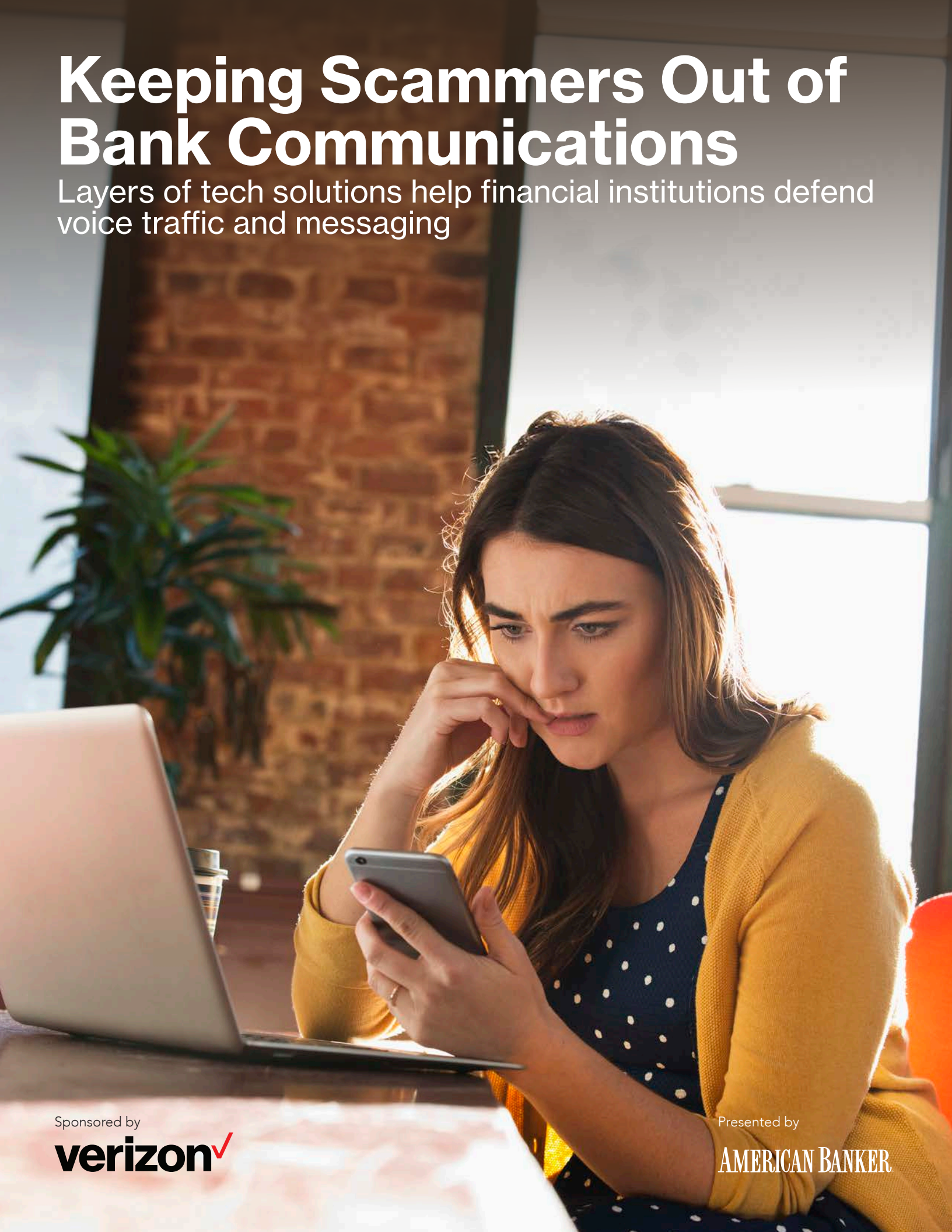
Keeping Scammers Out of Bank Communications

Layers of tech solutions help financial institutions defend voice traffic and messaging



Sponsored by

verizon

Presented by

AMERICAN BANKER

Spam calls have caused customer mistrust—a difficult barrier to overcome.

