



Broadcom Launches Arcot Scam Defense to Block Social Engineering Fraud

October 21, 2026

PALO ALTO, Calif., Oct. 21, 2026 (GLOBE NEWSWIRE) -- Broadcom Inc. (NASDAQ: AVGO), a global technology leader that designs, develops, and supplies semiconductors and infrastructure software, today announced the launch of Arcot Scam Defense, a groundbreaking new feature of Arcot by Broadcom, designed to block social engineering fraud during card-not-present (CNP) transactions.

"Financial institutions are experiencing broad increases in fraud attempts driven by sophisticated, AI-enhanced social engineering attacks," said Matt Cooke, vice president and general manager, Payment Security Division, Broadcom. "While technological security systems have advanced and are highly effective at blocking fraud, fraudsters have pivoted their efforts to hacking customers directly. By impersonating trusted brands and institutions, they trick cardholders into revealing passwords or completing step-up authentications. Cardholders usually remain unaware that they have handed over the keys to the castle until after the scam."

How Social Engineering Works

During a payment flow, once a cardholder completes a 3-D Secure authentication challenge, by entering a one-time password (OTP) or using a biometric, the transaction is treated as legitimate and is approved by a financial institution's primary risk models. While real-time risk assessment models are highly effective at flagging suspicious transactions, they are not designed to stop a legitimate account holder actively under the influence of a scam.

Introducing Arcot Scam Defense

"Arcot Scam Defense closes a critical gap," added Cooke. "It serves as the definitive safety net against social engineering attacks. Operating as a real-time second layer of defense, it leverages advanced intelligence during authentication to flag suspected fraud – even after a successful challenge. By closing the approval door on these attacks, we increase cardholder safety and drive down fraud losses, while continuing to allow legitimate transactions through."

Arcot Scam Defense analyzes a broad range of signals across transaction information, device intelligence, historical behavior, and the challenge interaction itself to identify patterns indicative of social engineering. These can include discrepancies in the location and behavior of the transacting checkout device and the authenticating device, delayed OTP entry, the use of an alternative authentication method, or a significant physical distance between the two devices. These signals are evaluated collectively to inform a real-time decision rather than relying on any single indicator. Additionally, the solution can integrate with third-party solutions to determine if the authenticating device is on an active phone call, which is a prime indicator of social engineering.

Even if a cardholder falls for a scam and hands over their credentials, Broadcom's Arcot Scam Defense feature can help identify the behavioral shift and block the transaction in real time.

The scale of the problem is immense, with nearly half a billion dollars in fraud reported over the last 12 months on successfully authenticated challenges. In pilot testing validated on a full month of live data, the Arcot Scam Defense feature demonstrated exceptional performance. For one major pilot issuer, reviewing just the top 1% of successful challenges would have protected an estimated \$4 million in fraud in just a month, at a cost of only 0.38 points off their authentication success rate.

Looking ahead, Broadcom expects to expand Arcot Scam Defense's capabilities by adding new signals, including cardholder and device attributes, and a dedicated challenge history profiling engine to learn each cardholder's past challenge behavior.

Arcot by Broadcom is exclusively focused on 3-D Secure payment authentication. For more information on how Arcot is redefining payment security, visit <https://www.broadcom.com/products/software/payment-security>.

About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a technology leader that designs, develops, and supplies semiconductors and infrastructure software for global organizations' complex, mission-critical needs. Broadcom combines long-term R&D investment with superb execution to deliver the best technology, at scale. Broadcom is a Delaware corporation headquartered in Palo Alto, CA. For more information, visit www.broadcom.com.

Broadcom, the pulse logo, and Connecting everything are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries. Other trademarks are the property of their respective owners.

Press Contact:

Eloy Ontiveros
Broadcom Global Communications
+1.650.427.6145
eloy.ontiveros@broadcom.com