



PCI DSS Compliance on Wi-Fi Devices? Easy as 1-2-3

White paper reveals three best practices to meet credit card security requirements

Akron, Ohio, May 2, 2008 – A new white paper from Summit Data Communications, a leading provider of Wi-Fi® radio modules and cards for mobile computers and other business-critical mobile devices, reveals three best practices for ensuring that Wi-Fi client devices are compliant with the Payment Card Industry Data Security Standard (PCI DSS). The best practices are to use the strongest standards-based security on every Wi-Fi client, minimize the number of Wi-Fi client configurations and radios in use, and rely on ease-to-use client configuration software.

“If you handle credit card information, then you must protect it from thieves that are growing increasingly sophisticated,” said Ron Seide, Summit’s president. “Without adequate network security, retailers run the risk of having credit card information stolen. Even a single theft can permanently damage your reputation and your business.”

Because credit card companies, not retailers, are held responsible for fraudulent charges due to stolen credit card information, major credit card companies have established the Payment Card Industry (PCI) Security Standards Council. The Council has created a common set of guidelines for how retailers must protect the credit card information stored, processed, and transmitted on their networks. Those guidelines are codified as requirements in the PCI Data Security Standard, or PCI DSS. A retailer that fails to comply with PCI DSS can face stiff penalties, including losing the right to accept credit cards.

An in-store Wi-Fi network with inadequate protections enables thieves to steal credit card information without entering the store. A Wi-Fi security scheme is viable only if it is supported by every client devices that is allowed on the network.

“The success of your entire PCI DSS compliance strategy can hinge on the Wi-Fi radios in your client devices,” said Seide. “If those radios support strong, standards-based security and can be configured quickly and easily, then achieving compliance is straightforward and easy. If not, then achieving compliance may prove extremely difficult.”

The Summit white paper, “Ensuring PCI DSS Compliance on Wi-Fi Client Devices”, focuses on PCI DSS requirements that apply to Wi-Fi client devices and identifies three best practices for those devices. The white paper is available free of charge from the Summit Web site, www.summitdatacom.com.

About Summit

Summit Data Communications, Inc. is dedicated to providing high-performance wireless LAN radio modules and cards for today’s business-critical mobile devices, such as mobile computers, portable printers, medical devices, and industrial automation equipment. Summit radios are optimized for the challenging radio environments in which business-critical mobile devices operate, including factories, warehouses, ports, hospitals, and retail stores.

Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

###