April 30, 2012

Re: i3 International PCI Compliance

To all of our customers and partners;

i^3 International software applications including PACDM (Point of Sales, ATM, and Card Access Data Management) and CMS (Central Management Software) are fully PCI compliant. PACDM and CMS software applications do not store and/or process information from credit, cash and other types of payment cards including gift and loyalty cards.

Shane Merem, PCI QSA of Magnus Software (Folerville, MI), an independent auditing firm, has confirmed that i3 International's PACDM and CMS software applications do not violate PCI DSS standard. A copy of the auditor's letter is attached to this bulletin.

i3 International Inc. is in compliance with the PCI DSS standards, Requirement 9: Restrict physical access to cardholder data and informs all customers that wish to host their own CMS server about the above PCI DSS standard requirement.

Should you have any questions or concerns regarding the above, contact Bob Hoang at 416.261.2266 Ext. 107 or bob@i3international.com.

Best regards,

B. Hoang

Bob Hoang
Director of Technical and Support services
1.877.877.7241
support@i3international.com

Magnus Software

Shane Merem - PCI QSA

Box 358
Fowlerville, MI
48836

4/27/2012

To:
Bob Hoang
I3 International

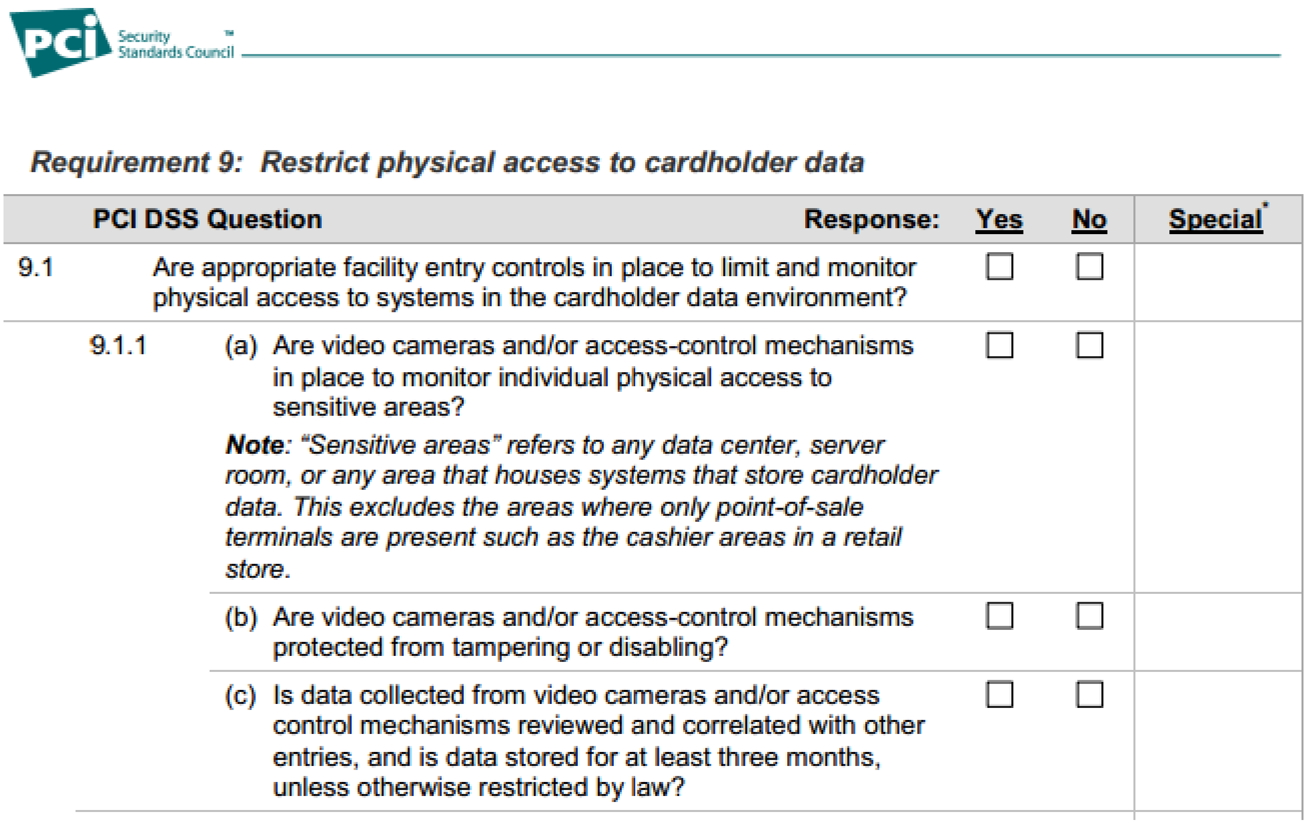
Opinion letter regarding PCI compliance of the I3 VMS Surveillance system.

Bob, after reviewing the VMS products and it's implementation I offer my opinion.

All organizations that transmit, store or process card holder data are subject to the PCI-DSS standard v 2.0.

Further, the use of a video system that correlates video to events in time can provide important evidence that can assist in a security audit. See PCI-DSS question 9.1 listed in the PCI SAQ document below.

I could not find a way, without violating the PCI DSS standard, to exploit your video system to compromise the security of cardholder data.



PCI Security Standards Council™

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question			Response: Yes	No	Special*
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?		□	□	
9.1.1	(a)	Are video cameras and/or access-control mechanisms in place to monitor individual physical access to sensitive areas? ***Note**: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.*	□	□	
	(b)	Are video cameras and/or access-control mechanisms protected from tampering or disabling?	□	□	
	(c)	Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries, and is data stored for at least three months, unless otherwise restricted by law?	□	□	

I have also contacted the PCI Security Council for any additional insight into this matter. It often takes weeks to receive an answer. I will follow up if I receive any useful information.

Please feel free to call me at 800-700-0918 Ext 205 or shane.merem@magnusoft.com with further questions.

Shane Merem - Magnus Software, Inc. - PCI QSA

Shane Merem