USE CASE

Frost Bank Relies on Advanced Solutions for Robocalls & Fraud Prevention

Identifying and Mitigating Fraudulent Call Patterns Helps Protect Operations

Facing an increasing number of robocalls across their calling operations, Frost Bank needed a solution that identified suspect calls in real-time to avoid impacting its operational efficiency and customer experience. What the bank needed was a defense against malicious incoming calls that allowed for increased response times to legitimate customer calls and filtered out the spam calls attempting to make contact with the bank's agents.

Incoming robocalls are not exclusive to private landline and cell phone numbers, they also are targeting enterprise phone numbers. These robocalls can impact customer service efficiency and create fraud risk for the enterprise. The need for a solution that can evaluate the legitimacy of a caller without disrupting legitimate customer interactions is paramount in high-touch services such as finance.

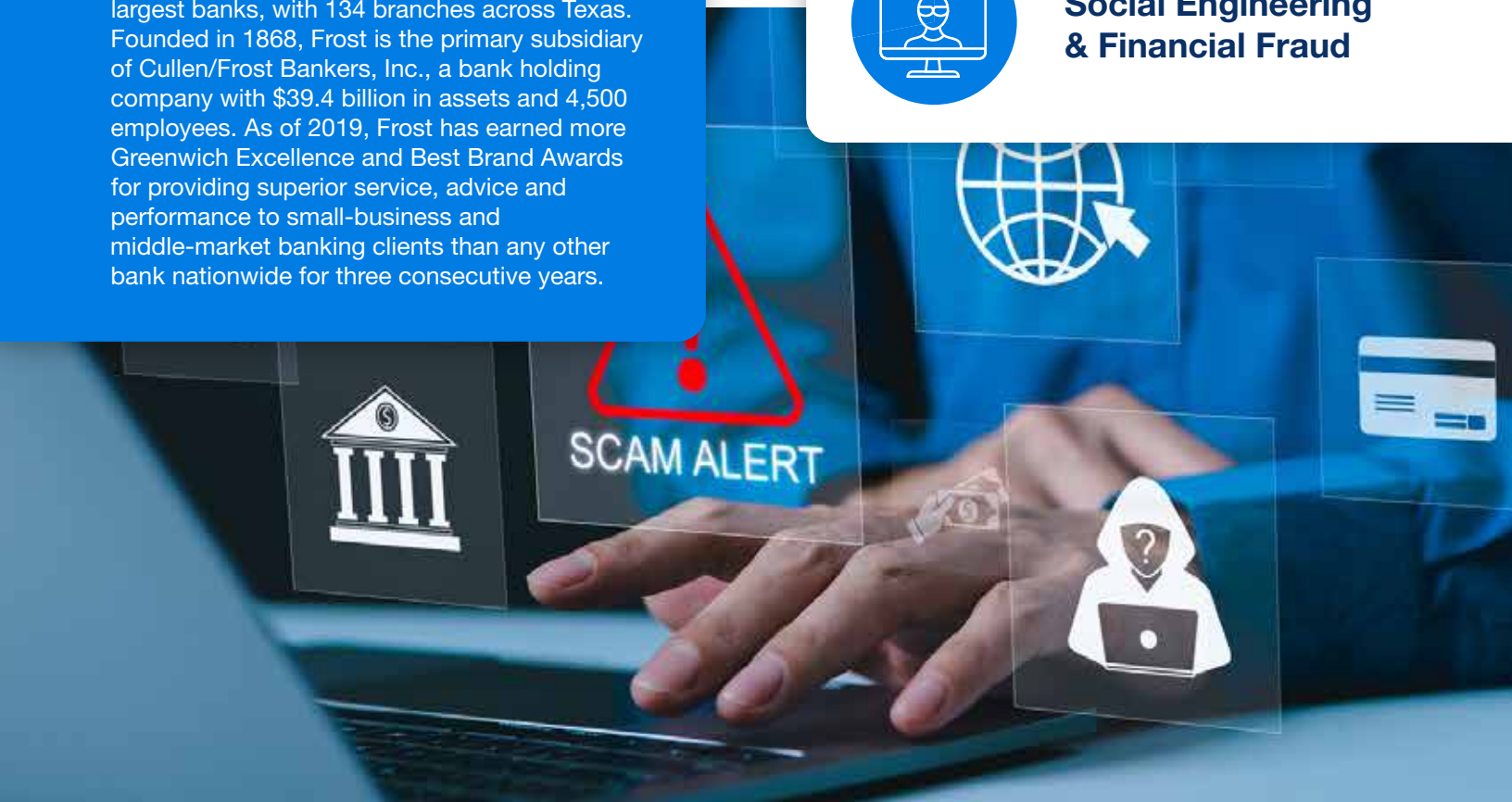
Business Challenge

Frost Bank was wrestling with the alarming growth in robocalls across its enterprise. The bank was concerned the volume of robocalls impacted customer service efficiency and introduced the potential for phone fraud.

Robocalls & Spam

Social Engineering & Financial Fraud

The San Antonio-headquartered financial services company is one of the nation's 60 largest banks, with 134 branches across Texas. Founded in 1868, Frost is the primary subsidiary of Cullen/Frost Bankers, Inc., a bank holding company with $39.4 billion in assets and 4,500 employees. As of 2019, Frost has earned more Greenwich Excellence and Best Brand Awards for providing superior service, advice and performance to small-business and middle-market banking clients than any other bank nationwide for three consecutive years.



Solution

Frost Bank quickly benefited from enhanced protection across its voice network through a managed call security solution. The service team leveraged continuously updated threat intelligence, drawn from malicious caller behavior and enterprise voice attack data, to identify and filter suspect calls in real time. As a result, the bank experienced faster response times for legitimate inbound customer calls, improving both operational efficiency and the customer experience.

Outcome

Frost Bank's voice network had on average about 750,000 monthly calls. The solution identified 3% to 5% of incoming monthly calls as fraudulent and blocked this malicious and unwanted traffic from reaching agents. While Frost's original concern was robocalls, the service was able to prevent all other types of fraudulent calls from spammers. These tools can proactively identify and mitigate fraudulent call patterns to prevent many types of fraud-risk phone calls from impacting operations.

TNS Enterprise Voice Security can help:

- Detect and filter suspicious voice traffic
- Deliver passive caller authentication through IVR integration
- Support dynamic threat mitigation and policy enforcement
- Improve inbound call answer rates and reduced wait times for customers.
- Use metadata and behavioral analytics to evaluate caller legitimacy without disrupting legitimate interactions
- Provide real-time insights and forensic call reporting

About TNS

Established more than 30 years ago, TNS has facilitated billions of branded calls, supporting thousands of organizations across more than 60 countries. TNS has over 10 years of call identification experience and handles over 1.5 billion daily call events from over 500 operators.

To learn how TNS Enterprise Voice Security can help your business, please contact our team.

solutions@tnsi.com
tnsi.com/solutions/communications/restoring-trust-to-voice/