

POS NEWS UPDATE 2011

more information for people



In 2006, Visa International, MasterCard Worldwide, Discover Financial Services and JCB jointly announced the formation of an independent council designed to manage the ongoing evolution of the Payment Card Industry (PCI) Data Security Standard (DSS). This focuses on improving payment account security throughout the transaction process.

These standards globally govern all merchants and organizations that store, process and/or transmit cardholder data. Compliance with the PCI set of standards is mandatory and is enforced by the major credit card brands that established the council.

The industry was faced with two, time-sensitive mandates in 2010. PCI mandates stated that:

- all POS software must be running PCI-approved and -audited code by July 2010.
- PIN Pads must process using a Triple Data Encryption Standard (TDES) encryption algorithm.

CITGO has worked diligently with our POS-approved vendors in order to meet 2010 POS software PCI requirements. As a result:

- we worked with our issuing banks to secure an extension on the July 2010 date for some POS equipment types due to a lag time in receiving PCI-validated code from POS vendors.
- we were informed that requirements for PCI TDES PIN Pads changed and no fines would be levied until 2012 if Derived Unique Key Per Transaction (DUKPT) Simple Data Encryption Standard (SDES) was being utilized within the PIN Pads.
- we now require inside PIN pads be upgraded to TDES. You are not required to run TDES at the pumps at this time, but this could change based on rules set forth by the card brands and when they begin fining for non-compliance.

CITGO continues to work closely with our partners and with industry organizations to better understand the complexities involved with PCI and what it means to our industry. Our focus is on education. We believe the best way to avoid PCI compromises is to keep data safe and secure, so we have provided you with this brochure, including a list of all POS software and the current state of PCI PA (Payment Application)-DSS for each equipment type. We also have provided you with information on our new e-Learning tool that will help you in understanding PCI and the steps to take to help eliminate overall fraud at your sites.

Table of Contents

CITGO POS PCI-Compliance Chart	1
Non-Compliance Fees	2
CITGO PCI e-Learning Center	2
Important Settlement Information	2
POS Equipment Program Information	3
PIN Pad Information	4
Point of Sale System	4
Broadband Internet Solutions	5
Dial-Up Communication Fee	5
Fraud Updates	5
Important Contact Information	6
Websites that Can Help You Navigate PCI DSS	6

CITGO POS PCI-Compliance Chart

Product	PCI-Compliant	Broadband Support	# of CITGO Locations Using System	Comments
VeriFone				
Ruby	Yes	Yes	4,192	CITGO Version 037/038 (VeriFone Version 5.10) is PCI PA-DSS compliant. All systems should have been upgraded by June 30, 2010. Visa fines for partial authorization began Jan. 1, 2010. *The next mandated software upgrade will require a Sapphire due to internal hardware space constraints.
Ruby/Sapphire	Yes	Yes	350	CITGO Version 038 (VeriFone Version 5.10) is PCI PA-DSS compliant. All systems should have been upgraded by June 30, 2010. Visa fines for partial authorization began Jan. 1, 2010.
Topaz/Sapphire	Yes	Yes	63	CITGO Version 038 (VeriFone Version 5.10) is PCI PA-DSS compliant. All systems should have been upgraded by June 30, 2010. Visa fines for partial authorization began Jan. 1, 2010.
Vx570	Yes	Yes	1,164	A lease program is available through CITGO at \$60/month. Software is upgraded via remote download. It does not currently support outside card readers.
Gilbarco				
G-Site	No	Yes	440	End of Life: Dec. 31, 2010. NOT PCI compliant and never will be.
Passport	Yes	Yes	526	PCI-compliant code 8.03 released August 2010.
GasBoy	No	No	6	End of Life. NOT PCI compliant and CITGO application never will be. *Deadline extended for the use of this software until further notice.
Dresser Wayne				
Nucleus	No	Yes	136	PCI-compliant software is available. *No new systems will be added to the CITGO network without CITGO management approval.
Pinnacle				
Palm	Yes	Yes	99	PCI-compliant software Version 10 was released to production in November 2010.
FISCAL	Yes	Yes	24	Production released in December 2009.

