EFTPlus PCI Compliance Summary

EFTPlus is PCI Compliant

EFTPlus does not process cardholder transactions for payment. Full cardholder information is not required to be stored or transmitted in any form to provide the EFTPlus service.

What does EFTPlus store?

To identify member transactions EFTPlus stores the mask number (the first six and last four digits) and a unique token representing the member's card(s) only. Each token is a random, unique & irreversible and unrelated to the card number or other card details.

EFTPlus may also inadvertently store the cardholder's name separately from the card record where the member has chosen to provide their name as part of their membership records and this happens to match the name on their card.

EFTPlus does not store or transmit:

- Primary Account Number
- Service Code
- Full Magentics Stripe Data
- CAV2 / CVC2 / CVV2/ CID
- PIN / PIN Block

EFTPlus complies with PCI DSS requirements

EFTPlus does not store, process or transmit the cardholder data elements that are specified as requiring protection under PCI DSS. However, PCI DSS provides a rigorous set of guidelines that provides a strong basis for best practice handling of member information. For this reason, and for the absence of doubt, EFTPlus complies with the twelve PCI DSS requirements where appropriate. This document details how EFTPlus meets the PCI DSS requirements and provides specific technical information regarding what is stored and transmitted and how it is stored and transmitted.

PCI PTS (PIN Transaction Security) Compliance

EFTPlus does not request, store or transmit cardholder PIN transaction data and the PCI PTS objectives do not apply to the service.

PCI DSS (Data Security Standard) Compliance

Requirement 1: Install and maintain a firewall and router configuration to protect cardholder data

EFTPlus Production and Staging servers are hosted on the Amazon AWS infrastructure which has Level 1 PCI compliance and ISO 27001 certification for infrastructure, data centers, and services.

EFTPlus development machines use dummy or obfuscated member data and are behind firewalls and routers that are set up to 'deny by default' all traffic, including from untrusted sources.

No employee machines can be directly connected to the network that hosts the EFTPlus servers, which stores member information.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Passwords on supplied software or hardware are required to be changed prior to implementation.

Different EFTPlus service functions are physically or virtually separated onto different machines or virtual systems. Each system has only those scripts; drivers and features required to delivery its functionality.

Console and non-console administrative access is fully encrypted using SSL or better.

Requirement 3: Protect stored cardholder data

Cardholder data storage is limited to the mask number (first six and last four digits) of the card number and card token.

Storage is limited to the lifetime of the member and these details can be completely deleted by the member at any time.

The full PAN number can never be displayed to any user because it is not stored.

Cardholder data, except for member name and mask number, is not made available to EFTPlus merchants or any other EFTPlus users.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Member's using EFTPlus do not enter any card holder data into the EFTPlus website. When entering card holder data they are transferred to our PCI compliant partner.

Requirement 5: Use and regularly update anti-virus software or programs

EFTPlus servers are physically separate and on a separate network from all employee machines.

Anti-virus software is required on servers and employee machines and is required to be kept up to date.

Requirement 6: Develop and maintain secure systems and applications

All server and employee operating systems and software are required to be kept up to date with the latest security releases. Updates are applied automatically or are checked automatically and applied within a maximum of one month after release.

EFTPlus software developers are required to know, understand and keep up to date on known exploitations such as SQL code injection and cross site scripting attacks and must develop code with the expectation that the EFTPlus service will be subject to these attacks and should be able to withstand them.

Along with web application firewalls, EFTPlus uses further protection systems, such as CloudFlare, to help identify and protect against future attacks.

Automated testing is applied to all new EFTPlus code prior to release. Automated testing includes testing against vulnerabilities to known attack mechanisms.

Requirement 7: Restrict access to cardholder data by business need-to-know

Cardholder data is restricted to mask number and token.

The mask number is only made available to the original member entering the number, merchants and EFTPlus administrators. Merchants do not have access to the token or any other cardholder data of their members.

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

All users of the EFTPlus service (apart from non-members visiting the EFTPlus public site) must login with an email address or username.

After first-time use all passwords are stored as a cryptographic hash that cannot be decrypted to the original password.

Non-consumer accounts have increased access requirements including minimum use, restricted login attempts, stronger password specification and re-use and idle-time timeout.

Requirement 9: Restrict physical access to cardholder data

No EFTPlus employees (including administrators), merchants or members have physical access to the EFTPlus servers which are hosted on Amazon AWS which has Level 1 PCI compliance and ISO 27001 certification for infrastructure, data centers, and services.

Backups are stored at a separate physical location but still within the AWS infrastructure.

Paper copies of member or transaction data are not made or kept.

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

EFTPlus does not store, process or transmit the cardholder data elements that are specified as requiring protection under the PCI DSS. Cardholder data specific logs are not recorded.

Requirement 11: Regularly test security systems and processes

Amazon complete regular testing of their security systems as part of their Level 1 PCI compliance and ISO 27001 certification.

EFTPlus maintains a LEAN continuous deployment methodology. Application security systems are regularly tested through automated testing prior to deployment. Tests are kept up to date as details of new exploits and vulnerabilities become available.

Requirement 12: Maintain a policy that addresses information security for employees and contractors

EFTPlus has a security policy available to employees, contractors, merchants and resellers.

This compliance declaration, the EFTPlus privacy policy, and Terms of Use form part of the security policy.

The security policy defines proper use of member data by employees, contractors, merchants and resellers according to their level of access.

The systems architect has overall responsibility for the security policy and it's implementation.

Requirement A.1: Shared hosting providers must protect the cardholder data environment

EFTPlus merchants have no access to mask number or other cardholder data (except name) of their own members, and no access to any member data of other merchants.