



1112 Railroad St. SE, PO Box 910, Bemidji, MN 56601 – 218.751.4140 – Fax 218.755.6038

IMPORTANT SECURITY NOTICE

September, 2011



Dear Valued Customer:

While NCBP strongly recommends that its customers comply with all of the requirements of the Payment Card Industry Security Standard, (PCI-DSS), we feel that it is especially important to address five particular vulnerabilities.

Insecure Remote Access: Remote access tools, such as PC Anywhere, should not be left always-on and in active listening mode when not in use for legitimate business purposes. This provides the attacker with a method of easy ingress into your network. You should ensure that your remote access application is disabled at all times except when needed for a specific task.

No Firewall or Improperly Configured Firewall: If your network is connected to the internet, a properly configured firewall is absolutely critical. All non-essential incoming and outgoing traffic should be blocked to prevent unauthorized access via the internet. Please refer to the PCI-SSC web site for more details:
https://www.pcisecuritystandards.org/security_standards/

Anti-Virus/Anti-Malware Application: Although in many cases a commercial anti-virus application may be deployed with a new system, many customers fail to renew the annual updates subscription. To be effective, it is imperative that any anti-virus application be deployed in active scanning mode and be maintained with the latest security updates at all times.

Generic User Accounts and Weak Passwords: The use of shared, generic or default user accounts, such as “service, administrator, manager”, etc. should be immediately discontinued. Each person accessing your network should have his/her own unique user name which should not denote their position or privilege level. Also, each user account should have a strong password (consisting of at least 7 characters and 3 different character types i.e. upper and lower case letters, numbers, symbols). User accounts should be promptly disabled or terminated if no longer needed or if inactive for 90 days. Passwords should be changed at least once every 90 days.

Wireless Protected Access (WPA/WPA2): WPA and WPA2 provide network administrators with a high level of assurance that only authorized users can access the network. It is critical that handheld wireless terminals are running WPA or WPA2. Wireless access points that are not WPA or WPA2 are not secured or PCI compliant.

Please contact your NCBP Account Manager if you have any questions.

Sincerely,

North Country Business Products
Ph: 866-819-7403

Offices In:

Appleton, WI – Belle Fourche, SD – Bemidji, MN – Davenport, IA – Des Moines, IA – Duluth, MN - Eau Claire, WI
Fargo, ND, Bismarck, ND - Madison, WI – Minneapolis, MN – Chicago, IL, Peoria, IL – Rochester, MN