Consumer Rights
If you are not satisfied with this product or service, you have the right to raise a verbal or written complaint to BSP.

We endeavour to resolve your complaint within but not more than 30 working days.

320 1212 / 7030 1212 - 24/7

servicebsp@bsp.com.pg

www.bsp.com.pg

Visit your nearest BSP branch

BSP Financial Group Limited 1-4815

1022

BSP

EFTPoS Security

Secure your BSP EFTPoS terminal

BSP

Merchant Alert

EFTPOS Skimming

EFTPoS terminal tampering also known as 'skimming', and occurs when someone illegally copies a cardholder's card details to a counterfeit card. If your terminal is not secure, a fraudster could replace your terminal with a tampered device that looks and works like your normal terminal. They could then use the tampered device to steal or copy bank card details to create fake cards and withdraw money from the customer's account.

EFTPoS skimming is difficult to detect and is usually not identified until we find irregular transactions on the cardholder's account.

EFTPoS terminals have many security features which help protect your customers' debit and credit card details. Implementing the below can further protect your business, your reputation and customers against misuse of your terminals and fraud.

You should:

- Conduct awareness with you staff on card skimming, especially those staff who handle card transactions
- Report to us any suspicious device attached to your BSP EFTPoS terminal(s)
- Never leave your BSP EFTPoS terminal(s) unattended to during business hours
- Perform end-of-day checks to ensure your account for all your BSP terminal(s)
- Report to us immediately if your BSP EFTPoS terminal(s) is missing or has malfunctioned
- Report to us immediately if there is any unusual device attached to your BSP EFTPoS terminal(s)
- Keep your BSP EFTPoS terminal(s) in a secure location after business hours
- Insist that any bank representative attending to your BSP EFTPoS terminal (s) produce their work ID card

Educate staff to look out for the following irregularities, suspicious behaviours or attachments to a device;

Suspicious

Distance

Safe

Distance

When a card is inserted, it slides further into the device than it normally should. The card should only slide in to read the chip.

We accept

Staff should be aware of the images of cards, pay attention to see if customer is using a card that is blank or unmarked (i.e. blank) or out of the ordinary e.g. a loyalty card or VIP card that is not on card accepted here displays.

Staff should pay attention to abnormal customer behavior
- Handling multiple cards
- Inputting PIN multiple times

If you believe your terminal, or any other equipment associated with your facility is stolen or tampered with, call us immediately on 3201212/70301212 or
email: servicebsp@bsp.com.pg