Your Guide to Signature Mobile Banking & Mobile Deposit

For Business and Personal Accounts

Enrolling in Signature Mobile Banking

1. Log in to Signature Internet Banking and select Administration > Manage Contact Preferences to confirm that your mobile number has been entered in your profile.

2. For Apple iOS (iPhone®, iPad®):
   Visit https://itunes.apple.com/us/app/signature-mobile-banking/id981716003?mt=8 and click on the link provided to be taken directly to the Signature Mobile Banking app within the iOS App Store®.

   For Android™ OS:
   Visit https://play.google.com/store/apps/details?id=com.mfoundry.mb.android.mb_bev85&hl=en and click on the link provided to be taken directly to the Signature Mobile Banking app within the Google Play Store™.

3. Once you have successfully downloaded the Signature Mobile Banking app, register your device by entering your mobile phone number.

4. To log in, enter your Company ID, User ID and Password.

Please Note:
You have a limit of 50 accounts that may be accessible through Signature Mobile Banking.

iPhone® and iPad® are registered trademarks of Apple, Inc. and App Store® is a service mark of Apple, Inc. Android™ and Google Play™ are registered trademarks of Google, Inc.

Signature Bank does not charge fees to download or use the Signature Mobile Banking app. Your mobile service provider may charge for data and text message usage. Check with your service provider for complete details.
GETTING STARTED

1. Enter your **Company ID & User ID**. Tap **Continue**.

2. Enter your **Password**. Tap **Continue**.

3. On the next screen you will select your mobile phone number and tap **Continue** to receive a security code by text message.

4. Enter the security code that you’ve received via text message and again tap **Continue**.

5. Then enter your phone # as directed to complete your enrollment in Signature Mobile Banking.

6. The Account screen will appear. Tapping the button at the bottom of the screen will lead you to further options.

INITIATING A TRANSFER

1. Tap the button at the bottom of the screen. Select Transfer from the Mobile Banking App menu.
2. When prompted select the appropriate Transfer From and Transfer To accounts.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
</table>
| Dos *9906  
Available balance $92.20 | Trees *9914  
Available balance $90.41 |
| Trees *9914  
Available balance $90.41 | Uno *8892  
Available balance $93.04 |

3. You will be taken to the Amount Screen to indicate an amount to transfer. Input the dollar amount and select Done when complete.

4. The Approve Transfer message will appear. Verify your transaction.

5. Once you approve, the Transfer Confirmation message will display.

Special Note Regarding Mobile Transfer of Funds Between Accounts:

The transactional limit when transferring funds from one Signature Bank account to another via Signature Mobile Banking is $99,999.99. There is no dollar limit on transfers made directly via Signature Internet Banking.

---

**SETTING UP BILL PAY**

To use the Signature Mobile Banking Bill Pay feature:

Whether using Apple iOS or Android™ OS, all Signature Mobile Banking enrollees must first visit their Signature Internet Banking account to set up all Payees and to select nicknames for each.
Paying a Bill

1. Tap the button at the bottom of the screen. Select Pay Bill from the Mobile Banking App menu.

2. Select the Payee and the Pay From account, and enter the Send On date and the Amount. Once complete select Continue.

3. The Approve Payment message will appear. Once you approve, the Payment Confirmation message will display.
MAKING A MOBILE DEPOSIT

1. Tap the button (+) at the bottom of the screen. Select Deposit from the Mobile Banking App menu.

2. You will be taken to the Deposit Screen. Select Continue at the upper right corner of the screen to proceed with making a deposit. (Tips for Photographing Your Check can be found on the next page.)

3. Please endorse all checks for deposit as follows:

   FOR DEPOSIT ONLY VIA SIGNATURE MOBILE BANKING

   ______________________________________
   Signature Bank Account #
   ______________________________________
   My Signature
   ______________________________________
   Date

4. You will then be taken to the Deposit photo image capture screen (left). Using your phone's camera, take the appropriate photos of the front and back of your endorsed check (right). Enter the check Amount, select Deposit To, and choose an account, and enter an email address in Email Receipt To. Select Continue at the upper right corner of the screen.

5. The Approve Deposit message will appear. You can select Approve or Cancel.

6. Once you approve, the Deposit Confirmation message will be displayed. Upon receiving this confirmation please note on the front of your check “Deposit Confirmed by SMB” with the date of deposit in order to avoid any possibility of mistakenly duplicating the deposit at a later time.
**PHOTOGRAPHING YOUR CHECK**

1. Place your check on a flat surface with a dark background and good lighting.
2. Be sure that the entire check appears within the frame (as shown on the left).
3. Take pictures of both the front and back of the check and upload them for verification. If the check cannot be verified, an error will be shown and you will need to retake the picture.

**PERFORMING SEARCHES OF ACCOUNT ACTIVITY**

1. On your Account Home screen, select your account.
2. On your Account ACTIVITY / SUMMARY screen, tap the Search Icon at the upper right corner.
3. On the Search screen, tap FILTER at the upper right corner.
4. On the Search Activity screen, choose the criteria by which you would like to search by clicking the arrow to the right of the appropriate selection.
5. When the criteria selection screen appears, enter the desired parameters or selection as shown in each sample screen below.
Special Notes
Regarding
Mobile Deposit

- Mobile Deposit cut-off time is 7:00 p.m. EST
- All mobile deposits are subject to review by Signature Bank. Once the item is reviewed by the Bank, we will email an approved or declined notice to the address you designated to receive the Email Receipt.
- The Daily Deposit Limit cannot exceed 5 checks or up to $25,000.00 in total. The Single Check Deposit Limit is likewise $25,000.00.
- A maximum of 25 checks or a total of $100,000 is allowed to be deposited via Signature Mobile Banking within a period of 22 consecutive business days. (Unlimited deposits may still be made via all other traditional deposit methods, i.e. ATM, Teller, etc.)
- Securely retain the original check for a period of 7 days and then securely destroy.
- Every day is a business day except Saturdays, Sundays and holidays. If you make a deposit before 7:00 P.M. EST on a business day, the Bank will consider that day to be the day of your deposit. All Items of Payment shall be credited to the Client’s account in accordance with the Bank’s Funds Availability Disclosure currently in effect.

Help

If at any time while using Signature Mobile Banking you feel that you need assistance, simply tap on the title at the top of the screen. A pop up will appear that will provide you with helpful information about that screen.

If you would prefer to speak with a Signature Bank Client Service Associate, call Client Services at 1.866.SIGLINE (1-866-744-5463). The regular hours for Signature Bank’s Client Services are 24/7.
SAFE MOBILE BANKING: OUR LATEST TIPS FOR PROTECTING YOURSELF

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. And 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 Website.**
  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 Website 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.

For more information, visit fdic.gov