

Added Services for Greater Security Protection

VeriFone supports you every step of the way during testing, setup, implementation, and ongoing operations. Our services program includes site surveys, consulting, installation, training, extended warranties and on-site maintenance, documentation, help desk support, and additional support via our Managed Services programs—where we host your payment and estate management systems.

PCI Certified Installation

VeriFone's PCI-Certified Installer program ensures Secure PumpPAY is installed correctly by a VeriFone Authorized Service Contractor (VASC) that is trained and certified in Payment Security Best Practices and secure dispenser card reader device installations.

PCI Assurance Program

Further protect your site with VeriFone's PCI Assurance Program. This turnkey service includes vital components to ensure your site remains compliant

- Managed intrusion detection monitoring
- Managed intrusion protection service
- Wireless network monitoring
- Dispenser alarm monitoring
- Online compliance reporting
- Periodic vulnerability auditing
- Log monitoring and management

Trust VeriFone—The Global Leader in Secure Payments

For over 25 years, VeriFone has been recognized worldwide as the leading provider of secure electronic payment systems. As an involved member of the International Forecourt Standards Forum (IFSF) and the **only payment products company to have been elected to the PCI Security Standards Council's Board of Advisors**—VeriFone's global knowledge of payment security standards and certifications is unmatched. Our solutions continually evolve to incorporate the most stringent security standards and industry best practices worldwide. In short, VeriFone is bringing peace of mind to the point of sale.

Trust VeriFone for all the information you need regarding secure payments.

Retail Payment Security Web site

www.secureretailpayments.com

The one place you can turn to for accurate and helpful information to better understand what is required to fully protect cardholder data from compromise.

VeriFone Retail Payments Security Conference

An annual conference you need to attend to stay up to date on payment security standards and how to ensure the security of your payment process, protect the privacy of your customers, and benefit from new payment technologies, trends, and applications.

VeriFone Payments Security Newsletter

Get the latest information on payment security news, trends, standards updates, events and technologies. Email securepayments@verifone.com to register today.



www.petro-c.verifone.com/securepumpay

© 2008 VeriFone. All rights reserved. VeriFone, the VeriFone logo, Secure PumpPAY, OP 4100, Ruby, Sapphire and Topaz are either trademarks or registered trademarks of VeriFone in the United States and/or other countries. All features and specifications are subject to change without notice. All other trademarks and brand names are the properties of their respective holders.
02/08 45590 Rev B JK



Secure PumpPAY Solutions

Think your pumps are secure? Think again.

"Using a credit card at a gas station could pose more of a risk for data theft than shopping online...petroleum and convenience retailers must react quickly to avert unnecessary exposure to fraud and the mitigation expense they will undoubtedly incur if left unchecked."

—Gartner Inc. analyst



Protect your customers' personal data and your business.

A PCI approved solution for your existing dispenser—available TODAY.

Security of payment systems is paramount, especially where unauthorized pump access is difficult to prevent and more vulnerabilities with existing non-secure systems are emerging every day.

You need to safeguard your customers' magnetic stripe card data and PINs from being illegally captured at your pumps. Every time a pump is opened—even for legitimate reasons such as changing paper rolls or performing routine maintenance—you are at high risk of a security breach and potentially facing extensive fines, negative publicity, damage to your reputation, reduced customer confidence and lost sales.

Secure and seamless retrofit solution for existing dispenser models from:

Secure PumpPAY

- Dresser Wayne
- Gilbarco
- Tokheim

Recent Dispenser Tampering News

- **Bank Account Data Swiped in Gas Station Scam**, The Orange County Register—Devices attached to pay-at-the-pump stations recorded info from hundreds of cards, police say.
- **ID Thefts Target Arco Stations**, Sacbee.com—Credit card information linked to more than 1,000 debit cards swiped at Arco ampm gas stations...was captured by a "skimming" operation used to withdraw at least \$110,000 in cash from ATMs.
- **Devices Stealing Data From Gas Pumps**, Convenience Store News—Thieves installed data-collection devices inside the pumps at several Palm Beach County gas stations...and the machinery copied and stored customers' information, reported the Orlando Sun-Sentinel.
- **Paying with Plastic at Gas Stations Could Cost You**, City News—Sophisticated crooks are waiting until dark to insert software into the credit card slots. A memory chip in the reader and the gel pad records everything, and the crooks simply download what they need.

