# Terminal Risk Management

## Important information you need to know.

As a valued customer on the Paymark network, we wanted to make sure you have all the information you need relating to your EFTPOS terminal. This communication covers Electronic Offline Vouchers (EOV), terminal security and fallback (when a chip card is not working as it should). Please take the time to read the following information, and share it with your staff. You can also find extra information on these topics on the Paymark website **www.paymark.co.nz**

### Electronic Offline Vouchers (EOV)

**What is EOV?**
EOV comes into effect when connection with the Paymark network has been lost (such as a telecommunications issue). When an EFTPOS terminal is in EOV mode transactions are stored in the terminal memory and are processed once connection to the Paymark network has been restored.

**How do I know the terminal has switched to EOV mode?**
The terminal will display the message *EFTPOS OFFLINE* and will ask *PROCESS TRANSACTION OFFLINE Y/N?* to which you will need to make a selection. Each receipt will have *AUTH xxxx* printed on it (below the card type).

**What do I need to do?**
Transactions will process as normal (i.e. you swipe or insert the card and proceed normally), however you will need to check the card type to ensure it is a valid type that you would normally accept. You must also ensure that the card has not expired, and have the cardholder sign the receipt as they will not be able to enter their PIN - even for EFTPOS transactions.

**Important stuff I need to remember**
- First check the terminal's cables and phone line to ensure they have not caused the loss of connection with the Paymark network.
- Try a manual logon.
- Transactions over $300 cannot be processed in EOV mode. Contact the Authorisation Centre and process these transactions on a manual voucher.
- Refunds and cash out transactions cannot be processed in EOV mode.
- EOV transactions must be uploaded once connection to the Paymark network has been restored, do not leave them stored in your terminal's memory. Do not make any changes to your terminal until the stored transactions have been uploaded - if the terminal ceases to operate or the software is replaced before the upload process is completed, you are at risk of losing your stored transactions.

For more information please visit **www.paymark.co.nz/eov**

### Terminal Security

It is vital that you do everything in your power to secure your customers' payments and protect their personal information, thus reducing the likelihood of credit and debit card fraud. We've come up with some best practice examples which we strongly suggest you consider:

- Always ensure that your terminals are secure and under supervision during operating hours. This includes any spare or replacement terminals you may have.
- Ensure that only authorised employees have access to your terminals and that they are fully trained on their use.
- Never allow your terminal to be maintained, swapped or removed without advance notice from your terminal provider. Be aware of unannounced service visits, check their credentials.
- Inspect your terminals on a regular basis - check there are no additional cables running from your terminals and that the casing has not been tampered with.

For a complete list of best practices, go to **www.paymark.co.nz/fraudprotection**

### Fallback - Chip card not working

Cards with chips embedded in them should always be processed by "dipping" (inserting) the card into the terminal.

There are however, occasions where the chip cannot be correctly read by the terminal, resulting in the terminal prompting for the card to be swiped. This is known as a fallback transaction and may be a caused by a faulty chip card or a faulty terminal.

The chip card must only be swiped if the transaction is unable to be processed via the chip. Merchants who force a transaction into fallback increase the risk of fraudulent activity.