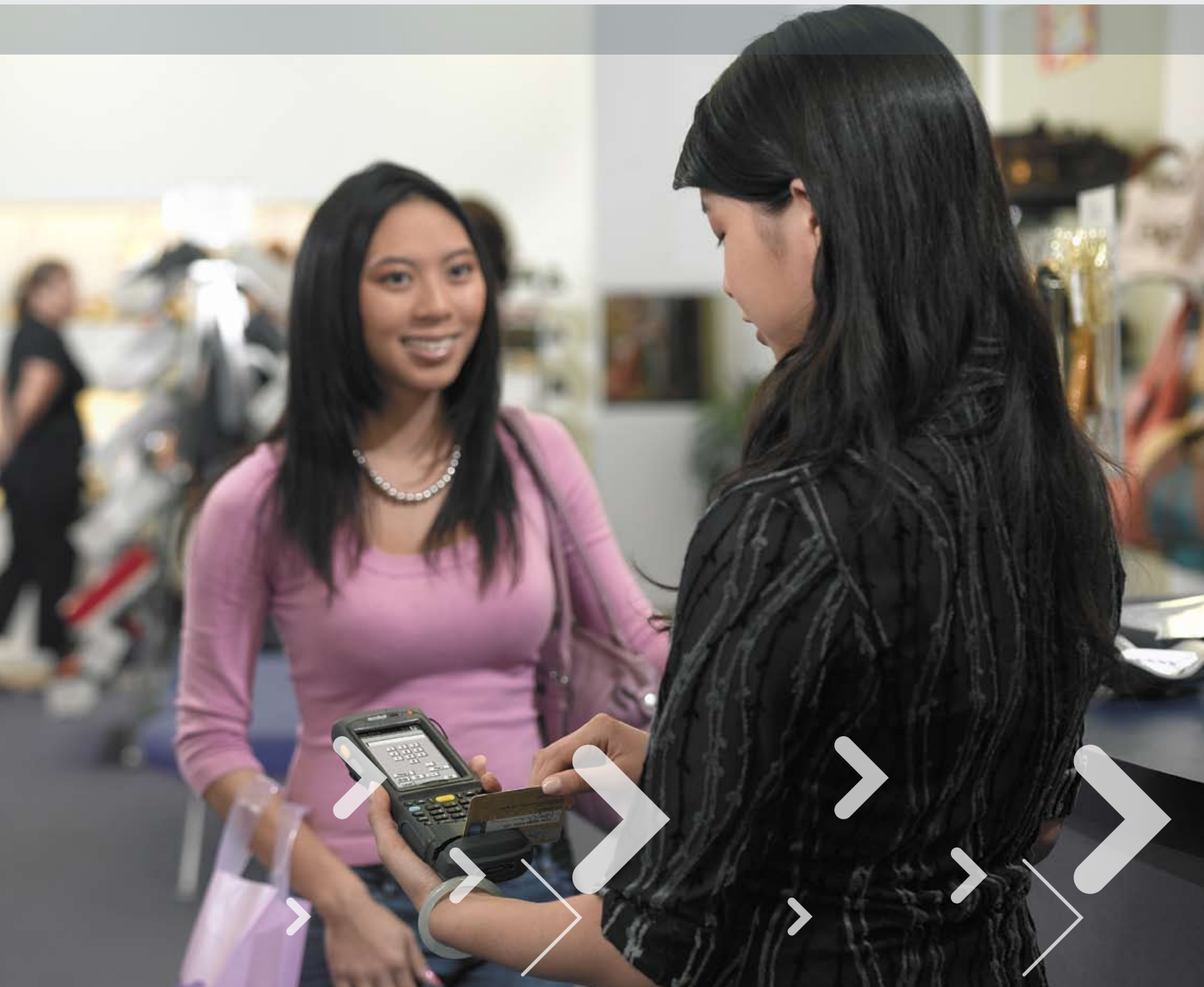




Motorola Helps Customers with PCI Solutions



SAFEGUARD YOUR INFRASTRUCTURE TO PROTECT CUSTOMER DATA

If you are like the many companies trying to understand how to keep customer information safe from data breaches, you are not alone. Wired and wireless technologies alike offer a lucrative opportunity for hackers to circumvent security architectures, allowing access to sensitive information that can result in brand damage, financial/regulatory liabilities and business disruption. Any business that has credit card information anywhere on their network is considering how to keep that information secure while complying with Payment Card Industry (PCI) standards.