Please contact local vendors for software upgrades and/or new equipment purchases. Software/hardware costs vary based on location and availability. See MarketNet or contact your Marketer for direct buy-options available for VeriFone and Pinnacle equipment.

Non-Compliance Fees

The following POS systems have PCI-compliant software available today and should be updated accordingly:

- VeriFone Ruby
- VeriFone Ruby/Sapphire
- VeriFone Topaz/Sapphire
- VeriFone Vx570
- Radiant
- Retailix
- FISCAL
- Pinnacle Palm
- Gilbarco Passport
- Wayne Nucleus

As of Aug. 1, 2010, any location utilizing VeriFone equipment with non-PCI-compliant software is being assessed an additional \$250/month network access non-compliance fee. This fee will continue until the software is updated to PCI-compliant code.

As of Dec. 1, 2010, any location utilizing a Gilbarco Passport with non-PCI-compliant software is being assessed an additional \$250/month network access non-compliance fee. This fee will continue until the software is updated to PCI-compliant code.

As of Jan. 1, 2011, any location utilizing a Gilbarco G-Site is being assessed an additional \$250/month network access non-compliance fee. This fee will continue until the software/hardware is replaced by a PCI-compliant POS system.

Please note: Effective Dec. 31, 2010, Gilbarco no longer supports the G-Site POS terminal.

To avoid being assessed PCI non-compliance fees, POS systems must be upgraded to the PCI-compliant software version within 90 days of the version being released by the vendor for production.

CITGO PCI e-Learning Center

CITGO, in conjunction with ProPay, has developed the CITGO PCI e-Learning Center. This free, online resource provides a single-source destination to help you with your PCI, information security and fraud prevention training needs.

Three online courses are available through the CITGO PCI e-Learning Center. They have been designed by industry experts with significant training experience. Enrollment and utilization is administered at the Marketer level. Available classes include:

- Basic Security and Fraud
- Intermediate Security Fraud and PCI-DSS
- PCI Compliance Basics

Important Settlement Information

As of Oct. 1, 2008, Credit Batch Reconciliation (CBR) transaction detail re-keys are NOT ALLOWED for any transaction older than 30 days. This requirement is mandated by the issuing card companies. In the past you have been able to send through “dropped” transactions, and CBR could re-key in order to settle the batch transaction amounts. Re-keying transactions older than 30 days is no longer an option and these transactions WILL NOT be processed.

With the introduction of PCI-approved software, your POS equipment is not allowed to store magnetic strip data within the software. Under certain conditions, storage of the credit card number is permitted.

If you have an incident whereby POS communication to the host is lost, be aware that you could lose transactions processed in fallback. If you have a reload or reboot of software for any reason, please go into your system using your protected passwords and copy the transactional information. Once the system is reloaded and the files are cleared, there is no way to retrieve transactions that did not complete processing to the host. If transactions were captured at the host, CITGO can help with resolving settlement issues. However, if transactions did not make it to the host, we cannot retrieve the account number for billing. **If CITGO cannot bill transactions, we cannot pay you for those transactions.**

If you use VeriFone POS equipment (other than the Vx570), the number of transactions processed within a batch is important. To avoid possible issues with settlement, NEVER set a size limit of more than 75 transactions per batch. VeriFone does allow a batch size of 99, and this does work for some of our sites. However, there have been instances in which these batches have caused major issues with settlement. As a reminder, any batch size other than the standard 35 should be cleared with CITGO. CITGO maintains this setting with the parameter download for the VeriFone terminals.

