Payment News

For Business Customers

1st QTR 2019

Planters First Bank
Quarterly Business Newsletters

PFB will be sending out Quarterly Newsletters beginning January 2019. These newsletters will have information for managing your Business through PFB's Business Online Banking. The topics we will be discussing are as follows:

- What's New- enhancements of products and services that PFB offers with Business Online Banking,
- Security Information- Fraud information and Prevention topics.
- Regulatory and Compliance- changes with Regulations and compliance issues that pertain to Online Banking for Businesses.
- Holidays and Events-Closure days and file instructions for processing. Events that PFB is hosting in your area.

The Importance of Layered Authentication

Authentication defined is a control that can be used to prevent unauthorized access, or simply to add a second layer of security to your current username and password combination. Client authentication and access control also enables organizations to meet regulatory and privacy compliancy. Financial institutions are required to comply with authentication as provided in the *FFIEC Guidance for Authentication in an Online Banking Environment*. Authentication practices include three basic factors:

1. Something the user **knows** (password, PIN)
2. Something the user **has** (e.g. token, smart card)
3. Something the user **is** (e.g. biometrics such as a fingerprint, device, etc.)

As your financial institution, it is important that you understand your obligations to protect your online banking system (cash management system). Fraudsters can steal your credentials through social engineering to trick you or your employees to surrender sensitive information or trick you or your employee to click on a link that produces a virus for the purpose of stealing your information. We are here to make sure you are educated and understand how to protect your money.

Please contact your account officer to ensure you have the right authentication for protecting your online banking credentials and your money.

Beneficial Ownership Rule

To help the government fight financial crime, effective May 18, 2018 for all new legal entities opening new accounts, financial institutions are required to obtain, verify and record information about the beneficial owners (individuals) of legal entity customers with 25% or more ownership or control over the legal entity. Legal entities can be used to disguise involvement in terrorist financing, money laundering, tax evasion, corruption, fraud and other financial crimes. This requirement allows the financial institution to obtain information on the beneficial owners who ultimately own or control the legal entity.

For the purposes of this new Rule, a legal entity includes a corporation, limited liability company, partnership, and any other similar business entity formed in the United States or a foreign country. Contact your branch for additional information.

A Reminder about Your ACH Obligations to Verify OFAC

As part of your obligations to comply with *NACHA Operating Rules* and the agreement with the Bank, you are required to validate that individuals and/or countries that have their assets blocked. This is considered a "hit" and should be reported to the Bank and OFAC immediately.

OFAC stands for Office of Foreign Assets and Control (OFAC). OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them

For more information visit

https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

A Reminder of Our Holiday Schedule

Monday, January 21, 2019 Martin Luther King Day

Monday, February 18, 2019– Presidents Day

Compliance Awareness: When there is a Need to Reverse a File or Entry

You may have had this in the past – you realize that you sent an ACH direct deposit file or entry or direct debit file or entry in error. You may have also experienced a situation when you duplicated an ACH file or entry. So, what do you do? First, the first rule is contact us immediately if you need assistance. If you don't know how to proceed, a call is the best answer. Below are reminders for you to ensure that you can perform a reversal without having a negative impact on your customer while still complying with the *NACHA Operating Rules*.

- A reversal of an ACH file or entry is only to be performed if the item or file is erroneous or a duplicate (e.g. you can't reverse a file or entry because you realized the file or entry wasn't appropriately funded);
- You are required to place the word **"REVERSAL"** in the company batch header as this provides the receiving financial institution information on what just happened.
- You are required to send a reversal within **5 banking days** after settlement date of the erroneous or duplicate file.
- When reversing an entry that is erroneous, the Originator must make a **reasonable attempt** to notify the Receiver of the Reversing Entry and the reason for the Reversing Entry no later than the settlement date of the reversing entry.

More information can be obtained in the NACHA Operating Rules Book which can be purchased at www.nacha.org.

Common phishing attacks: The Importance of Educating your Employees

DECEPTIVE PHISHING: The most common type of phishing scam, deceptive phishing refers to any attack by which fraudsters impersonate a legitimate company and attempt to steal people's personal information or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing the attackers' bidding.

SPEAR PHISHING: Fraudsters customize their attack emails with the target's name, position, company, work phone number and other information to trick the recipient into believing that they have a connection with the sender. The goal is the same as deceptive phishing: lure the victim into clicking on a malicious URL or email attachment, so that they will hand over their personal data. Spear-phishing is especially commonplace on social media sites like LinkedIn, where attackers can use multiple sources of information to craft a targeted attack email.

CEO FRAUD: Fraudsters can choose to conduct CEO fraud, the second phase of a business email compromise (BEC) scam where attackers impersonate an executive and abuse that individual's email to authorize fraudulent wire transfers to a financial institution of their choice.

PHARMING: A method of attack which stems from domain name system (DNS) cache poisoning. The Internet's naming system uses DNS servers to convert alphabetical website names, such as "www.microsoft.com," to numerical IP addresses used for locating computer services and devices. Under a DNS cache poisoning attack, a pharmer targets a DNS server and changes the IP address associated with an alphabetical website name. That means an attacker can redirect users to a malicious website of their choice even if the victims entered in the correct website name. To protect against pharming attacks, organizations should encourage employees to enter in login credentials only on HTTPS-protected sites, implement anti-virus software on all corporate devices, and implement virus database updates, along with security upgrades issued by a trusted Internet Service Provider (ISP), on a regular basis.