PLANTERS FIRST BANK

Payment News

For Business Customers

2nd QTR 2019

Planters First Bank
Technology Enhancement Notification

As part of our commitment to remain on the cutting edge of banking technology, we are pleased to announce that we are upgrading our computer processing system. Our enhanced system will help us continue to provide the extraordinary customer service you have come to expect, while enabling us to offer the most up-to-date products and services

Mobile and Online Banking

Business User ID

If you are currently a Company Administrator, your Online Banking ID will be the same. In order to complete the initial setup, each cash user must select the Treasury Management tab located on the main navigation bar.

Password
To log on the new system on **May 28** you will use a temporary password that will be the last 4 digits of your Social Security number or Tax ID. Business customers will need to use the last 4-digits of the TIN that is on that business profile.

Example customer:

John Smith Business
John Smith Business's Tax ID Number: 58-1234567
John's temporary password:4567

You will be prompted to select a permanent password for future use. Your password is case- sensitive and must be a minimum of 8 characters in length. Your password must include:

1) a number,
2) an uppercase letter,
3) at least 1 lowercase letters, and
4) a special character such as + _ % @! $ * ~

Important Dates for Enhancement

Monday May 20th

Commercial Remote Deposit is unavailable beginning **3:00 pm**

Treasury Management Specialist will begin working with Commercial RDC Customers to update Drivers and train.

Wednesday May 22nd

Consumer and Business Bill Pay goes offline

Thursday May 23rd

Mobile Banking goes off line at **4:00 pm** and Online Banking goes off line at **5:00 pm**

Tuesday, May 28th

8:00 am all Systems should be online

Any changes will be posted on our Website www.bankpfb.com

ATTENTION

Business Online Banking Admins

Please DELETE any user that no longer needs access prior to PFB's Technology Enhancement

Security Data If you are an existing Online Banking customer, you have used Multi-Factor Authentication for some time. You currently use device recognition to authenticate.

You will be prompted to verify by receiving a text, call or you can now use an App called Authy.

Authy is a free Multi Factor (2FA) App. 2FA is sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

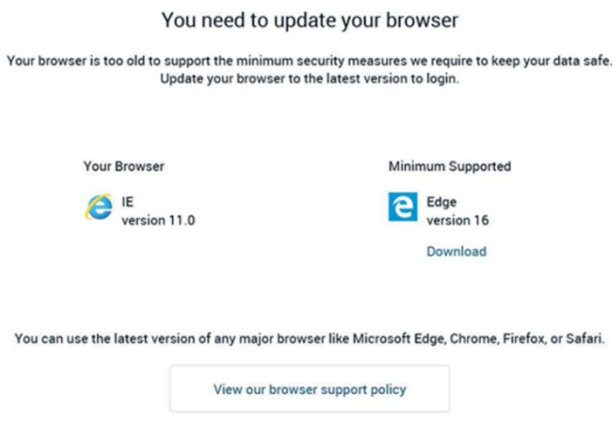
You can download Authy for phone/tablet by visiting your App Store on your device or Install directly from the Authy Website to your desktop computer.

If you have the ability to process ACH or Wires you will need to use your token to login and process your files. Wire Customers will be assigned new tokens. If you do not have a token for your Wire Transfer access before May 20th please contact Tracy NeSmith tnesmith@bankpfb.com .

Business Online ACH for Direct Deposit and Direct Payments is now accessed within Business Online Banking no more separate logon.

Browser Security Update

If you are using an older version of an internet browser it could put your computer/device security at risk. With our enhanced Online Banking and Mobile Banking, it will require you use the latest version of the browser you are using like Microsoft Edge, Chrome, Firefox or Safari. If you use Internet Explorer at login you will be prompted to download the latest Version of Microsoft Edge and a link to download will be provided. See screen shot below.



Email Address

Once you log in, please go Setting/User and update your email address in your Profile. This will allow us to notify you when your statements are available.

Check Images & Statements

Statement and Check Images produced after **May 23, 2019** will be available. Be sure to view or download all statements prior to **May 23, 2019 at 4:00pm** for our current Online Banking system.

Once available you will be able to view your Statements and images of checks through PFB's Mobile App.

Recurring Loan Payments

If you previously set up recurring loan payments within Online Banking, we anticipate that these will carry over in the new system. Please confirm your recurring loan payments by clicking on the "Transfer" link.

Automatic Transfers

If you previously set up automatic, recurring transfers within Online Banking, we anticipate that these will carry over in the new system. Please confirm your automatic transfers by clicking on the "Transfer" link.

Alerts

If you set up alerts in Online Banking, they will not carry over to the new system. To create alerts in the new system, go to Settings/Manage Alerts. You will need to verify your contact information. Under the two categories Balance and Transaction Alerts choose **+Add alert.**

Cash management will have additional CM-specific (e.g. wires) alerts within the Cash Manager tab > Settings.

Online Bill Pay

During PFB's system enhancement which is scheduled to begin on May 22, 2019 through May 28, 2019, your Bill Pay will be disrupted for a short time. This system enhancement DOES NOT require you to re-enter your existing biller relationships or alter your recurring or future dated payments. For eBill users, there WILL be one additional step required and you may temporarily receive a paper bill in order to initiate your payment. If you have automatic payments in response to an eBill presentment, they will be discontinued until you have re-enrolled into the eBill service.

If you Bill Payment is set to be paid/process on Friday May 24th there will be 1 business day delay. So, this means the payment will not be process until Tuesday May 28th. Please adjust your payments for this delay.

