and over 3.2 million spoofed call attempts have been blocked in the initial months of service — with the program expanding to cover more numbers on a scheduled basis.
- Mass attack events — including a single week in which nearly 5 million calls were blocked — demonstrate both the scale of the threat and the effectiveness of the protection.
- Carrier level reports confirm that fraudsters are aware the bank has become a significantly harder target, with displacement effects already observed toward unprotected competitors.
- SecureLogix's proprietary Automated Vetting Solution can enable program scaling across any bank's large portfolio of phone numbers — unmatched scalability no competing service has achieved.

Voice Security & Outbound Call Trust

The Full SecureLogix Platform

SecureLogix is the only vendor in the industry delivering a single, unified platform that addresses the full spectrum of enterprise voice security and outbound call trust challenges, from inbound attack protection and call authentication to outbound number health, spoofing defense, and branded calling. The engagement at this major financial institution draws on several elements of that platform, and the full portfolio is available to enterprises at any stage of their voice security journey.

Call Secure™ managed call security service	SecureLogix's managed security service for enterprise voice delivers Call Defense System capabilities — voice firewall, IPS, and policy-driven call control — to protect against TDoS attacks, robocalls, fraud, social engineering, vishing, call pumping, and other inbound voice threats. SecureLogix has provided Call Secure protection at this bank since 2013.
Orchestra One™ inbound call authentication service	The SecureLogix inbound call authentication service leverages real-time carrier APIs with AT&T, Verizon, and T-Mobile, to deliver a risk score on every inbound call, enabling enterprises to route, challenge, or block suspicious calls before they reach agents. Orchestra One authentication is currently active in the bank's contact center environment.
Reputation Defense™ call number management service	The SecureLogix phone number reputation management and monitoring service works with major carrier analytics vendors to remove Spam and Fraud labels from enterprise calling numbers, restore healthy reputation scores, and maintain ongoing monitoring to prevent future mislabeling. SecureLogix currently manages over 900,000 phone numbers for this institution under Reputation Defense.
TrueCall™ spoofing protection service	The SecureLogix outbound call spoofing protection service integrates with all major wireless carriers and their analytics engines to authenticate outbound calls at the carrier network level, ensuring that only legitimate calls from the enterprise are delivered while every spoofed attempt is blocked. TrueCall's unique line-of-sight architecture, race condition mitigation, and Automated Vetting Solution deliver industry-leading protection scalability and accuracy.
Contact™ call branding service	The SecureLogix branded calling service enables enterprises to display a full rich-call identity — company name, logo, and call purpose — on the recipient's screen, dramatically increasing answer rates for legitimate outbound calls. Proposals for Contact deployment are in active discussion with this institution.

