Mobile Banking Education

One of the biggest barriers to consumers adopting Mobile Financial Services is fear of security threats. Most consumers are afraid that their mobile device may be "hijacked"; some fear their sensitive information may be intercepted as it travels across a wireless network; and still others worry about the consequences if their mobile phone is lost or stolen. With most mobile devices lacking the personal firewall, anti-virus software and other protections common today on personal computers, these devices can be vulnerable to a variety of security threats, including:

- Malware: A term for "malicious software" that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system, or otherwise annoying or disrupting the victim
- Phishing: Luring unsuspecting customers to provide sensitive personal information or downloading malware through an email. Popular scams including phishing emails that appear to be coming from a FI and contain a link to a spoofed website; the site tricks victims into logging in using their personal credentials, which are then captured by the criminal.
- SmiShing: A contraction of "SMS and phishing", in which criminals pose as a FI and use SMS in an attempt to gain access to confidential account information. The typical scam informs the mobile device owner that the person's account was compromised or credit/ATM card was deactivated. The victim is directed to call a phone number or visit a spoofed website to reactivate the card. Once at the website or through an automated phone system, the victim is asked for card, Pass code and/or account numbers.
- Vishing: A contraction of "voice and phishing", in which victims are tricked into disclosing sensitive personal information through a phone call or voice response unit (VRU).

Mobile Fraud Prevention

- Monitoring

An example of fraud monitoring is the ability to detect a "bad digital identity (MUID)". Fraud detection in this case ensures a secure identity between the device and the host system. MNB utilizes an MUID to secure communications, preventing anyone who acquires a consumer's credentials from actually using them.

- Account/Customer Data

Additional security measures were taken in building the Mobile Banking solution. No customer identification or account information is stored within the Mobile Banking databases other than the mobile phone number. This information is used for logging purposes to report on activity and transactions that may be used by customer service representatives to support end-users.

Best Practices for Mobile Banking

- Modify the phone's settings so that only messages from authorized numbers are allowed.
- Add the FI short code and customer service phone number to your contacts and only initiate SMS and phone calls from your contact list. Do not reply to SMS messages that do not exist in your contact list.
- Do not click on links in SMS messages unless you initiated the SMS conversation with your FI.
- Do not call phone numbers not in your contact list. If you are unsure about a phone number, you may text "Help" to your FI short code and compare the phone numbers. Only call the numbers in your Help response or in your contact list to avoid Vishing
- Bookmark the FI's mobile web site and only use this bookmark to access the site to avoid phishing.
- Avoid using unsecured, public WiFi networks to access financial accounts with mobile devices.
- Always use your cellular network when conducting mobile financial services.
- Only download apps from stores, such as Apple & Android, that are submitted and branded by the FI.
- Finally, know that FIs will not ask users to provide confidential information over an email or SMS message.
- Always use your cellular network **or a secured private network** when conducting mobile financial services.
- Do not access Mobile Financial Services from a "jail broken device"