

Network Connection

Are you PCI Compliant?

INSIDE THIS ISSUE:

Partial Authorization - Ruby	2
New Ruby Software Released	2
Voice over Internet Protocol	2
Passport Upgrade	3
PCI PED – Visa Mandates	3
About Network Connection	4

As a merchant that accepts credit cards, the PCI standards apply to you. **Compliance to the standards is your responsibility.** The goal of the PCI security standards is to protect cardholder data.

The PCI Data Security Standard (PCI DSS) can be found on the PCI Security Standards Council (PCI SSC) website, which is www.pcisecuritystandards.org. The core of the PCI DSS is a group of six principles and twelve accompanying requirements.



All merchants are required to evaluate whether they are compliant to PCI DSS. The PCI SSC has developed self assessment questionnaires (SAQ) as a tool to assist merchants to evaluate their compliance. There are various versions of the SAQ depending on the type of point of sale device, communication method, and whether cardholder data is stored electronically. The SAQ with instructions on which version to use is available on the PCI SSC website.

As you are evaluating your compliance to the PCI DSS, any security gaps that are uncovered will need to be remedied as soon as possible. Also, during your evaluation, you should inspect your dispensers if you accept pay at the pump. You will need to ensure that no tampering has occurred. Criminals may have inserted skimmers or may have engineered overlay card readers that would allow them access to cardholder data.

In addition, if you process credit cards using an Internet connection, an annual vulnerability scan is required. The PCI SSC has certified companies to complete this scan. The list of Approved Scanning Vendors (ASV) can be found on the PCI SSC website.

If you have questions on the PCI standards or need assistance complying with them, you should contact a PCI SSC Qualified Security Assessor (QSA). A list of the QSA companies is available on the PCI SSC website.

PCI compliance is not a one-time event. It is important that you stay informed, train your employees on requirements, and continually validate your location's compliance to the current requirements.

Additional information on PCI can be found at the following websites:

www.pcisecuritystandards.org

www.askaboutpci.com

www.visa.com/cisp

www.mastercard.com/sdp

Partial Authorization – Ruby Indoor Transactions

An issue has been discovered with the VeriFone Ruby software version LNKPAK 4.01.01 with the handling of certain partial authorization indoor transactions. (Partial Authorization allows merchants to authorize a lesser amount when a cardholder's account does not have sufficient available funds to approve the entire amount.) When a card is swiped inside and the card holder does not have the proper funds to cover the transactions, the Ruby will prompt the cashier with the following message:

```
Insufficient Funds  
Card Balance XX.XX  
Apply to Sale? [Y/N]
```

If the cashier selects "Yes", then the remaining balance on the card is applied to the sale and there is no issue. But, if the cashier selects "No", the software is supposed to void the transaction. The issue is the software is not properly handling the void and the cardholder is incorrectly being charged for the transaction.

The issue has been fixed in LNKPAK 4.01.02 and greater software versions. If you are on LNKPAK 4.01.01, do not select "No" when receiving the above prompt. Always select "Yes". If the card holder does not want the remaining balance applied to the sale then process a return for the amount that was applied to the card.

New Ruby Software Version Released

VeriFone Ruby software version LNKPAK 4.01.02 was released to production in January. The newer version of software has fixed some minor issues that were discovered in the previous version of software, including the issue with partial authorization as described in the article above.

All locations that are new to the Clark credit card network should ensure that the VeriFone authorized service contractor that is setting up the location is installing the newest version of software.

The upgrade is optional and locations that are currently using LNKPAK 4.01.01 are not required by Clark to upgrade their software.

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) is an alternative that many business are looking into to replace their standard phone line. For standard voice calls, this does not present issues. But, when considering VoIP for use with credit card machines, you may create problems with connectivity and also may be out of compliance with PCI depending on the configuration at your location. Many VoIP providers are not able to handle the data transmissions causing transactions to not settle. In addition, most providers are not encrypting the data properly which exposes cardholder data to hackers which is a violation of PCI DSS.

