Safe Mobile Banking

Using a smartphone, "tablet" computer or other mobile device to manage your finances can be convenient and help you monitor your money from practically anywhere. At the same time, it's important to take steps to protect your account information.

- **Be proactive in securing the mobile device itself.** Depending on what security options are available on your device, create a "strong" password (consisting of unusual combinations of upper- and lower-case letters, numbers and symbols) or PIN (with random numbers instead of, say, 1234 or the last four digits of your Social Security number) and periodically change it.

  "Always secure the device with a strong password or PIN in case it falls into the wrong hands," said Elizabeth Khalil, a Senior Policy Analyst in the FDIC's Division of Depositor and Consumer Protection. "Don't give that password or PIN to anyone or write it down anywhere." Also, never leave your mobile device unattended. Make sure you enable the "time-out" or "auto-lock" feature that secures your mobile device when it is left unused for a certain period of time.

- **Be careful about where and how you conduct transactions.** Don't use an unsecured Wi-Fi network, such as those found at coffee shops, because fraud artists might be able to access the information you are transmitting or viewing. Also, don't send account numbers or other sensitive information through regular e-mails or text messages because those are not necessarily secure.

- **Take additional precautions in case your device is lost or stolen.** Check with your wireless provider in advance to find out about features that enable you to remotely erase content or turn off access to your device or account if you lose your phone. Quickly contact your financial services providers to let them know about the loss or theft of your device. Notifying your bank quickly will help prevent or resolve problems with unauthorized transactions.

- **Research any application ("app") before downloading it.** Just because the name of an app resembles the name of your bank — or of another company you're familiar with — don't assume that it is the official one of that bank or company. It could be a fraudulent app designed to trick users into believing that the service is legitimate.

  "The best place to download an app is from the official Web site of the bank or company that you are doing business with or from a legitimate app store. Note that the business will often direct you to an app store," said Jeffrey Kopchik, a Senior Policy Analyst in the FDIC's Division of Risk Management Supervision. "Also, if possible, be sure to protect your financial apps, ideally with a password that is different from the password for your device."

- **Be on guard against unsolicited e-mails or text messages appearing to link to a financial institution's Web site.** Those could be "phishing" messages containing some sort of urgent request (such as a warning that you need to "verify" bank account or other personal information) or an amazing offer (one that is "too good to be true") designed to lead you to a fake Web site controlled by thieves.

  "The concern is that on that fraudulent site you may provide sensitive information while believing you are providing the information to your bank or another trusted party," said Matthew Homer, a Policy Analyst in the FDIC's Division of Depositor and Consumer Protection.

- Information courtesy of the FDIC