

November 7, 2005

Dear Valued Customer:

Recently, you may have received a security alert message from Visa regarding their Cardholder Information Security Program, (CISP). This message describes a possible security risk involving connection software used to remotely support your MICROS Point of Sale (POS) system. Specifically, the Visa message warns about the use of generic userID's and passwords with the PCAnywhere (PCA) application.

MICROS agrees with the Visa CISP recommendations regarding PCA; *"We highly recommend that organizations using PCAnywhere to manage POS systems implement as many of PCAnywhere's security features and best practices as practicable. We have included a link to Symantec's website on how to secure PCAnywhere (Chapter7)."*

[ftp://ftp.symantec.com/public/english\\_us\\_canada/products/pcanywhere/pcanywhere32/ver10.5/manuals/pca\\_105\\_admin.pdf](ftp://ftp.symantec.com/public/english_us_canada/products/pcanywhere/pcanywhere32/ver10.5/manuals/pca_105_admin.pdf)

There are a few things you will need to check and possibly change to your PCA configuration. First, if PCA is automatically configured to start and run as a service on your Personal Computer (PC), we recommend you reconfigure it to be manually started. Also, if you have a current "default" UserID and password configured, you should change these and only a few trusted members of your staff should have this information. Taking these steps will prevent unauthorized remote access to your system through PCA and ensure that access to your system is under your control. Note: After making these changes, it is critical that certain members of your staff are aware of the procedure for starting PCA and your unique UserID and password. These will be needed by MICROS any time you require support on your MICROS system. Otherwise, we will be unable to access your system remotely. Note: If you lose your UserID and password, this could prolong your down time and necessitate a costly on-site visit to correct. After each support call with MICROS, we recommend you change your UserID and password, and turn off PCA.

We have included, with this document, the steps needed to properly configure PCA.

Although this correspondence refers to PCA, a similar potential security issue applies to all remote connection methods. Appropriate action should be taken to secure user and password information for your system, regardless of the remote connection method deployed.

If you have already taken steps to secure your system against unauthorized remote access, then further action on your part may not be needed.

Please contact your local service office if you have any questions regarding this correspondence.

Sincerely,

MICROS Customer Services