Businesses large and small are not only worried about compliance, but ongoing security - and with good reason:

- *In a 2009 data breach study conducted by Verizon Business, over 285 million records were compromised in 2008. Of the confirmed breaches within the report, 98% of the lost records were payment card related.*
- *The Ponemon Institute found the total cost of coping with the consequences rose to \$6.6 million per breach, up from \$6.3 million in 2007 and \$4.7 million in 2006 in its study of companies that suffered a data breach last year.*
- *And according to Forrester Research the cost of a data breach is \$300 per compromised record, which can easily be twenty times the cost of PCI compliance.*

So all vendors, regardless of their size or the kind of network they run, are looking at how to achieve compliance while safeguarding their infrastructure for today's requirements and tomorrow's threats.

Key Wireless Requirements for PCI Compliance

Since its inception in October 2008, the PCI Security Standards Council released the global Data Security Standard (DSS), where any organization who processes, stores or transmits cardholder data must take steps to implement security best practices.

Now, with the increasing prevalence of wireless technologies, the PCI Security Council has mandated more stringent network security measures, placing strong emphasis on rogue wireless prevention and location scanning. PCI guidelines also recommend a wireless Intrusion Protection System (IPS) to automate intrusion detection for large organizations. The use of WPA2 is recommended as well as other best practices concerning wireless firewalls, wireless monitoring/logging, physical security and wireless policy enforcement. Other key highlights include:

Scanning:

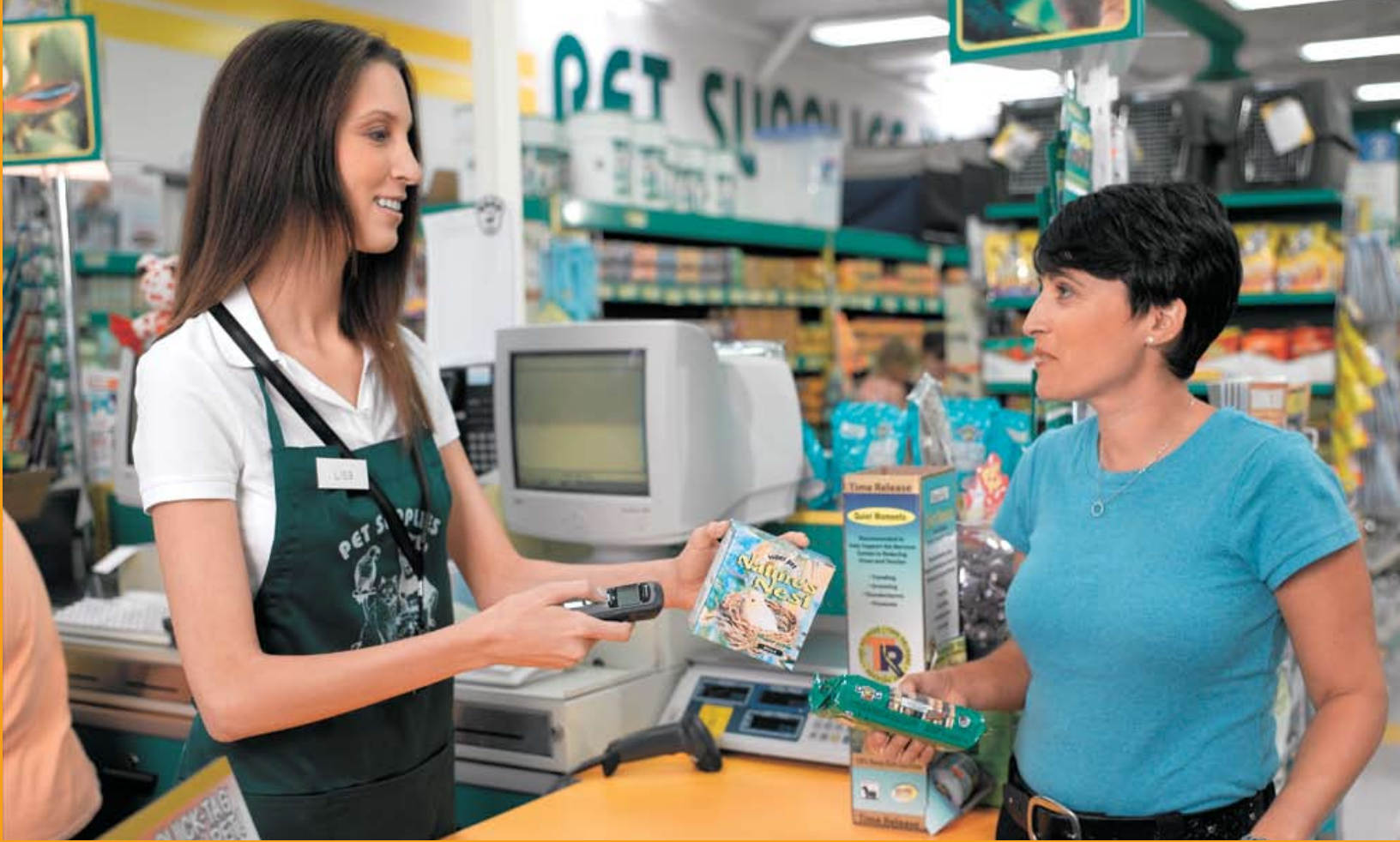
- All locations need to be scanned for rogue wireless devices regardless of deployment
- Automating the process with a wireless IPS is recommended for large deployments
- Wired-side scanning tools are inadequate
- Rogues on the network need to be eliminated