If you are using VoIP at your location, you will need to ensure that your provider is equipped to handle credit card transmissions and is in compliance with PCI DSS. When evaluating compliance with PCI DSS, locations using VoIP are to be considered as processing over an Internet connection and **not** as a dial up location. This means that locations utilizing VoIP are required to have a firewall.

To avoid the connectivity issues inherent with VoIP and to remove the encryption concerns, the POS device can communicate over the Internet using the services provided by Echosat. Echosat will provide a SPG to encrypt the cardholder data and a Cisco firewall. To sign up for Echosat services, go to the website sign up page found at www.echosat.com/clarkbrands.

Passport Upgrade

A software patch was developed by Gilbarco® a few months ago to fix an issue with the acceptance of certain Visa Fleet cards on the Passport point of sale system. This issue, if not fixed, will result in the location being in violation of Visa U.S.A. Operating Regulation 5.2.B, which states “A Merchant that wishes to accept Visa Cards must accept any valid Visa Card in its category of acceptance”.

If your location is running version 6.00, you will need to be on at least the L patch. For version 6.01, the B patch is the minimum needed. To determine which software version and patch your Passport is running, complete the following steps:

1. From the Cashier Workstation – click on the “More” button above the Yellow message bar on the right.
2. Click on the “Stats” button above the Yellow message bar in the center.
3. Passport Version Number is listed. Service Pack/Patch is the letter at the end of the number.

If you have any questions on this patch or need to upgrade, please contact your distributor or Gilbarco. If needed, the patch should be provided to your location at no cost.

PCI PED – Visa Mandates

Visa has mandated that all newly deployed automated fuel dispensers must have a PCI-approved Encrypted PIN pad (EPP) as of January 1, 2009. This means that if you are purchasing dispensers for your location, you will need to ensure that you are complying to this mandate.

Visa has also mandated on July 1, 2010, all POS PIN entry devices must be using triple DES encryption. If you accept PIN debit at the pump, you will need to replace the hardware that controls your encryption at the pump.

Gilbarco® has the FlexPay™ Encrypting PIN Pad (EPP) available factory installed in Encore® S and 300 dispensers, and as a retrofit for the entire Encore® line, the Advantage® and Eclipse® models. For more information, please contact your Gilbarco® distributor.



Gilbarco® FlexPay™ Encrypting PIN Pad (EPP)

As of January 1, 2009, new fuel dispensers must have a PCI-approved Encrypted PIN Pad (EPP).

If you are purchasing new dispensers, ask your supplier if the dispensers meet this requirement.

**Clark Brands, LLC**

1601 Bond Street
Suite 103
Naperville, IL 60563

Phone

(630) 355-8918, ext.15

Fax

(630) 355-8923

E-mail

customerservice@
clarkbrands.com

We are on the Web!

See us at:

www.clarkbrands.com

About Network Connection

The Clark Network Connection newsletter is part of Clark Brands' ongoing effort to add value to your business, and to educate you about regulations and requirements set by PCI and by the credit card associations. The newsletter will also provide you with information on new programs and initiatives that Clark Brands is providing to you, our customers.

Our goal is to not only communicate to our Licensees, credit card customers, and dealers their responsibilities but also to assist them to ensure they have PCI-compliant software and hardware. Clark will also inform you of changes needed due to requirements outside of PCI but mandated by the credit card associations.

If you have questions about information provided in this newsletter, please contact your Licensee or Clark Brands.

For Credit Card, POS, or technical questions, Clark provides two help desk numbers as your first point of contact:

877-851-4430 for VeriFone Ruby, Omni 3750/Vx570, Gilbarco G-SITE, and PetroSmart

800-347-8224 for Wayne Nucleus, Ruby Sapphire, Passport, Smart Echo, and Gas Boy

Clark Brands, LLC

1601 Bond Street
Suite 103
Naperville, IL 60563



*****Important Information – Please Read*****