75% of Americans will never answer calls from unknown numbers.

Financial institutions are scrambling to protect customers and themselves from scammers generating fraudulent communications, but there is no silver bullet in a fast-changing threat landscape. Telephone fraudsters are draining consumer bank accounts using AI-faked voices, spoofed phone numbers and texts, and unauthorized call forwarding. Banks and credit unions are battling a breathtaking wave of social engineering scams as criminals find ingenious methods to mimic voices, steal account credentials, and defraud customers.

Sophisticated impersonation scams are built across multiple communication channels, including voice calls, texts and emails. Calls coming into financial institutions can be scammers masquerading as customers, and outgoing calls – sometimes even authentic-looking branded calls – may be spoofed. A common tactic is for fraudulent callers to pose as bank employees investigating identity theft, or as officials from a consumer protection agency, such as the Federal Trade Commission (FTC) or Consumer Financial Protection Bureau (CFPB). Pretexting schemes often break down a victim's defenses by instilling a false sense of urgency to keep victims on long phone calls, exhausting their ability to reason.

Organized crime rings have the resources and patience to conduct scams that unfold over days, weeks or months, often leveraging consumer data obtained from previous corporate breaches. "We're seeing massive attacks happening, with bad actors loading malware, ransomware, and doxxing or swatting executives. We think it's going to get worse with AI," says Will Gordy, Director of Workplace Collaboration and Customer Experience at Verizon. Once a consumer is targeted and their credentials compromised, fraudsters typically make calls to the bank or financial institution. Banks and financial institutions also need to guard against becoming a link in the chain for fraud attacks.

While many still think of scams as targeting mainly older adults, this is a fallacy. Fraud today affects consumers and businesses across the board. In fact, Gen Xers, millennials and Gen Zers are 34% more likely than people in their 60s or older to report being defrauded, according to data from the FTC. Bank customer losses are on the rise, with $12.5 billion reported lost to fraud in 2023, according to the IC3 2023 Internet Crime Report. Actual losses are likely higher, as not all cases are reported.

In 2023, more than 800,000 cases of imposter fraud were reported, with 21% of cases resulting in financial loss, according to the FTC.

Today's evolving threat landscape

Various forms of imposter fraud leverage voice calls, text messages or emails to defraud consumers and businesses. Here are some findings from the 2023 IC3 report:

Business email compromise: BEC schemes resulted in over $2.9 billion of losses in 2023. Criminals are increasingly "using custodial accounts held at financial institutions for cryptocurrency exchanges or third-party payment processors, or having targeted individuals send funds directly to these platforms where funds are quickly dispersed," the report said.

Tech and customer support scams: Reports of such scams increased 15% in 2023, resulting in losses of over $924.5 million.

Government impersonation: These include schemes in which callers claim to be officials investigating identity theft or credit card scams. These scams rose 63% and led to losses of $394.1 million in 2023.

Confidence and romance scams: A scheme in which the perpetrator preys on the target's heartstrings to induce them to send money. This could be a romantic partner or family member. For example, in "grandparent schemes," a victim may receive a voice call that sounds like it is from a grandchild who urgently needs assistance. Losses reached $652.5 million in 2023.

Voice call attacks come in many forms:

- Impersonation
- Telephony denial of service (TDoS) attacks
- Harassing or malicious calls
- Robocalls
- Account takeover
- Unwanted calls flooding contact centers
- Social engineering attacks

Financial institutions' ability to operate through voice and text channels is jeopardized when consumers lose confidence in the integrity of those networks. Public trust in voice and text communications is already badly eroded as news headlines frequently report that even well-respected members of society – financial experts, government scientists, television personalities – are falling victim to social engineering. Last year, a former White House science advisor lost over $600,000 in a scam that started with an identity theft alert on her computer screen, prompting her to call a fake Microsoft toll-free support hotline. She was then instructed to call the customer service number on the back of her credit union banking card. The victim believed that initiating the call herself, to a known number, was a safe course of action – but she didn't know that bad actors had put in place unauthorized call forwarding, enabling them to intercept calls from her credit union as they drew her into a devastating cryptocurrency scheme.

