

how can we help you?



protect cardholder information in your business.



Payment Card Industry Data Security Standards (PCI – DSS)

PCI DSS is a global industry standard focused on the protection of cardholder information and is applicable to any entity which stores, processes and transmits card data.

Merchant Responsibilities:



- Train your staff on security and the protection of cardholder data



Processes followed when storing, processing and transmitting cardholder data:

- Identify and record your processes when dealing with cardholder data
- Analyse your processes for vulnerabilities
- Take immediate action to correct any vulnerabilities
- Compile and submit the required reports as and when requested



Reporting Required:

Please refer to the Reports table on the last page for reporting requirements



Merchant Responsibilities

Guidelines for storing of cardholder data

Some DO's and DON'T's

Reporting Required

Contact Us



Guidelines for storing of cardholder data:

		Data Elements	Storage Permitted
ACCOUNT DATA	Cardholder Data	Primary Account Number (PAN)	✓
		Cardholder Name	✓
		Service Code	✓
		Expiration Date	✓
	Sensitive Authentication Data	Full Magnetic Stripe Data	X
		CAV2/CVC2/CVV2/CID	X
		PIN/PIN Block	X

Cardholder Data may be stored as long as they are stored SECURELY as per the Payment Card Industry Data Security Standards

Some DO's and DON'T's:

- ✓ Always change default passwords
- ✓ Always use strong passwords
- ✓ Use a firewall on your networks and computers
- X Do not store any sensitive data in your computer, cell phone or on paper
- X Do not permit any unauthorised people to access stored cardholder data
- X Do not store cardholder data unless it is absolutely necessary

⚠ Remember non-compliance can lead to fines.



Merchant Responsibilities

Guidelines for storing of cardholder data

Some DO's and DON'T's

Reporting Required

Contact Us



Reporting Required:

	Criteria	Reports Required
LEVEL 1	Any merchant who processes over 6 million VISA or MasterCard transactions per year, regardless of acceptance channel.	Appoint a Qualified Security Assessor (QSA) to conduct an Annual Onsite Audit.
	Any merchants who has suffered a hack or an attack that resulted in an account data compromise.	Appoint a Approved Scanning Vendor (ASV)* to conduct a quarterly network vulnerability scan .
	Any merchant specified by VISA, MasterCard or other payment card brand.	
LEVEL 2	Any merchant who processes between 1 – 6 million VISA or MasterCard transactions per year, regardless of acceptance channel.	Appoint a Qualified Security Assessor (QSA) to conduct a Annual Self Assessment Questionnaire (SAQ).**
		Appoint a Approved Scanning Vendor (ASV)* to conduct a quarterly network vulnerability scan .
LEVEL 3	Any merchant who processes 20 000 to 1 million VISA or MasterCard eCommerce transactions per year.	Complete a Annual Self Assessment Questionnaire (SAQ).**
		Appoint a Approved Scanning Vendor (ASV)* to conduct a quarterly network vulnerability scan .
LEVEL 4	Any merchant who processes fewer than 20 000 VISA or MasterCard eCommerce transactions per year.	Complete a Annual Self Assessment Questionnaire (SAQ).**
	Any merchant who processes fewer than 1 million VISA or MasterCard transactions per year, regardless of acceptance channel.	Appoint a Approved Scanning Vendor (ASV)* to conduct a quarterly network vulnerability scan .

* Visit www.pcisecuritystandards.org for Approved Scanning Vendor details

**Contact the Specialised PCI - DSS Help Desk for more information on the Annual Self Assessment Questionnaire



Merchant Responsibilities

Guidelines for storing of cardholder data

Some DO's and DON'T's

Reporting Required

Contact Us



Contact Us:

For more information please contact our Specialised PCI - DSS Help Desk on 0242 435 050 / 050 158 0838 or msgghana@firstnationalbank.com.gh