Encryption:

- WEP must be removed from the cardholder environment beyond June 30th, 2010
- WPA2 Enterprise with AES encryption and EAP authentication is recommended
- Wireless firewalls segmenting unnecessary wireless traffic from CDE is required

Other Requirements:

- Change defaults on wireless devices and disable unnecessary protocol and services
- Log all wireless access for one year and review logs daily
- Develop and enforce wireless usage policies by actively monitoring connections
- Physically secure wireless devices to prevent tampering



Why Motorola?

The good news is that Motorola can help bring together the critical pieces of your business to create a PCI and EMV (Europay MasterCard VISA) compliant solution, so you can mitigate the risks of security breaches and help decrease the cost of compliance. Motorola has successfully deployed security solutions for numerous retailers and businesses globally with a portfolio of enterprise mobility products that when implemented, managed, and maintained according to recommended PCI guidelines, offer a fully PCI and EMV compliant solution.

The best way to ensure compliance is to invest in technology that is PCI-capable. A Motorola Enterprise Mobility Solution — including data capture devices, mobile computers and enterprise WLAN infrastructure, implemented and maintained with advanced services — can provide the technology necessary to build a complete end-to-end PCI-capable solution.

PCI compliance is dynamic; ongoing maintenance and management must be performed to ensure continued compliance. The reference table in the inside spread provides a snapshot of the many products and services within Motorola's enterprise mobility solution portfolio that can be leveraged to help meet PCI requirements and secure your infrastructure. And at the end of the day, nothing is more important than protecting your customers.