Current Dispenser Vulnerabilities

- Easy access to card reader devices—many models share common pump keys that allow station employees and technicians to gain access to the interior of the pump
- PINs are not encrypted until they reach the POS (TDES is required at the dispenser)
- Card data transmitted in the clear is most susceptible to a security breach
- No alarms on the door panel to alert management the door has been opened
- The terminals that connect the components (card reader, keypad, display and printer) are clearly marked
- Cameras easily mounted to capture PIN entry
- Many stations are unattended during night hours

Payment Card Industry (PCI) Requirement Dates

- **January 1, 2009**—All new fuel dispensers must have PCI approved PIN entry devices installed
- **July 1, 2010**—All existing fuel dispensers need to support the Triple Data Encryption Standard (TDES) which is required for PCI certification and mandatory in all automated fuel dispensers

FACTS YOU SHOULD KNOW

- There are no secure fuel pumps with PCI compliant card-reading and PIN pad devices working today
- Secure payments at the fuel dispenser require a PCI approved EPP (Electronic PIN pad) keypad, secure MSR (Magnetic Stripe Reader) and the TDES method of data encryption
- Fuel dispenser card-reading devices represent the weakest link (least secure component) in the card payment security chain
- Debit payments at the fuel dispenser are growing 26% annually, increasing the liability of a data breach dramatically each year
- The cost to retrofit an existing dual-sided dispenser is less than 25% of the cost of a new dispenser
- The average security data breach costs a company \$5 million

WHAT ARE THE RISKS FOR NON-COMPLIANCE?

Large Legal Fees
Expensive Financial Institution Fines
Loss of Merchant Services Agreement
Embarrassment
Negative Brand Exposure
Reduced Customer Confidence
Lost Sales



VeriFone's Secure PumpPAY is a PCI approved solution that includes PCI certified keypad, secure MSR, and TDES encryption. It also supports VeriFone's VeriShield DSS, a patent pending technology that cryptographically masks all customer account information at the card reader.

VeriFone's Secure PumpPAY is a powerful solution for petroleum stations, convenience stores and supermarkets that need to upgrade their existing fuel dispensers to support PCI approved secure payments. Backed by a suite of PCI compliant services including managed intrusion detection and protection systems, VeriFone provides a complete end-to-end security solution. Years of leadership in secure payment technology have earned VeriFone the prestigious honor of being selected as the only equipment manufacturing company to be invited to join the PCI DSS Board of Advisors.

Convenient Retrofit Solution for Existing Pumps

Secure PumpPAY is easy to use, easy to integrate into existing pumps and works seamlessly with everything in your fuel station. The PCI approved solution incorporates the use of VeriFone's OP 4100 payment module, which consists of the PCI EPP encrypting PIN pad and the PCI approved secure card reader. Secure PumpPAY packs the latest payment technology into a compact integrated solution designed to easily replace non-PCI compliant systems in a wide range of dispenser models and card reader devices. It also includes Ethernet access to deliver rich graphics and dynamic content to the full-color display.

Secure PumpPAY includes custom retrofit kits for most dispenser models where installation is simple and most sites can be completed in one day. These compact retrofit kits replicate the existing dispenser door panels ensuring a sleek and consistent look across your brand. The Secure PumpPAY solution is completely integrated with your Ruby, Sapphire and Topaz POS systems and is easy to integrate at a mechanical, electrical and software level—no changes to your inside hardware or software are required. Due to its modular design, PCI certified installers simply remove the old dispenser door panel, disconnect a few cables, mount the payment module to the new dispenser door panel, reconnect the cables and seal the unit with the supplied gasket seal kit to meet IP65 requirements.

More Than Just Secure Payments

- ATM-style keypad, screen-addressable keys and a hybrid card reader that accepts EMV chip and magnetic stripe cards
- Built-in contactless reader supports a variety of contactless payment schemes
- Large 5.7 inch color display and LAN network interface provide for a dynamic digital merchandising solution allowing retailers to highlight bright, attention-getting messages to customers while they are filling up their tanks
- Housing is constructed from a rugged and durable polymer that is specialized for use in tough outdoor conditions with exposure to adverse weather and petroleum and diesel splashes
- A fast, high-resolution graphics-enabled thermal receipt printer displays store logo or bar coded receipts and includes a wider paper roll, reducing the number of paper changes
- Display screen is recessed 3.5 inches from its tamper-resistant housing, aiding privacy and ensuring that it is clearly visible even in bright sunlight