Mobile Banking Security Tips

- Lock your phone when not in use. This password protects your device so that nobody else can use it or view information. Also be sure to store your device in a safe location.
- Clear your mobile device frequently by deleting text messages from financial institutions, especially before sharing, discarding, or selling your device.
- Watch what you send **-** never disclose via text message any personal information (account numbers, passwords, or personal information that could be used in ID theft).
- Keep your device updated through iTunes for iPhone. For all other devices, contact your mobile service provider.
- Do not hack your device (also known as "Jailbreaking") as this can leave it open to infection from a virus or Trojan. We recommend you also install security software, if available.
- Stick with a secure network by ensuring wherever possible, that all internet connections are password protected.
- Use trusted apps - always download mobile apps from reputable sources. Get the Apps from the App Store or Android™ Market.
- You should never follow a banking link sent to you in a text message or e-mail; instead navigate directly to the Bank's Website.
- Avoid public Wi-Fi spots for banking. You might be tempted to check your balance or make some transfers while you grab a quick drink at a coffee shop. Before you log into your account, make sure you're not connected to the public network.

Account Takeover Protection Security Tips

- Online computer users should avoid using weak or default passwords for any online site and should refrain from using the same password for multiple sites. Use a "password manager" to put all your passwords in one database and avoid using the same password for more than one website.
- Before clicking on links or attachments in emails, always verify that the correspondent sent you the email with the link or attachment. Hackers are known for breaking into email accounts and sending malicious links and attachments. Verify with the sender to confirm the links or attachments are safe to click or open.

  The following applies mainly to business accounts:

- Institute and enforce a centralized plan for keeping computer applications, operating systems. and security software updated. Make sure servers and workstations are fully patched promptly and regularly.
- Implement a robust Intrusion Prevention Solution (IPS) to defend against cyber threats. An IPS provides policies and rules to block suspicious network traffic such as Web exploit kit attacks, SQL injection attacks, and banking Trojans that infect computers and steal data that allow intruders access to your banking accounts.
- Use a computer that is dedicated only to handling online banking and bill pay. That computer or virtualized desktop would not have any other capabilities, such as sending and receiving emails or surfing the Web, since Web exploits and malicious email are two of the key malware infection vectors.