Summary of Requirements and How Motorola Can Help

Motorola Solutions	Enterprise Mobility Services				
	PCI Planning & Assessment Service	PCI Policy and Procedure Design Service	PCI Network Design Service	PCI Design Implementation Service	PCI Security Monitoring Service
PCI Requirements					
Build and Maintain a Secure Network					
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	●	●	●	●	
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	●	●			
Protect Cardholder Data					
Requirement 3: Protect stored cardholder data	●	●	●	●	
Requirement 4: Encrypt transmission of cardholder data across open, public networks	●	●	●	●	
Maintain a Vulnerability Management Program					
Requirement 5: Use and regularly update anti-virus software or programs	●	●	●	●	
Requirement 6: Develop and maintain secure systems and applications	●	●			
Implement Strong Access Control Measures					
Requirement 7: Restrict access to cardholder data by business need to know	●	●	●	●	
Requirement 8: Assign a unique ID to each person with computer access	●	●	●	●	
Requirement 9: Restrict physical access to cardholder data	●	●			
Regularly Monitor and Test Networks					
Requirement 10: Track and monitor all access to network resources and cardholder data	●	●	●	●	
Requirement 11: Regularly test security systems and processes	●	●	●	●	●
Maintain an Information Security Policy					
Requirement 12: Maintain a policy that addresses information security for employees and contractors	●	●			
Additional PCI DSS Requirements for Shared Hosting Providers					
Requirement A.1: Shared hosting providers must protect the cardholder data environment	●				

Motorola Enterprise Mobility Solutions can help bring together the critical pieces of your business to address network security. This table outlines how Motorola's enterprise mobility solutions portfolio can help you build a PCI-capable solution.

Footnote 1: Motorola devices are capable of meeting this requirement when operating in a PCI compliant system.
Footnote 2: End customer driven.

Enterprise WLAN			Enterprise AirDefense	Mobility Services Platform	Mobile Computing Devices	Advanced Data Capture Devices
Access Points	Wireless LAN Switches	RF Management Software			Enterprise Class and Industrial Class	General Purpose, Rugged and MicroKiosks
•	•			•	•	•
•	•	•	•	•	•	•
					1	1
•	•	•			1	1
				•	•	•
				•	1	1
					2	2
					•	•
					•	•
					•	•
•	•		•		2	2
•	•		•		•	•
			•	•		

A TOTAL PCI SECURITY SOLUTION FROM MOTOROLA

Enterprise Mobility Services

- **PCI Planning and Assessment:** Motorola helps you prepare for PCI compliance audits by identifying the systems and resources that must be PCI compliant and determine where gaps exist.
- **PCI Policy and Procedure Design:** Motorola helps establish practical security policies in the Technology, Management, and Operations domains across all 12 requirements of the PCI DSS that work in your business environment.
- **PCI Network Design:** PCI Network Design addresses security gaps associated with your network infrastructure to help create a Cardholder Data Environment (CDE) that is compliant with PCI DSS requirements.
- **PCI Design Implementation:** The PCI Design Implementation service provides turnkey delivery of the PCI Network Design, including:
 - Project Planning for equipment installation and turn-up
 - Staging of equipment
 - Installation of equipment
 - Acceptance Testing
- **PCI Security Monitoring:** Motorola's Security Operations Center (SOC) provides around-the-clock real-time monitoring of the wired and wireless PCI CDE.

www.motorola.com/business/services; click Security Services

Enterprise WLAN

Motorola's Enterprise Wireless LAN & Security solutions are designed to provide out-of-the-box PCI compliance, robust wireless security and cost-effective compliance validation.

Motorola's portfolio of wireless LAN infrastructure is built on an integrated upgradeable platform, allowing organizations to cost-efficiently extend wireless networking from headquarters to other locations. The WS2000 Wireless Switch offers a network-in-a-box solution for small enterprises and remote sites, including an integrated router, gateway, firewall, and Power-over-Ethernet (PoE). The RFS7000 provides robust, highly scalable support for enterprise mobility, offering enhanced roaming, security, quality of service and management features. Motorola's RF Management Suite (RFMS) is a powerful set of integrated applications that enable administrators to execute end-to-end design and management of wireless LANs — pre- and post-deployment. All Motorola APs are designed for enterprise class wireless security supporting IEEE 802.11i (WPA and WPA2 certified) and 3DES IPsec encryption.