On Thursday May 16, 2019 eBill links will no longer be available in your current Bill Pay. If you currently are using eBill we recommend that you make a list of the eBills you are currently receiving, noting the following:

- The payee names.
- Due date of the last bill received
- Date paid (if paid before the system upgrade)
- Amount paid (if paid before the system upgrade)

Following your normal log-in you will see links on your biller list inviting you to "Set up eBills". Simply click the link and follow the online instructions. Upon re-enrollment of the eBill service, your billers may provide a duplicate bill. Please review your list against the bills presented and watch for any of the following situations:

- The bill presented is for the next month than the one on your list – PAY this bill.
- The bill presented is for the same month and amount as the one on your list –this is a duplicate bill, only pay if you have not paid before the system upgrade. If you have paid it before the system upgrade, click FILE BILL.
- A paper bill was received in the US Mail – pay this bill and watch for eBill in the coming months.
- No bill was presented nor received in the US Mail around the usual receipt date -contact the biller and verify your account due date and amount due.

It is also recommended that prior to **May 23, 2019**, you record the last eBill received and paid in order to monitor the flow from eBill to paper and then back to eBill.

Here's what you can expect when your Online Bill Pay upgrades on **Tuesday, May 28, 2019.**

- You will be prompted to answer a challenge phrase the first time you login to your upgraded Online Bill Pay account. This is an enhanced security that happens when making changes in Bill Pay.
- All of your payees and any scheduled payments will automatically carryover to the new system.
- 12 months Bill Pay history is provided for both retail and business
- The Admin users will need to login and add any users that were setup and their access.

You will find this information and a way to document your eBill payee profile in the eBill Online Enrollment Guide on our Website www.bankpfb.com .

Commercial Clients & Treasury Management Customers

If you need assistance related to commercial services such as Remote Deposit, ACH or Online wires, please call (478) 892-4024 or email tnesmith@bankpfb.com You may also use our toll-free number,(800) 684-8118, and ask to be transferred to Treasury Management Support.

Online Info Center

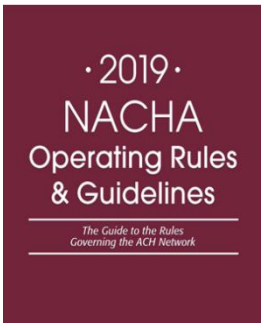
To learn more about the changes that will take place, please visit our website www.Bankpfb.com and go to the Technology Upgrade Info Center. You'll find demos for our new systems and answers to many commonly asked questions.

Commercial Remote Deposit Enhancement

Here is what to expect:

- On **Monday, May 20, 2018** the Current Commercial Remote Deposit will be unavailable after **3:00 pm** and will be back up **Tuesday May 28, 2019 at 8:00 am**.
- During this time, we ask that if you have a local Branch please make your deposits there and if you are a remote customer you can send your deposit next day and we will reimburse you the cost.
- A Treasury management Specialist will be reaching out to you soon to schedule a time to update your scanner driver and train you on the new software. If you do not get a call before **May 20th** please contact Tracy NeSmith at 478-892-4024.

The Importance of Understanding Your Obligation to Comply with the NACHA Rules to Participate in the ACH Network



The National ACH Association administers the operating rules for ACH payments, which define the roles and responsibilities of financial institutions and other ACH Network participants and the customers they serve. As a part of being able to participate in the ACH Network, you must comply with the *NACHA Operating Rules*. The Rules apply to all participants that use the ACH network for depositing ACH files such as payrolls, and other types of payments. This means that you as an ACH commercial client must comply with *NACHA Operating Rules*. Failure to comply may result in termination from the network making it difficult and, in most cases, impossible to transmit ACH payments.

When you signed your ACH agreement with us, you agreed to comply with *NACHA Operating Rules* and all U.S. laws. Simply put, you must follow *NACHA Operating Rules* and comply with U.S. law when sending and/or receiving ACH entries.

Tips for Complying with *NACHA Operating Rules*

Understand your requirements to comply with the NACHA Operating Rules and ask us to explain anything that you may not understand. Here are some guidelines on some of your requirements; however, for more information, contact us.

GUIDANCE FOR FRAUD PREVENTION

Unfortunately, fraudsters take advantage of many consumers and businesses by trickery or social engineering for the purpose of stealing their funds. The important lesson is for you and your employees to be aware of these threats and implement effective business practices. We dedicated to ensuring that you have information that could potentially prevent a fraudster from compromising either a system **or** tricking an employee at your location into surrendering credentials, personal information and/or funds. We are always working to help protect you and your accounts from fraudulent activity. Please contact us if there has been any fraudulent activity on your account or you suspect fraudulent activity. Along with security upgrades issued by a trusted Internet Service Provider (ISP), on a regular basis.

The Importance of Cyber Insurance: "Just in Case"

Cybercriminals are always out to get your money through stealing your online banking credentials and/or manipulating your employees to surrender your account information. While many corporate clients train their employees not to download unknown videos, click on unknown links or respond to individuals that are demanding sensitive information, it is also important to understand what insurance in case you need it. Insurance is a risk mitigator often called the "transference of risk". This is sometimes referred to "just in case" risk mitigation. Cyber-insurance gives you the protection in case you have fraud – like your insurance for other catastrophes or risk events. If you do not have cyber-insurance, we encourage you to learn about it. We always want to educate you on best business practices. Insurance for a possible fraud event is important and helps protect you "just in case".