



IMPORTANT  
LEGAL NOTICE

APRIL 2, 2007

Dear MICROS Customer:

As you have been notified previously, it is absolutely imperative that you comply with all of the credit card security requirements. Please be advised again that Visa, MasterCard, American Express and Discover (collectively known as the "Association") are exerting great pressure on their member banks to ensure that all merchants accepting their card brands strictly adhere to the Payment Card Industry – Data Security Standard, or "PCI". The PCI mandate defines strict standards for the processing and storage of credit card information to which all **merchants** must adhere in order to continue accepting credit cards and to avoid substantial fines. Over the past two years you have received communications from your bank about PCI and its importance in reducing or eliminating credit card fraud.

As your technology provider, we continue to take this initiative very seriously. When the new Association guidelines were announced, which prohibited the long-accepted and approved practice of storing track data, MICROS implemented changes to all of its PMS/POS applications to prevent the storage of full magnetic stripe data. These enhanced MICROS products have been made available to all MICROS customers since March 2004, subject to standard upgrade charges. Additionally, we are pleased to announce that MICROS has submitted to Visa many of its products to have them certified as compliant with Visa's "Payment Application Best Practices", which are guidelines established by Visa to assist software vendors in creating secure payment applications compatible with Visa "Card Information Security Program", or CISP. Compliancy status of all of our products may be found at [www.micros.com](http://www.micros.com).

One of the highest priority elements of the 12-point PCI security program is to ensure that full credit card track (swipe) and CVV data is not stored in any form after an authorization is completed. This point is extremely important due to the concern that one could create a fraudulent credit card if access to this sensitive data is gained. There are several other steps that merchants will need to address in order to become fully compliant with this standard. Additional information can be found at [www.visa.com](http://www.visa.com).

As you know, the Association now proactively administers fines to member banks that have merchants that are storing full magnetic stripe data. These fines could be imposed at any time, and could be very large. If you are identified as a merchant storing track data at individual sites or corporate offices, there is an increased likelihood that your bank may be fined and will pass the fine to you for non-compliance. The Association is aware that certain predecessor versions of PMS/POS products still in use store track data and they will aggressively pursue the merchants continuing to use those versions.

For those merchants that still have not upgraded to one of the currently available versions of the MICROS PMS/POS software that have been validated as adhering to the Payment Application Best Practices, you are in violation of Association standards, and risk being subject to significant penalties and fines. Again, the fines that are being proposed are not trivial and could have serious financial impact to your business.

**It is imperative that you immediately upgrade your systems to versions that adhere to Visa's Payment Application Best Practices.** We urge you once again to contact your local MICROS office or account manager to determine if you need to upgrade the MICROS software you are utilizing. Neither MICROS nor your service provider is liable for any damages you incur in connection with using non-compliant products.

Best Regards,

MICROS Systems, Inc.