Huge Connect
267 West Avenue
Centurion, 0157
PO Box 11691
Zwartkop, 0051
Tel: (087) 820 0220
Fax: (012) 663-5184
www.hugeconnect.co.za

PCI-DSS Security

Huge Connect's Directive pertaining to any correspondence containing Primary Account Numbers (PANs)

Introduction

As a PCI-DSS compliant company, Huge Connect is not permitted to access or view any credit or debit card information and any correspondance recieved to this effect will be deleted immediately. Such correspondence will be replied to informing the sender of the possible dangers associated with sending such correspondence as stated below.

1.1 PANs in Correspondance

- According to the PCI DSS (Payment Card Industry Data Security Standard), e-Mail, instant messaging, SMS, and chat can be easily intercepted by "packet-sniffing" software or hardware during delivery across internal and public networks. Packet sniffing is a tactic similar to wiretapping a phone network and can be used by hackers to capture your Internet traffic and card data.

- Even if your email server is configured to provide strong encryption when you connect to read your email, you have no guarantee that the receiving end has the same level of encryption. One must never utilize these messaging platforms to send PANs when utilising these messaging platforms for any means of correspondence.

- Information must not be captured, transmitted, or stored via end-user messaging platforms (such as email, SMS etc.). Please take note that messaging platforms are insecure and leave trails of unencrypted credit card data in inboxes, trash bins, web browser caches, etc. and as such must never be used to transmit and PANs in the open.

[End of Document]