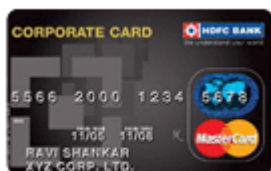


## Case Study: Corporate Credit Cards

Corporate Credit Card has been introduced within a number of organisations as an alternative for purchasing and payment rather than petty cash or personal accounts. They are typically being used for high volume but low value transactions and to assist staff members who travel on behalf of the company. In doing so, the internal finance department is responsible to ensure its corporate credit cards system expenditure is legitimate. Often they will receive statements for Credit Cards that are distributed to cardholders to verify claimable travel expenses and purchase of minor goods or services. These statements contain the actual Credit Card Payment Account Number (PAN) which means that organisation is now required to become PCI DSS Compliant.



Each month, the Finance Officer receives the monthly statements for Corporate Credit Cards. These statement files are often distributed to each cardholder so that they can reconcile the expenditure on the statement. These statements can contain the full Credit Card number within the report files, which exposes that organisation to PCI DSS Compliance. Organisations using corporate credit cards need to ensure Credit Card details are masked so that internal IT systems are not unintentionally brought into scope for PCI DSS.

### Background: About PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is an international data security standard that applies to any organisation that stores, processes or transmits Credit Card data. The purpose of the PCI DSS is to provide guidelines for organisations on the implementation of security controls, so as to protect cardholder data residing in IT Systems. By implementing PCI DSS recommendations, an organisation is able to demonstrate sound business practice and good corporate citizenship, both to its customers and compliance regulators.

The PCI DSS Standard states under Requirement 3 that any stored cardholder data must be protected. Specifically, the DPM solution can address the following requirements

- **Requirement 3.3: Mask Credit Card PAN when displayed**  
The DPM solution provides a suite of options for data masking within Databases Servers, File Repositories and Applications. Masking rules can be static or dynamically configured for on-the-fly masking.
- **Requirement 3.4: Render Credit Card PAN unreadable anywhere it is stored**  
The DPM solution allows data masking of Credit Card numbers so that the full PAN is no longer stored. Additionally, the DPM solution provides plug-in options for encryption and/or tokenisation whereby the original number is still required.

*securing your business*

## The Randtronics DPM Solution

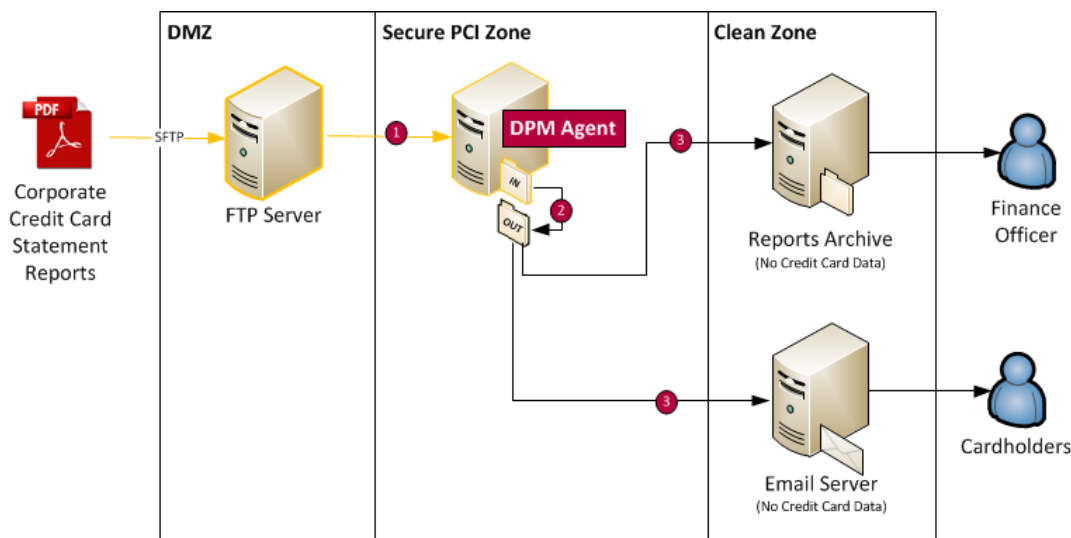
The DPM data masking solution was required to ensure any statement files being transferred by financial institutions or acquiring banks are scanned and masked for proper handling of Corporate Credit Cards internally. The DPM solution allows files to be scanned and masked to ensure other IT system that were required to have access to the files, were no longer part of the PCI DSS Scope.

Once a Credit Card PAN number has been masked, it is no longer considered to be in-scope for compliance. The DPM solution allows data to be masked, with the first 6 digits and last 4 digits remaining on the original statement. Organisations that currently store the full Credit Card PAN number, but do not have a business requirement for doing so should ensure that the data is masked and removed.

Credit Card data can be identified by a combination of two methods.

1. Regular expressions that represent the Credit Card formats of VISA, MasterCard and American Express. These regular expressions have been provided by the PCI DSS Council for identifying Credit Card numbers.
2. LUHN algorithm that verifies any identified Credit Card number to ensure that it passes the checksum.

### Customer ABC Environment



Steps for removing Credit Card data within Reports, Statements and any Files

1. Files are received from various acquiring banks and are transferred to a host running the DPM Agent software.
2. The DPM Agent software scans incoming reconciliation report files for Credit Card data. Any data identified is immediately masked within the file, thereby removing it from scope of PCI DSS.
3. The resulting files are considered to be sanitised and can be move to any internal systems without being in-scope for PCI DSS. They can be archived into file servers and emailed to internal staff (cardholders) for review without concerns for PCI DSS Compliance.

*securing your business*



Data masking is a simple and easy way of removing or reducing the burden of PCI DSS for organisations looking to demonstrate compliance. The DPM solution provides data masking capabilities for the enterprise that can be applied for incoming statements and report files that contain Credit Card information.

In fact, as part of the 'Prioritised Approach to Pursue PCI DSS Compliance' and recommended by the PCI DSS Council, the first milestone to be addressed is to limit data retention. Randtronics DPM data masking approach allows organisations to reduce the overall instances where Credit Card data is being stored and to remove it where there is no business requirement for storage.

For further information on the Randtronics DPM solution, please feel free to contact us or visit our website [www.randtronics.com](http://www.randtronics.com)

*securing your business*