Business Online & Mobile Banking Alerts

Business Mobile Banking

First Bank Business Mobile Banking Application has been enhanced with some new features. Details of these new features are described below:

Android Fingerprint Login

As part of the new release, users with an Android device that allows the setup and registration of a fingerprint can now sign into the Business Mobile Banking app using fingerprint login instead of entering a password. This feature is similar to the functionality already offered for Apple iPhones.

Deposit Tiles for all Users

This feature provides the ability for the mobile application to display the Deposit main menu tile to all users, regardless of whether the user's account is enabled for mobile deposit capture. If the user account is enabled for mobile deposits, the application will display the Deposit menu. If the user is not enabled for mobile deposit, the application will display the Deposit menu with a message to contact their financial institution for assistance.

Auto Populate Account on New Deposit Screen

This enhancement to the New Deposit screen will automatically select the deposit account when only one account is available.

Limit Loan Payment Types by Account

This enables users making a loan payment to see only the payment types available (i.e. principal, interest or principal and interest).

Mobile Device and Operating System Updates

The following have been added to our list of approved Mobile Devices and Operating Systems. The updates include: **New Mobile Devices**

FIRST BANK OF HIGHLAND PARK
1835 First Street
Highland Park, IL 60035
(847) 432-7800

FIRST BANK OF HIGHLAND PARK
633 Skokie Blvd.
Northbrook, IL 60062
(847) 272-1300

FIRST BANK CHICAGO
8833 Gross Point Road, Suite #202
Skokie, IL 60077
(847) 272-7800

FIRSTBANKHP.COM
FIRSTBANKCHICAGO.COM

Member FDIC | Equal Housing Lender | NMLS# 421795

- iPhone 8
- Samsung Galaxy S8+
- Samsung Galaxy S9
- Google Pixel 2XL
- Google Pixel 2
- Motorola Moto Z2 Force
- iPad (2018)

New Operating Systems
- Android O
- iOS11

The following list of Mobile Devices have been removed from our approved list. These devices are no longer supported due to low market usage.

- Apple iPad Touch 5th generation
- Apple iPad Mini
- Apple iPad 2, 3 and 4
- iOS 8
- Android 4.4 (KitKat)
- Google Pixel
- LG G3
- HTC One M7
- Motorola Nexus 6
- LG Volt

Business Online Banking 5.0 Upgrade

We upgraded Business Online Banking. This upgrade includes enhancements designed to provide more efficient cash management services and integration capabilities. This upgrade also changes the minimum internet browser and operating system requirements. Click here to view the "Certified Browsers and System Requirements" to ensure your current internet browser and operating system will remain compatible with Business Online Banking.

FIRST BANK OF HIGHLAND PARK
1835 First Street
Highland Park, IL 60035
(847) 432-7800

FIRST BANK OF HIGHLAND PARK
633 Skokie Blvd.
Northbrook, IL 60062
(847) 272-1300

FIRST BANK CHICAGO
8833 Gross Point Road, Suite #202
Skokie, IL 60077
(847) 272-7800

FIRSTBANKHP.COM
FIRSTBANKCHICAGO.COM

Member FDIC | Equal Housing Lender | NMLS# 421795

Here are some tips from the FBI that you can use to avoid becoming a victim of cyber fraud:

• Do not respond to unsolicited (spam) e-mail.

• Do not click on links contained within an unsolicited e-mail.

• Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. • Only open attachments from known senders. Always run a virus scan on attachment before opening.

• Avoid filling out forms contained in e-mail messages that ask for personal information.

• Always compare the link in the e-mail to the web address link you are directed to and determine if they match.

• Log on directly to the official Web site for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.

• Contact the actual business that supposedly sent the e-mail to verify that the e-mail is genuine.

• If you are requested to act quickly or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act impulsively.

First Bank of Highland Park