



The Payment Card Industry (PCI) Data Security Standards were established by major payment card industry providers such as Visa, MasterCard, American Express, Discover and JCB as a guideline for companies to protect sensitive cardholder data from fraudulent activities and attack.

Each payment card industry provider may have their own specific management program and guidelines for protecting sensitive cardholder data (ex., Visa CISP) but the PCI Security Standards Council currently owns, maintains and distributes the official PCI Security Standards and all supporting documents. The PCI Security Standards Council's web site (www.pcisecuritystandards.org) includes many helpful materials including; the official PCI Data Security Standards, supplements to the standards, security assessment procedures, FAQs and a glossary of abbreviations and acronyms.

As CSFi's u/SWITCHWARE[®] Enterprise Transaction Processing and Management System stores sensitive cardholder data on its system, this document describes some of the protective measures available to u/SWITCHWARE[®] users. As the scope of the PCI Security Standards are broad in nature and include security recommendations for database access, user audit trails and network protection, this document also provides references to some third party companies who provide solutions that will be transparent to the u/SWITCHWARE[®] application. These solutions range from restricting access to the database and providing audit trails to the encryption of the data stored in the database.

PCI Data Security Standard

Principles and Requirements

The PCI Data Security Standard consists of 12 requirements organized into 6 different groups. In the following topics, you can click on blue links for more information.

- **Build and Maintain a Secure Network**
- **Protect Cardholder Data**
- **Maintain a Vulnerability Management Program**
- **Implement Strong Access Control Measures**
- **Regularly Monitor and Test Networks**
- **Maintain an Information Security Policy**

Build and Maintain a Secure Network

- Requirement 1:** Install and maintain a firewall configuration to protect data
- Network Segmentation
 - Identify servers that store / use cardholder data (Test/QA/Development/Production)
 - Segment Cardholder servers from Non-Cardholder servers
 - Routers behind Firewalls
 - Databases containing cardholder data must be located on internal network
- Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3:** Protect stored data
- Keep Cardholder data to a minimum
 - Evaluate each server to determine of storage of cardholder data is necessary
 - Look at encrypting servers which store cardholder data
 - Backup media encryption

u/SWITCHWARE® has triggers to remove cardholder sensitive data from transactions.

Following are the different trigger options and the scripts to create the triggers:

NOTE: When running the Informix scripts, Informix must have exclusive access to the `log_record` and `pos_recon` tables. For that reason, before running the scripts, u/SWITCHWARE must be brought down and all System Monitor clients that are using Query Builder must be closed.

- **To Completely eliminate track1, track2, Cardholder Expiry Date and PIN fields** in the `log_record` table:

`infx_null_track2` (Informix Users)

`orcl_null_track2` (Oracle Users)

NOTE: PIN field will be set to all 1's if the original value was greater than 0. The new PIN field and expiration date will be set to zeros

- **To Eliminate the data on track2 after the expiration date** (discretionary data, start at +4 after the =) in the `log_record` table

`infx_truncate_track2` (Informix Users)

`orcl_truncate_track2` (Oracle Users)

NOTE: PIN field will be set to all 1's if the original value was greater than 0. The new PIN field and expiration date will be set to zeros

- **Eliminate the data on track2 after the service charge code** (discretionary data, start at +7 after the =) in the `log_record` table

`infx_truncate_track2_aftersvc` (Informix Users)

`orcl_truncate_track2_aftersvc` (Oracle Users)

Example: Track 2 will end up as:

1234567890123456=YYMMSCV

Where: **YYMM** is the Expiration Date and **scv** is the Service Charge Code

NOTE: PIN field will be set to all 1's if the original value was greater than 0. The new PIN field and expiration date will be set to zeros

- **Eliminate the data on track2 after the service charge code** in the `pos_recon` table

`infx_truncate_pos_recon` (Informix Users)

`orcl_truncate_pos_recon` (Oracle Users)

All scripts are available on CSFi's ftp server in the following folders:

`/Customers/_Common/PCI_scripts` folder

`/Distributors/_Common/PCI_scripts` folder

Additional information is also available in CSFi's web support **FAQ** area. Simply select '**All**' in the topics field, enter '**track2**' in the keyword search field and click on the '**GO**' button. A line item entitled '**How to comply with Visa and MasterCard requirement that track2 not be stored**'.

u/SWITCHWARE® client applications (3.11.2.5) have been modified to mask cardholder sensitive data.

○ **Encrypting Data**

Informix users – With Informix 11, IBM offers ‘Database Encryption Expert’ to help organizations comply with regulations and legislative acts and ensure that private and confidential data is strongly protected.

Data encryption capabilities:

- Protects sensitive Informix Dynamic Server (IDS) data without requiring changes to the database schema or database applications (i.e. u/SWITCHWARE®)
- Provides a method for creating a centralized encryption and key management policy
- Minimal performance impact particularly when compared to alternative encryption techniques
- Protects database table containers and any other sensitive IDS files
- Provides access control to IDS files by user and application

Note: Contact IBM for the correct version of IDS to support Database Encryption Expert.

Oracle users – With Oracle 11g, Oracle supports ‘Transparent Data Encryption’ that can be utilized to encrypt entire tables, indexes, and other data storage. Oracle 11g uses authentication, authorization, and auditing mechanisms to secure data in the database, but not in the operating system data files where data is stored. To prevent unauthorized decryption, transparent data encryption stores the encryption keys in a security module external to the database.

Data encryption capabilities:

- Applications such as u/SWITCHWARE® do not need to be modified to handle encrypted data. Data encryption/decryption is managed by the database.
- You do not need to create triggers or views to decrypt data. Data from tables is transparently decrypted for the database user.
- Database users need not be aware of the fact that the data they are accessing is stored in encrypted form. Data is transparently decrypted for the database users and does not require any action on their part.
- You can use Enterprise Manager to manage transparent data encryption.

Note: Contact Oracle for the correct version of Oracle to support Transparent Data Encryption.

- Requirement 4:** Encrypt transmission of cardholder data and sensitive information across public networks
- Secure cardholder data during transmissions
 - Do not send Cardholder sensitive data through email unencrypted.

Maintain a Vulnerability Management Program

- Requirement 5:** Use and regularly update anti-virus software
- Ensure anti-virus software remains up to date

- Requirement 6:** Develop and maintain secure systems and applications
- Install relevant security patches for all servers, PC's and terminals are kept up to date.

Implement Strong Access Control Measures

- Requirement 7:** Restrict access to data by business need-to-know
- Limit SQL access

- Requirement 8:** Assign a unique ID to each person with computer access

- Requirement 9:** Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10:** Track and monitor all access to network resources and cardholder data

- Requirement 11:** Regularly test security systems and processes.

Maintain an Information Security Policy

- Requirement 12:** Maintain a policy that addresses information security

Links of Interest:

PCI Data Security Standards

<https://www.pcisecuritystandards.org/index.htm>

Visa Cardholder Information Security Program (CISP)

http://usa.visa.com/merchants/risk_management/cisp_overview.html?it=c/merchants/risk_management/cisp.html|CISP%20Basics

Vormetric (Disk Encryption)

<http://www.vormetric.com/index.html>

Guardium (Database Activity Monitoring, Security and Auditing)

<http://www.guardium.com>

IBM Database Encryption Expert

<http://www-01.ibm.com/software/data/db2imstools/database-encryption-expert/index.html>

Oracle Transparent Data Encryption

<http://www.oracle.com/database/advanced-security.html>