POS Equipment Program Information

Because of PCI requirements and the work required to roll-out new software for each POS vendor, CITGO has limited the use of some previously approved POS systems. Please be aware that no locations using the following POS hardware can be added to the CITGO network without CITGO management approval:

- Wayne Nucleus
- Radiant
- Retailix

Vx 570 Equipment

These units are available through CITGO and are shipped from Heartland Payment Systems. CITGO bills the Marketer for this equipment. All billing inquiries should be directed to the CITGO POS Settlement Desk at 1-800-533-3421, option 2, option 3. To return a Vx570, contact the CITGO Helpdesk to request a box and label. Please note that pick-up service is not provided; packages should be dropped off at the nearest FedEx counter. **The full replacement cost of any non-returned equipment will be charged to the Marketer.**

Roll paper for the Vx570 is provided four times a year at no charge (February, May, August and November). If additional paper is needed, it can be purchased via credit card from:

- Heartland – 1-800-533-3421, option 2, option 2
- GCF – 1-800-805-8492
- Anywhere that roll paper is sold

VeriFone Managed Service Program

Ensuring that retail location POS systems are PCI compliant can be both expensive and time consuming. As an alternative to purchasing, CITGO has partnered with VeriFone to provide a Managed Service Program for CITGO Marketers. For a set monthly fee, this new program provides:

- the use of VeriFone Integrated POS equipment.
- 24/7 VeriFone Helpdesk access.
- on-site technician visits.
- software maintenance.

This option is only available through a Marketer contract agreement.



PIN Pad Information

CITGO no longer provides PIN Pad encryption. Heartland does re-injection of the CITGO TDES key. The charge is \$18 for new equipment. If old equipment needs to be re-injected, there is an additional check and test fee of \$15. Total cost for re-injection of older equipment is \$33.

Please note: Only certain model numbers can be re-injected. If you have questions, please contact a POS product manager. Your local POS provider should also have access to the CITGO TDES key. Make sure you ask for the PCI-compliant TDES CITGO key when requesting CITGO key injection.

Point of Sale System

Certified Service Contractors

Service technicians who physically upgrade your software or hardware are required to be certified by your POS vendor. The technician should have a vendor-assigned certification number. Certification can be validated by contacting the vendor helpdesk. POS vendors can provide a list of certified contractors in your area. Service contractors register POS issues with the vendor by using their certification number. Most vendor helpdesks will not assist a location with issues that may have been caused by an unauthorized service technician. Poorly or incorrectly configured POS systems can cost you money by losing settlement transactions. Please make sure you always use a reputable and certified service contractor.

Helpdesk and Maintenance Contracts

CITGO strongly suggests that each location have a current POS vendor maintenance or helpdesk contract. CITGO currently maintains ONLY the Vx570 terminal. The resolution of software/hardware issues for all other POS types is the responsibility of the location owner and the POS vendor.

VeriFone has a new, mandatory Annual Software Maintenance Program, which went into effect on Aug. 1, 2010. The program applies to the following POS systems:

- Ruby SuperSystem
- Ruby PLUS Sapphire or Topaz XL
- Secure PumpPAY
- VeriFone Smart Fuel Controller

CITGO has arranged with VeriFone to offer this program at a reduced price to our Marketers. If a location does not want to take advantage of the CITGO reduced pricing, then an opt-out form is required to be sent in to CITGO by the Marketer.

We want to make sure that you have a complete understanding of the risk involved with cancelling your enrollment in the service plan. If you are not enrolled in the VeriFone Software Maintenance Program either through VeriFone or through CITGO, then:

- service providers cannot get assistance from VeriFone while working on your POS equipment.
- service providers cannot register any software they install on your VeriFone equipment.
- you will not be able to call the VeriFone Helpdesk for support or report any issues to them.
- CITGO will not be able to report any issues to the VeriFone Helpdesk for you.

Broadband Internet Solutions

We're excited about our new, wireless broadband solution for high-speed, secure transaction processing. The CITGO Wireless Broadband Solution meets all PCI security standards and consists of SPRINT Wireless Internet Service and Heartland's SMARTLink Data Encryption Service. Additional information is available by calling 1-800-423-8434, ext. 4333.



