Special Issue—March 2008

Distributor Update

A Special Issue Newsletter for Sinclair Oil Corporation Distributors

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS UPDATE

- Some Sinclair distributors have been fined by credit card companies for disclosing cardholder data.
- PCI requires any entity that stores, processes or transmits any credit card data be in compliance with PCI… "Right Now"

> *"PCI requires **any entity** that stores, processes or transmits any credit card data be in compliance with PCI DSS"*
>
> *(source: searchcio)*

It has come to Sinclair's attention that some Sinclair distributors have been fined by credit card companies for violations of Payment Card Industries (PCI) Data Security Standards (DSS).

What is PCI & PCI DSS?

Payment Card Industry (PCI) Data Security Standard (DSS), developed the first-ever industry standard to set guidelines on improving payment account security throughout the transaction process. "The Payment Card Industry Data Security Standard (PCI DSS) applies to every organization that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit credit card/ debit card data." (see footnote—*PCI Compliance Guide 1*)

I don't process many debit cards, do I have to comply?

There is no difference in compliance requirements. "PCI requires **any entity** that stores, processes or transmits any credit card data be in compliance with the PCI DSS" *(footnote— searchcio).*

When do I have to be compliant?

"PCI assumes that each entity is always fully in compliance with PCI. Companies often take that to mean they must be compliant by such and such a date. That is wrong. Companies are assumed to be complaint **right now**" *(see footnote—searchcio)*

What if I'm not PCI compliant?

Non compliance could result in real cost to your business. "The Ponemon Institute has released an update showing the cost has gone up to $197 per account in data compromise." "PCI compliance is a good business decision. Compliance is just cheaper than suffering the financial costs" *(see footnote -Treasury Institute).* "Add to that that Visa can typically fine a merchant around $30 dollars per card lost, and it make sense to take the time." *(see footnote—PCI Compliance Guide II)*

Are petroleum merchants any different?

Certain Automated Fuel Dispenser ("AFD") models share common pump keys (aka "brass keys") that allow service station employees and technicians to gain access to the interior of the pump. This ease-of-entry feature supports legitimate maintenance activity. However, criminals have exploited the use of 'common' brass keys to access the AFD in order to attach devices that capture or 'skim' cardholder information'. *(see footnote: Visa Data Security Alert 11-17-06)*

'Merchants that fail to restrict AFD access to designated employees may be vulnerable to skimming attacks. These attacks occur when criminals and/or 'collusive' employees access the interior of the pump and attach devices that capture PIN and account information'. *(see footnote: Visa Data Security Alert 11-17-06)*

What should I do?

Protect equipment & information: "Visa has received an increasing number of reports regarding point-of-sale (POS) Pin Entry Devices (PED) thefts from merchant store locations. Typically occurring late at night, evidence indicates POS PEDs are being physically removed from their locations and are being replaced with modified devices designed to skim account and PIN data. Suspects in most cases were able to remove and install POS PED in under one minute." *(see footnote: Visa Data Security Alert 11-19-07)*

Typical skimming devices installed inside fuel dispensers

(see footnote: PIN Security & AFDs)

What should I do? (continued)

"Merchants are reminded that storage of full magnetic stripe data post authorization is prohibited by Visa Operating Regulations. Further, retention of full magnetic stripe data can significantly increase a merchants' risk of compromise, as hackers are now aware that certain payment applications store track data by default, and merchants may not be aware of it. Merchants can reduce their risk of compromise by ensuring they are fully compliant with the Payment Card Industry Data Security Standard ("PCI DSS") and by ensuring any payment card data is securely stored in a PCI compliant manner." *(see footnote: Visa Data Security Alert 11-17-06)*

"Purchase only PCI approved PEDs that have been lab evaluated." "Visa/Interlink merchants must deploy PEDs listed on the Visa PIN-entry Device Approval List found at http://partnernetwork.visa.com/dv/pin/pedapprovallist.jsp

"Merchants should train employees about the potential of PIN compromise when POS PEDs are stolen or missing. Merchants should immediately contact the merchant bank and law enforcement if they suspect tampering of any POS PED." *(see footnote: Visa Data Security Alert 11-19-07)*

"Ask your POS vendor to confirm your software version does not store prohibited magnetic strip data"
*(see footnote:
Data Security Brief 11-09-07)*

"Merchants are encouraged to work with their merchant bank and/or Encryption and Support Organization (ESO) to create a plan that ensures ***all*** deployed POS PEDs are Visa-approved, lab evaluated and comply with the *Triple Data Encryption Standards (TDES)* by July 2010". *(see footnote: Visa Data Security Alert 11-19-07)*

Sinclair anticipates that distributors will investigate PCI requirements now to insure they are compliant and as they make purchase decisions in order to avoid purchasing non-compliant products and avoid capital and security losses.

