PLANTERS FIRST BANK

Business Online Banking News

2023 Issue 3

NEW TREASURY SUPPORT INFORMATION

To ensure that our customers are supported without delay, Planters First Bank now has a dedicated email address and phone number:

treasury@bankplanters.com

877.645.1146

BANK HOLIDAY SCHEDULE

Christmas Day
Closed Monday, December 25th

New Years Day
Closed Monday, January 1st

Martin Luther King Jr. Day
Closed Monday, January 15th

For ACH files please take holidays into consideration for payroll effective dates. Files received on these days will be processed the next business day. For half day closures please submit your ACH file before noon to ensure the processing of the file. If you have any questions, please contact Tracy NeSmith, Genny Newton, or the Solution Center at 877.645.1146.

Customer Spotlight

Video from GHS

https://youtu.be/yvKnQ-_QFhs?si=WBs0wqukgDdHLypT

Treasury Support

Treasury Support has grown to meet the needs of our business customers. You may have already been assisted by some of these team members. Each of these team members have been trained to assist with Business Online Banking, Business Bill Pay, Positive Pay, ACH, Remote Deposit and Online Wire Transfers.

Brandie Ward
Solution Center CSR

Ashley Sumner
Solution Center CSR

Cindy Burch, AVP
Solution Center Supervisor

Tammy Lynn
Solutions Center CSR

Genny and Tracy are still available for assisting with the setup of the products that you choose to implement, onsite visits and training. They are also backup to our support team.

BE PROACTIVE INSTEAD OF REACTIVE TO FRAUD.

Planters First Bank has a way to assist our business customers that will help them from falling victim to fraud. Positive Pay is a product/service that takes a company's daily transactions and compares them to a registry of their accounts payables that they have uploaded to Business Online Banking as they are paid or set up as an ACH filter. Daily after processing if there are any exception transactions the customer must login by 10 am and work their exceptions.

- ACH Positive Pay - customer has the bank set up filters of payees they do not want to be included. All other transactions will be listed to be worked as exceptions.
- Check Positive Pay - compares a registry uploaded by the customer and is compared to the daily paid items. Exception items are worked. Customer can also download an Outstanding and a Paid Check report daily. Software is looking at the following before deciding.
    - Payee Match
    - Check number.
    - Amount
    - Date issued.

ONSITE VISITS ARE STILL ONGOING

Tracy NeSmith and Genny Newton are preforming onsite visits. They are looking forward to seeing all of you and meeting in person. Please be on the lookout for an email to verify the time and date of our visit. If the timing is not good, please let us know so they can schedule a more convenient time to meet.

NEW TREASURY SERVICE-BAI2 FILE FORMAT EXPORT

Planters First Bank now has the option for our customers to import their payment information to a bookkeeping application that performs bank reconciliation if necessary, using File Manager. BAI2 files are a cash management reporting standard. Please call 877.645.1146 if you would like more information.

FRAUD TRENDS IN SMALL BUSINESSES: PROTECTING YOUR MONEY AND REPUTATION

Small business owners may feel that fraud is only something that happens to bigger companies. The truth is fraud may happen to any size business. What we know today is that fraud itself is a business whether that is internal or external fraud. The first step of preventing fraud is understanding how to identify it. Below are a few types of common fraud schemes and tips you can take to prevent it.

ONLINE PHISHING ATTACKS

Cyber security is a major issue for small businesses, who may not have dedicated teams to monitor online safety. While technology is a big win to reduce inefficiencies and process payments, it may also leave you vulnerable. Phishing scams are one of the most common fraud types. The way online phishing happens is that you first receive an email or attachment, which once opened exposes your business data to malware. This potentially compromises sensitive information, resulting in both financial and reputational damage.

To prevent technological fraud, use tools like IP address trackers, third-party payment processors, multi-factor authentication, positive pay, and data encryption. Ensure that your systems are updated with the latest security patches.