www.motorola.com/business; click Wireless LAN

Motorola AirDefense Solutions – Wireless LAN Security

Motorola Enterprise AirDefense provides a cost-effective mechanism to comply with PCI DSS wireless requirements, by recognizing all WLAN devices, including APs, WLAN user stations, "soft APs," and specialty devices such as wireless bar code scanners and mobile terminals. The solution identifies rogue behavior from ad-hoc or peer-to-peer networking between user stations and accidental associations from user stations connecting to neighboring networks. Motorola Enterprise AirDefense can also distinguish neighboring devices from rogue devices and can automatically terminate a rogue device over the air. Alternatively, the device can be blocked on the wired side using switch port suppression. To find the location of the rogue device, Motorola provides accurate map-based location tracking using signal strength triangulation. The system intelligently sorts through multiple floor plans and enables the IT administrator to locate and track rogue devices in real-time.

www.motorola.com/business; click Wireless LAN Security



Motorola also offers an innovative PCI Warranty, for assurance that our services will help you attain PCI compliance.

When you engage Motorola for PCI Planning and Assessment Service and follow up with our PCI Network Design and PCI Network Implementation services, our PCI Warranty ensures that you will pass your next PCI audit. If you do not, Motorola will come back and rework the solution at our expense. Ask for more details since some restrictions apply.

Mobility Services Platform

Motorola's Mobility Services Platform (MSP) is a management system that allows central control to be imposed over mobile devices that are deployed throughout an enterprise. While MSP does not currently have any features that are specifically focused on PCI compliance, it nonetheless can provide an invaluable tool in helping to achieve PCI compliance.

Depending on the nature of your enterprise network(s) and the applications in which you have mobile devices engaged, you may well have mobile devices that are considered in scope and subject to PCI guidelines. When this is the case, achieving PCI compliance will almost certainly require you to demonstrate that your mobile devices meet the PCI guidelines.

Your overall plan for PCI compliance will need to include specific definitions of what configurations will be applied to mobile devices and what management activities will be performed on them on an ongoing basis. MSP provides a powerful tool for executing those portions of your PCI compliance plan that relate to mobile devices and to collect evidence to demonstrate that your plan is being followed.

www.motorola.com/business;
click Mobility Software

Mobile Computing Devices

When it comes to selecting handheld computers that will securely mobilize your enterprise applications, there is a Motorola mobile computer designed to meet your needs. Motorola mobile computers keep the world's largest retailers up and running every day, regardless of requirements, application or environment. Motorola has a line of PCI-certified, and international EMV-certified, payment devices which form an end-to-end PCI-complaint solution, when used with new or existing Motorola mobile computers, a PCI-certified payment solution, and when operating within a PCI-compliant system. The PCI-complaint system can be realized by using an infrastructure designed with the Motorola Services, WLAN products and Enterprise AirDefense solutions.

www.motorola.com/business;
click Mobile Computers

Advanced Data Capture Devices

Motorola provides the industry's most robust and innovative line of Symbol scanner products — from front-end POS scanners to next-generation industrial scanners. Combining best-in-class performance — and outstanding customer productivity — Motorola is the scanner leader. Available for a wide variety of data capture applications, Motorola's Symbol scanners are capable of meeting PCI requirements when used with a PCI-certified payment solution, and when operating within a PCI compliant system, such as an infrastructure designed with the Motorola Services, WLAN products and Enterprise AirDefense solutions.

www.motorola.com/business;
click Bar Code Scanning

Summary

Motorola has over 30 years of experience in providing our customers security solutions and enterprise mobility products that work together to create a flexible PCI solution. We have the team and industry expertise to talk to you about PCI and are here to help you strategize and tackle your security issues.

Motorola currently participates on the PCI Security Standards Council – the administrative body that decides how to implement future iterations of security standards. With this in mind, find out how Motorola can help you on the road to securing credit card data and creating an overall security strategy that will meet PCI Standards today and beyond.

Call us at 1.866.416.8545 or visit www.motorola.com/business

For more information on PCI Security Standards, visit <https://www.pcisecuritystandards.org/>



MOTOROLA

motorola.com

Part number BRO-PCI. Printed in USA 12/09. MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©2009 Motorola, Inc. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.