A Critical Note on Sequencing: Protect Before You Amplify

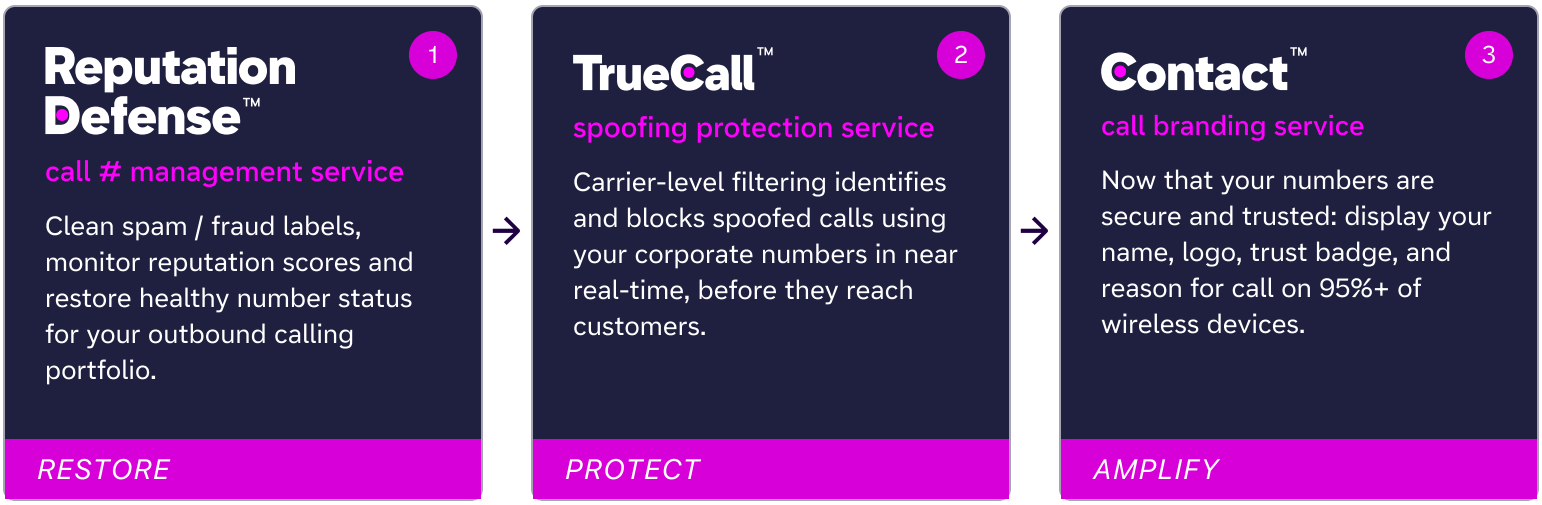
The Dangers of Naked Branding

Branded calling is a powerful tool, but deploying it on unprotected numbers is one of the most dangerous moves a financial institution can make. Every spoofed call now carries your verified name, logo, and trust badge, and the branding itself becomes a weapon to lure and empower more fraudsters. This is not a theoretical risk: spoofers actively monitor which companies launch branded calling and immediately target those numbers. For a high-profile financial brand, the consequences compound fast, with customers deceived into authorizing fraudulent transfers under your trusted identity, while spoofed activity triggers carriers to flag your legitimate numbers as spam, collapsing the very answer rates branding was designed to lift.

Establish Call Trust Before Branding

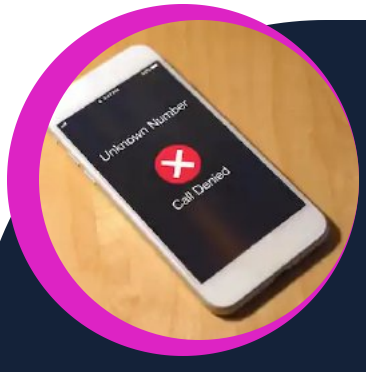
SecureLogix offers the full spectrum of outbound call trust services, from phone number reputation management and spoofing protection to full branded calling, and many enterprises deploy these capabilities in combination or independently based on their specific needs and priorities. SecureLogix encourages the layered approach that this institution has pursued: start by restoring the health and reputation of outbound calling numbers, add spoofing protection to lock down the identity of those numbers at the carrier level, and then layer in branded calling to amplify a call identity that is already secure and trusted. When all three services work together, branded calling becomes the capstone of a trusted outbound strategy, not an unprotected enhancement that increases your exposure to fraud, impersonation, and brand damage.

Secure Before Amplifying Brand



One Universal Platform. Full Call Security & Trust.

SecureLogix offers comprehensive voice network security and call trust services for inbound and outbound calls in one fully integrated universal platform helping enterprises increase outbound call answer rates while protecting their voice networks from fraud, spam, abuse & other threats.

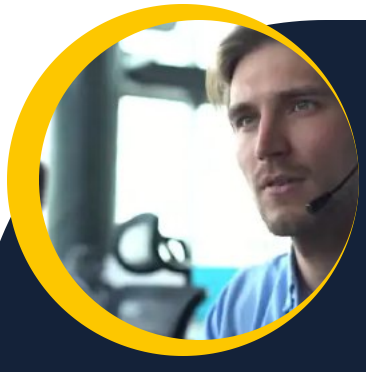


Outbound Call Trust

Increase answer rates, remove spam + fraud labels, and protect your outbound number from spoofing.

Inbound Call Security

Protect your business from robocalls, spam, fraud, TDoS attacks and other abuse.



Inbound Call Authentication

Verify every inbound call with automated call authentication and spoofing protection.

www.securelogix.com

v1.0.0 | K1-0415 | D-4000