"The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities," according to the Verizon 2023 DBIR.

In another case, a financial advice columnist for New York Magazine's "The Cut" was scammed out of $50,000 after answering a spoofed call that seemed to be from an Amazon customer service rep confirming an $8,000 transaction. When she denied having purchased multiple MacBooks and iPads, the pretexting scheme expanded. Two subsequent callers impersonated officials at the FTC and the Central Intelligence Agency, and used Cowles's accurate date of birth and Social Security number to further the charade. The columnist later wrote, "I never thought I was the kind of person to fall for a scam."

The Bravo TV celebrity, Andy Cohen, was defrauded in an imposter scam in which he believed he was communicating with his own bank. He clicked on an email link that led to a spoofed bank website, where he logged in – unwittingly giving scammers access to his online banking. He became

suspicious when he was asked for his Apple ID and password, but the groundwork for the scheme was already in place. A fake bank-branded text message asked him to confirm a credit card purchase, followed by a spoofed call which displayed his bank's name on caller ID. The thieves read him accurate information from his hacked account to gain his trust, then they convinced him to enter numerical codes that initiated wire transfers out of his account and forwarded bank calls to the fraudsters.

A crime ring in Pennsylvania defrauded credit union members of nearly $2 million last year, spoofing branded calls and impersonating employees. "The suspects disguised their phone numbers to make it seem as if the calls were coming from the banks' phone numbers," reported CBS News. The victims were then locked out of their accounts while money was directed out of them.

"74% of all breaches include the human element," according to Verizon's Data Breach Investigation Report (DBIR), whether that means human error, misuse of employee privileges, stolen credentials, or social engineering.

AI voice clones

Video and voice deepfakes are a potentially devastating problem for banks and credit unions. Fraudsters can use a voice deepfake together with stolen account data from past breaches to trick customers or bank employees into approving wire transfers. Many financial institutions have adopted voice biometrics for customer identification and authentication, but fraudsters now have ready access to AI-based tools that mimic real customer's voices based on small recorded samples from social media accounts or corporate websites. One generative-AI tool on the market can create a voice deepfake from just three seconds of audio recording. "The falling costs of generative artificial intelligence programs and the wide availability of recordings of people's voices on the internet have created the perfect conditions for voice-related A.I. scams," reported the New York Times in an August 2023 article, "Voice Deepfakes Are Coming for Your Bank Balance."

C-suite attacks

Financial executives and board members are high-value targets since their powerful positions can be co-opted for monetary gain or influence. Not only are executives' corporate cellphones and tablets vulnerable, but attacks can be directed at their personal mobile devices, or those of friends and family members. Fraudsters can then impersonate the executive to trick employees into wiring funds or exposing sensitive information.

