2017 ABA Issue Summary

# Mobile Banking

Contact: Sarah Grano, ABA Public Relations (202) 663-5470 or sgrano@aba.com

**Mobile banking has revolutionized the way consumers do their banking.**

- Mobile banking involves using your mobile phone or other mobile device to access your bank account, credit card or other financial accounts.

- With this technology, you have the ability to remotely access your bank account and conduct transactions using your bank's website, mobile "app," or by text messaging.

**The popularity of mobile banking is growing fast.**

- Eighty-seven percent of the U.S. adult population have a mobile phone and 43 percent of all mobile phone owners with a bank account have used mobile banking.[1]

- Of those adult cell phone owners, 77 percent have smart phones and 53 percent of smartphone users have accessed mobile banking from their phone.[1]

**The banking industry is leading the way and responding to consumer demand.**

- According to the Federal Reserve Board, 81 percent of U.S. banks offer mobile banking services to their customers, with one-third of their customers using these services.[2]

**Mobile banking helps customers manage their accounts through mobile alerts.**[1]

- Mobile banking users are able to check their account balances before making a purchase and monitor their account for fraudulent activity while on the go. Among mobile banking users in the past year:
  - 52 percent receive low balance alerts
  - 43 percent receive deposit or withdrawal alerts
  - 43 percent receive payment due alerts
  - 38 percent receive statement notifications
  - 36 percent receive fraud alerts

**Mobile banking lets consumers manage their accounts in several ways.** [1]
**Among mobile banking users in the past year:**

- 94 percent have checked their account balance or recent transactions
- 58 percent have transferred money between their accounts
- 56 percent received an alert from their bank
- 48 percent deposited a check using a mobile phone camera
- 47 percent have made a bill payment on a banking app

**Mobile banking technology can help draw the "unbanked" into the mainstream financial system.**

- The Federal Reserve says 68 percent of the "unbanked" have access to a mobile phone and 40 percent have access to a smart phone.[1]

**Mobile banking technology is an attractive option for the "underbanked," providing them with an alternative way to conduct their banking transactions.**

- In the past year, 55 percent of underbanked adults used mobile banking services.[1]

# Mobile Banking

(continued)

**Customers should view their mobile device as a tool to help protect their account.**

- With 24/7 access to your account activity, you can use your mobile device to monitor your account for fraudulent transactions.

- Keep in mind, your mobile device is like a little computer. It's important to protect it against viruses and malicious software. (see consumer tips below)

**The American Bankers Association recommends following these tips to protect your mobile device:**

- **Use the passcode lock on your smartphone and other devices**. This will make it more difficult for thieves to access your information if your device is lost or stolen.

- **Log out completely when you finish a mobile banking session.**

- **Protect your phone from viruses** and malicious software, or malware, just like you do for your computer by installing mobile security software.

- **Use caution when downloading apps.** Apps can contain malicious software, worms and viruses. Beware of apps that ask for unnecessary "permissions."

- **Download the updates for your phone and mobile apps.**

- **Avoid storing sensitive information** like passwords or a Social Security number on your mobile device.

- **Tell your financial institution immediately if you change your phone number or lose your mobile device.**

- **Be aware of shoulder surfers.** The most basic form of information theft is observation. Be aware of your surroundings especially when you're punching in sensitive information.

- **Wipe your mobile device before you donate, sell or trade it** using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen.

- **Beware of mobile phishing.** Avoid opening links and attachments in emails and texts, especially from senders you don't know. And be wary of ads (not from your security provider) claiming that your device is infected.

- **Watch out for public Wi-Fi.** Public connections aren't very secure, so don't perform banking transactions on a public network. If you need to access your account, try disabling the

# Mobile Banking

(continued)

Wi-Fi and switching to your mobile network.

- **Report any suspected fraud to your bank immediately.**

*Sources:*

[1] *Consumers and Mobile Financial Services 2016,* Federal Reserve (March 2016). Retrieved from https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf

[2] *Mobile Banking and Payments: New Uses for Phones...and Even Watches,* FDIC (August 2015). Retrieved from https://www.fdic.gov/consumers/consumer/news/cnsum15/mobilebanking.html