EchoSat SPG is also available for high-speed processing. This service does not bill through CITGO. Contracts and billing are handled directly with EchoSat.

Dial-Up Communication Fee

As of Sept. 1, 2010, an additional one-cent, per-transaction cost is applied to all transactions that process on the network using dial-up technology. Locations using broadband or high-speed processing do not incur the dial-up communication cost, but do incur the additional costs associated with broadband or high-speed processing as outlined in the broadband agreements.

Fraud Updates

The following fraud alert notices were sent out in 2010.

1. Gift Card Fraud

DO NOT accept any gift cards if your stores' POS equipment is offline. Decline sales if:

- individuals are attempting to make multiple transactions on multiple gift cards.
- individuals are using gift cards to purchase large quantities of cigarettes.

If presented with a gift card, please ensure the last four digits of the card match the last four printed on the receipt. If they do not match, reverse the sale and decline further transactions.

2. Beware of Criminals Attempting Fraudulent Purchases Using Credit Cards Reported Lost or Stolen

The criminal provides a card to the clerk who swipes or manually enters the card number and receives a "Declined" or "Call Center" message. The criminal uses their cell phone to place a call – ostensibly to the card issuer, but actually to an accomplice – and gives the phone to the clerk. The accomplice then provides the clerk with an illegitimate authorization code to be used with the transaction. To minimize your risk of fraudulent sales, the clerk should:

- place the call for voice authorization. Never rely upon the cardholder to place the call.
- obtain a valid authorization code.
- review the card security features.
- verify the signature on the receipt matches the signature on the back of the card.
- obtain additional identification.
- obtain an imprint of the card showing the stylized "D" on manually keyed transactions.

ZIP Code Verification Program

A useful tool to combat ICR (island card reader) fraud is the ZIP Code Verification Program. This program requires the cardholder to enter their ZIP code into the keypad at the pump. The card issuer verifies that the ZIP code entered matches the billing address on record for the customer's credit or debit card. If an incorrect ZIP code is entered, the transaction will be denied, and the customer will be referred inside. The ZIP Code Verification program is designed to protect customers and Retailers against fraudulent use. The process is speedy and effective. If you would like to have ZIP Code Verification activated at your location, or if you have further questions regarding this program, please contact Kay Carlisle at kcarlis@CITGO.com or 1-800-423-8434, ext. 4340.

Important Contact Information

For all software/hardware and broadband questions, please contact the CITGO Product Managers:

Jeff Maybray – 1-800-423-8434, ext. 4782

Sherry Thompson – 1-800-423-8434, ext. 5494

Donna Gordon – 1-800-423-8434, ext. 4781

For all software/hardware and broadband production issues, please contact:

CITGO POS Helpdesk – 1-800-533-3421, option 2, option 2

For questions regarding batch settlement or equipment return, please contact:

CITGO Settlement Desk – 1-800-533-3421, option 2, option 3

If you have questions regarding PCI compliance, please contact:

Charlotte Loomiller – 1-800-423-8434, ext. 4718

Rhonda Todd – 1-800-423-8434, ext. 5366

If you have questions regarding fraud inquiries, please contact:

Kay Carlisle – 1-800-423-8434, ext. 4340

Websites that Can Help You Navigate PCI DSS

PCI Security Standards Council

www.pcisecuritystandards.org

Here you will find the compliance standards and can obtain any of the validation documentation.

Visa PCI Mandates

www.visa.com/cisp

This site contains information about Visa's CISP-compliance program for PCI DSS. Check out the Alerts section for news and information about compromises or risks within the industry.

Visa PIN Pad Mandates

www.usa.visa.com/merchants/risk_management/cisp_pin_security.html

This site provides information on Visa's PIN security enforcement program. You will also find deadlines and other information.