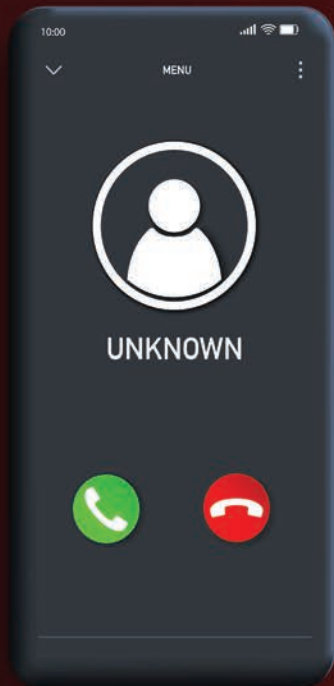


SecureLogix



**TOTAL DHS SBIR
INVESTMENT**
\$1M

**SBIR AWARDS
DHS**

**PHASE III
REVENUE**
Over \$6M

13750 San Pedro Ave.
Suite 820
San Antonio, TX 78232
www.securelogix.com

This once common response to a phone call, “Who is it?”, has become increasingly complicated in recent years. As reported by Truecaller, nearly 1 in 3 Americans say they’ve fallen victim to a phone scam in the past year. Whether it’s someone pretending to be from the Internal Revenue Service or from a company inquiring about an expiring vehicle warranty, these calls are not just a nuisance, they can also be a costly problem, with roughly 59.4 million Americans having lost money to phone scams over the past year.

This type of intrusion is called spoofing, and it enables a long list of illegal activities from impersonation attacks to account takeovers, and financial fraud. Combined with the advent of low-cost robocall technology, caller ID spoofing has spurred an exponential increase in phone-based attacks on contact centers and enterprise voice networks in just a few years. Spoofing makes all inbound voice call-based attacks more difficult to manage, including robocalls in general, scams, vishing, Telephony Denial of Service (TDoS) attacks, social engineering, and Account Takeovers (ATO) in financial contact centers.



These pervasive scams—in which callers pretend to be government employees or financial service representatives and mislead victims into providing personal information or make payments—have become a scourge on the American public, with the Federal Trade Commission reporting victims lost nearly \$153 million to government impostor scams in 2019.

Recognizing this threat, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and Small Business Innovation Research (SBIR) program sought solutions to curb these attacks by funding research and development efforts with SecureLogix, a small business based in San Antonio, Texas, through the SBIR program.

To begin with, DHS S&T set out to identify the evolving threat and enterprise and service provider countermeasures that would enable solutions to be built for these environments. The resulting innovation, the Orchestra One™ call authentication service, stops Caller ID Spoofing by auto-authenticating calls in real time. This solution means that customer calls can be delivered to the contact center with a higher degree of confidence, malicious calls can be automatically filtered out, and questionable calls can be sent through a configurable series of additional filtering

and evaluation for the most efficient and cost-effective decision.

The contracts received by SecureLogix from SBIR, America's Seed Fund, were critical to the early-stage development of the technology. The company leveraged the funding and now Orchestra One™ is a commercially successful product generating over \$6 million in revenue from industry customers, including Verizon and AT&T.

“We’re a small company,” said Mark Collier, SecureLogix Chief Technology Officer, “and in order to add new capabilities and reach new customers we used S&T and SBIR funding to add talent! Without this investment, we would not be able to keep pace with the issues and continually innovate.”

The foresight by DHS S&T to develop topics in this area, and support from Drs. Ann Cox and Dan Massey provided SecureLogix with a business and innovation-friendly environment in which to mature Orchestra One™. Today, the Orchestra One™ call authentication service from SecureLogix is helping to protect U.S. citizens, organizations, and government from call spoofing and other threats.