ACCOUNTS PAYABLE FRAUD

Accounts payable fraud is a common type of fraud that targets a company's accounts payable department, which is responsible for paying suppliers and other vendors. The fraudster emails the accounts payable department demanding an immediate payment or claims their payment is overdue by 30, 60, or longer. The fraudster may disguise themselves as a current vendor and just states their payment information has changed or the fraudster may have already hacked into the CEO or CFO's email and generated an email to the accounts payable department instructing them to pay the invoice as this is a new vendor. Either way, the accounts payable department unknowingly pays the fraudulent invoice. A typical organization loses 5% of its revenue to fraud every year, with a median loss of $125,000, according to the Association of Certified Fraud Examiners (ACFE).

Detecting fraud in small businesses is an ongoing process, with new scams popping up regularly. Here are a few general tips to keep your finances safe.

1. Implement Strong internal controls: Controls like fraud training, codes of conduct, management reviews, and countersignature requirements can all help prevent fraud.
2. Implement an escalation procedure for your internal teams to make it easier for them to report unusual/suspicious behavior.
3. Implement multi-factor authentication controls when sending payments including dual control procedures.
4. Contact us to determine security procedures we offer to help you mitigate fraud such as text alerts, positive pay, and other security offerings.
5. Don't pay anyone based on a single email without verifying the authenticity of the request.

It's sometimes easy to believe that fraud is something that happens to other businesses, not your own; however, detecting fraud in a small business using the tips above helps you avoid becoming complacent and protects your money and reputation. By putting safeguards in place, you'll be able to make your company a less attractive target.

Nacha Rule Requirements for Differentiating Between Corporate and Consumer Accounts.

The Nacha Rules allows Originators to send different types of standard entry class (SEC) codes. An SEC code is a three-letter code that describes how a payment was authorized by the consumer or business receiving an ACH transaction. SEC stands for 'Standard Entry Class'. SEC codes are defined and maintained by NACHA, the governing body for the ACH network. The most used SEC Codes are PPD (Prearranged Payments and Deposits) and CCD (Corporate Credits and Debits).

Since the file format requires only one SEC code, consumer and corporate transactions are to be in separate batches with the appropriate SEC code.

Consumer transactions are to reflect a consumer name in the "Individual Name" field and corporate transactions are to reflect the corporate name. A receiving financial institution relies on these codes when returning transactions; however, it is a Nacha requirement for the ACH Originator to select the correct code based on the type of account (e.g., consumer vs. corporate account).

The Type of Account Drives the Return Timeframe

When a receiving depository financial institution receives a transaction, there are return timeframes that apply based on if it is a consumer or corporate account. Consumer transactions have a 60-day deadline to return and corporate transactions have a 2-day deadline to return. This does not mean an ACH Originator may choose a CCD to shorten the amount of time the receiving depository has to return the transaction as this is a direct violation of the Nacha Rules. The receiving depository financial institution has rights under the Rules to respond to an incorrect use of a standard entry class code.

For example, if the ACH Originator sends a CCD to a consumer account, the receiving depository financial institution may return the transaction as an R05 return code. An ACH Reason Code R05 is a code used to indicate that an unauthorized debit to a consumer account has been detected using a corporate standard entry class code.

To comply with Nacha Rules, it is important to include this requirement as part of your ACH Procedures. If you have any questions regarding the proper use of standard entry class codes, contact us and we will be happy to discuss.

REAL-TIME PAYMENTS IN THE U.S.

The Federal Reserve Bank has recently implemented their real-time payment system called FedNow in addition to The Clearing House's RTP® network. The introduction of FedNow will increase the use of real-time payments in the U.S. Instant payments are a 24x7x365 service and can be used for consumers or businesses.

For some companies, the greater availability of real-time payments represents an opportunity to improve efficiency. As each company is different, there may or may not be a use case which will depend on your needs.

If you have any questions regarding how instant payments can work for you, let us know.

Tracy NeSmith, AAP
VP/Treasury Support Officer
Toll Free: 877-645-1146

Genny Newton
Treasury Management Specialist
877.645.1146

Contact us if you have any questions about NACHA Rules, fraud tips or other inquiries about your treasury services.