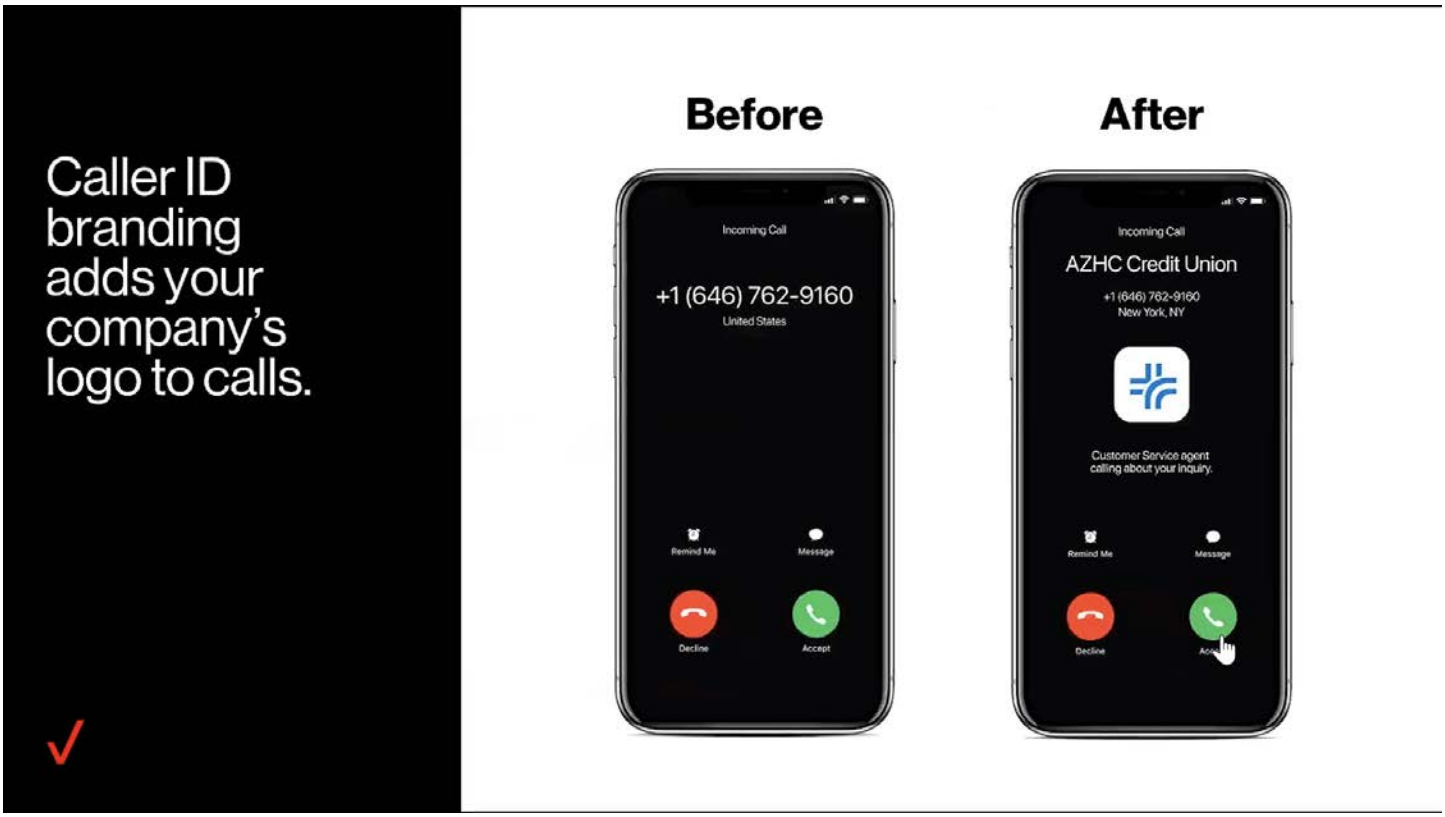
"Posing as a C-level executive can create an entry point for fraudsters. The contact center is a landmine because it's a source of knowledge for an organization. If a fraudster can crack into the contact center, they can access a lot of information," says Alicia Gee, Director of Consulting Services Customer Experience at Verizon.

"These criminals can't be stopped by banks alone...Banks also need the telecom companies and their regulators..." – Paul Benda, Executive Vice President, Risk, Fraud and Cybersecurity for the American Bankers Association.

Improving defense through strong telecom partnerships

Banks don't need to fight fraud on their own. Telecom companies can be effective partners.

The growing sophistication of international fraud rings, the pace of technological change, the widespread use of AI deepfakes – these factors make it extremely challenging for financial institutions to combat voice and text fraud on their own. This is why banks and credit unions need effective partners with deep industry knowledge to help stem the proliferation of phishing, smishing, vishing, social engineering, spoofing and other threats.



