**KCB Bank**
**Best Practices: Debit Card Usage**

Due to an increase in breaches at popular merchants, cardholder diligence and account monitoring is becoming more important as the first line of defense in fraud mitigation. Here are some best practices to follow:

- Monitor activity on your accounts regularly. Fraudsters are becoming savvier at avoiding detection of fraud monitoring programs by following transaction spending patterns that are similar to cardholders as well as by using less popular merchants that may not be monitored as heavily.

- Ensure KCB Bank has current contact information to reach you in case of suspect activity on your account.

- When shopping online, do not store your login credentials or your debit/credit card information on websites.

- Ensure your login credentials (user IDs and specifically passwords) for your computer, online banking, smart phones, web sites or any system where you log in has secure, complex passwords that are difficult to guess (ex: minimum of 9 characters long using a combination of upper & lower case letters, number and characters).

- Update passwords for web sites regularly to ensure continued protection.

- Be cautious of accessing personal information and of purchasing online if on an unsecured or public Wi-Fi network.

- Ensure that personal computer and smart phone protections are kept current (ex: firewalls, anti-virus software, etc.)

- Be aware of current fraud trends related to social engineering (ex: phishing) and social networking sites (ex: Facebook).