Financial Institution Saves $400,000 in Call Center Fraud After Only 3 Months

Spoofing & Impersonation

Social Engineering & Financial Fraud

Challenge

A global financial institution was habitually targeted for financial fraud and account takeover attacks over phone calls into its call centers. Malicious callers used spoofing to mask the source of their numerous calls to service representatives in the institution's contact centers.

The malicious callers would glean pieces of relevant account information by making multiple social engineering calls about a single account. Once they had enough personal information, they would make a final call to take over a customer's bank account and commit financial fraud.

Approach

SecureLogix helped the bank identify patterns of fraudulent calls to stop the spoofed impersonation attacks. Using the SecureLogix® Call Defense™ System and related services, SecureLogix saved the client over $400,000 in just the first three months.

SecureLogix identified the unusual pattern of calls coming from same area code and exchange. The platform stopped the spoofed robocalls after new policies redirected these spoofed calls to fraud detection agents. The bank used the recorded calls as evidence for prosecution and to train agents on how to prevent future account takeover attacks.

Result

SecureLogix prevented millions of dollars in fraudulent wire transfers for the customer. By treating those calls differently, the banking institution stopped about $400,000 in fraudulent transfers in just the first three months of implementation.

SecureLogix continues to prevent account takeover fraud, enhance account security for their customers, and strengthened their overall contact center security posture for increased customer satisfaction.

Solution

CALL DEFENSE™
system

SecureLogix®

https://securelogix.com