Government regulations are certainly one important layer in this battle. Federal Communications Commission (FCC) rules requiring IP voice network providers to use the STIR/SHAKEN standard go part of the way in protecting the integrity of voice calls. STIR/SHAKEN — the acronym stands for Secure Telephone Identity Revisited and Signature-based Handling of Asserted Information Using toKENs — is a caller ID authentication protocol that allows calls to be validated by carriers as they travel through interconnected phone networks, an important step in combating spoofed robocalls.

But this authentication standard does not block calls or identify malicious intent. It only helps identify and validate calls on IP networks. STIR/SHAKEN, on its own, doesn't solve voice fraud.

In a February hearing before the Senate Banking Committee, fraud expert Paul Benda testified on behalf of the American Bankers Association that banks are making extraordinary efforts to safeguard accounts against fraud. However, "the fight against these criminals is one that banks cannot win on their own."

Benda called for carriers and telecom regulators to partner with banks and financial institutions in fighting the wave. Fraud rings are "becoming more sophisticated, using new advanced deepfake technologies to change their voice and appearance in real-time video calls to execute romance and impersonation scams," he said.

Speaking for banks, Benda cited the need for assistance from the telecom industry in identifying and blocking spoofing calls, stopping denial of service attacks, recognizing suspicious phone numbers and more. He emphasized that financial institutions — despite their extensive technology investments — aren't equipped to fight all new forms of fraud on their own. Instead, they must partner with carriers, law enforcement, social media companies, and others. "Banks also need the telecom companies and their regulators to close regulatory loopholes that allow criminals to spoof legitimate names and phone numbers to convince customers they are speaking with a bank," said Benda.

Layers of fraud protection

To protect business communications, contact centers and customer experience, banks and credit unions will need to invest in layers of technological solutions to defend against a variety of forms of attacks. In the physical world, brick-and-mortar banks have long employed multiple layers of

fortification to assure customers that their money is secure. Walking into a bank or credit union, consumers are able to see armed guards, armored trucks, fortified buildings, bulletproof glass and strong steel vaults.

Similarly, in the digital world, financial institutions will want to invest in layers of voice security solutions to help protect business communications, safeguard contact centers, enhance customer experience and restore trust. The leading carriers in the industry are on the forefront of working with the FCC to improve standards, identify suspicious phone numbers and shut down sources of fraudulent activity domestically and internationally. Not all carriers operate at the same level, however. Strong carriers can assist financial institutions with putting in layers of protection at the network level, the enterprise level, and more, including:

- Monitoring at the network level, carriers utilize 24/7 monitoring to identify and block the largest sources of fraud.
- Adding firewalls that block or terminate calls according to rules and policies and send real-time alerts of attacks.
- Engaging TDoS detection and mitigation and other enterprise-level protection.
- Identifying voice security solutions that can analyze the audio of a call, detect audio from the caller and device, and analyze behaviors, to provide a deeper level of caller authentication.
- Providing branded outbound calls, so customers can be assured that the calls are legitimately from the financial institution.

How can banks and credit unions assess their voice network's vulnerabilities and which defense solutions to prioritize? "Many of our clients look to us to advise them on where the next threats are coming from. We provide knowledge training and table top exercises to develop a framework for reestablishing trust with customers and members," says Gordy.

Next steps

Voice and text-based threats originate from both the U.S. and overseas. Inbound and outbound calls require different fraud solutions. Banks and credit unions need to protect their call centers from a wide range of bad actors. Financial institutions will want to work with a strong telecom partner to assess their vulnerabilities and help them identify the right strategies and technology solutions.

It starts with a conversation. Strong carriers, such as Verizon, stand ready to assist financial institutions in navigating the evolving digital fraud landscape. To help protect banks — and their brand reputations — from voice security breaches and voice call fraud, Verizon offers consulting, risk assessment services and a portfolio of voice security solutions. To learn more, you can visit us at https://www.verizon.com/business/products/contact-center-cx/voice-security/
Or reach out to Mark Bubar to schedule an appointment with one of our voice security specialists.

The author of this content is a paid contributor for Verizon.