PCI specifies that "all transactions originating at attended ***and*** **unattended POS PEDs** must be encrypting PINs from the point of transaction to the issuer (end-to-end)" by 7/1/2010. *(see footnote: PIN Security & AFDs)*

"Ensure that all POS devices are tamper proof". *(see footnote-Visa Fraud alert 11-13-07)*

"Visa has reported that POS devices are being re-sold while containing prohibited stored data. Visa reminds merchants to use proper procedures to prevent the storage of prohibited cardholder data. Prohibited data includes unencrypted account number, magnet strip "track data" Card Verification and PIN blocks. PCI PIN Security requirements state that all PIN Entry Devices (PEDs) and Hardware Security Modules (HSM) must have all cryptography keys and any other sensitive data securely removed prior to being decommissioned. *(see footnote: Data Security Brief 11-09-07)*

"Entities must ensure that no prohibited data is stored on any POS hardware that is in service or has been removed from service" *(footnote: Data Security Brief 11-09-07)*

"Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on portable media, printed out, or left on someone's desk. Consider procedures and processes for protecting cardholder data on media distributed to internal or external users. Without such procedures data can be lost or stolen and used for fraudulent purposes. Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. Cardholder data leaving secure areas can lead to lost or stolen data. If steps are not taken to destroy information contained on PC hard disks and CDs, and on paper, disposal of such information may result in compromise and lead to financial or reputation loss. For example, hackers may use a technique known as "dumpster diving," where they search through trashcans and recycle bins, and use found information to launch an attack". *(see footnote: Navigating PCI)*

How can I find out if I'm PCI Compliant & where do I begin? You may find the Self Assessment Questionnaire helpful. (see footnote: *PCI Self Assessment Questionnaire). A place to begin may be "5 Guidelines to Gaining PCI Compliance" (see footnotes)*

Note: This document is not intended to answer all questions regarding PCI compliance. Sinclair presents this synopsis and references with the intent of providing information on the important subject of PCI compliance for Sinclair distributors. The following are some resources that may be useful in becoming and remaining PCI compliant and protecting your business interests. *(see Page 3, "Selected Reference Resources" for source references)*

PAYMENT CARD INDUSTRY - SELECTED REFERENCE RESOURCES

Footnotes:

- *PCI Compliance Guide 1:* http://www.pcicomplianceguide.org/step2a.html
- *Searchcio:* http://www.searchcio.com.au/tips/tip.asp?DocID=6100745&SiteID=19
- *Treasury Institute:* http://www.treasuryinstitute.org/resourcelibrary/5Strategies.pdf
- *PCI Compliance Guide II:* http://www.pcicomplianceguide.org/posdss/pos-pcicompliance.html
- *Visa Data Security Alert 11-17-06:* http://usa.visa.com/download/merchants/20071117_datasecurityalert_petroleum.pdf?it=c|/merchants/risk_management/cisp_alerts.html|Risks%20Affecting%20Petroleum%20Merchants%20-%20November%2017%2C%202006
- *Visa Data Security Alert 11-19-07:* http://usa.visa.com/download/merchants/20071119_datasecurityalert_pospinentry.pdf
- *PIN Security & AFDs:* http://usa.visa.com/download/merchants/pin_security_and_automated_fuel_dispensers.pdf
- *Visa Fraud alert 11-13-07:* http://usa.visa.com/download/merchants/20071113_datasecurityalert_fraud_alert.pdf
- *Data Security Brief 11-09-07:* http://usa.visa.com/download/merchants/20071109_datasecurityalert_eliminatestorage.pdf
- *Navigating PCI:* https://www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-1.pdf
- *PCI Self Assessment Questionnaire:* http://www.pcicomplianceguide.org/step5.html
- *"5 Guidelines to Gaining PCI Compliance":* http://www.pcicomplianceguide.org/aboutpcicompliance.html

Other Resources:

- http://usa.visa.com/download/merchants/payment_application_security_mandates.pdf
- *Power Point presentation on Automated Fuel Dispensers and Pin Security:* http://usa.visa.com/download/merchants/pin_security_and_automated_fuel_dispensers.pdf?
- *PCI Standards Council Approved PIN Entry Devices* https://www.pcisecuritystandards.org/pin/
- *Self Assessment Questionnaire:* *https://www.pcisecuritystandards.org/tech/saq.htm*
- *Approved PIN Entry Devices (PEDs):* *http://usa.visa.com/merchants/risk_management/cisp_pin_security.html?*
- *PCI Audit Procedures:* https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf

> *"The cause of such problems, however, is less important than the reality that your institution is vulnerable. The only uncertainty is how much the inevitable breach will cost when it happens. Direct financial costs can mount when you must notify individuals that their data have been compromised, pay for credit monitoring, and repair faulty systems and procedures. For breaches related to payment card information, potentially significant liability—and even fines—may be involved. It's not unusual for these overall direct costs to total $1 million for even a relatively small breach."*

Source: http://www.treasuryinstitute.org/resourcelibrary/BOM_DataSecurity.pdf

Sinclair Oil Corporation
550 E. South Temple
Salt Lake City, Utah 84102

Editor—Greg Iverson
giverson@sinclairoil.com
801-524-2957

Posted on the web at:
www.sinclairoil.com, click on the
Distributor Services link