PFB BUSINESS FIRST ONLINE

4th Quarter

Planters First Bank
Electronic Banking Branch Support Team

Cordele-Casey Tyson
Fitzgerald-Cindy Burch
Hawkinsville/Pineview-Melanie Bush
Macon-Sheila Lanier
Ocilla-Amy Douglas
Operations-Ashley Greene
Perry-Terri Cumbus
Warner Robins-Kristina Gibbs

Treasury Management-Tracy NeSmith

These team members will be able to help support the Commercial Customers with products below.

- Password Resets
- Help with Electronic Statements
- Bill Pay

Digital Tokens

Customers that use our Treasury products:

- Commercial Remote Deposit,
- ACH Direct Deposit/Payments
- Online Wires Transfers

will be set up with an easier and more secure way to access their Treasury Products. Our Treasury Specialist Tracy NeSmith will be contacting you sometime before year end to set up a time for installation. After the install you will access everything with one set of credentials.

ACH FILE PICKUP

8:00 AM
12:00 PM
4:30 PM

Reminder: New Return Code R11 Becomes Effective April 1, 2020

The National ACH Association has approved a rule change regarding clarification of unauthorized return types to more clearly instruct the ACH Originator of the reason for the reject at the Receiver's institution. It is important in preparation for this new rule that you train your staff on (1) understanding the meaning of this return reason code and (2) understanding appropriate actions to take when receiving this return code from our financial institution.

WHAT THE RULE MEANS TO YOU

The rule re-purposes an existing, little-used return reason code (R11) that will be used when a receiving customer claims that there was an error with an otherwise authorized payment. Currently, return reason code R10 – Customer Advisors Unauthorized Improper, Ineligible, or Part of an Incomplete Transaction is used a catch-all for various types of underlying unauthorized return reasons, including some for which a valid authorization exists, such as a debit on the wrong date or for the wrong amount. In these types of cases, a return of the debit still should be made, but the Originator and its customer (the Receiver) might both benefit from a correction of the error rather than the termination of the origination authorization. The use of a specific return reason code (R11) enables a return that conveys this new meaning of "error" rather than "no authorization." This differentiation will give ODFIs and their Originators clearer and better information when a customer claims that an error occurred with an authorized payment, as opposed to when a customer

claims there was no authorization for a payment. ACH Originators will be able to react differently to claims of errors, and potentially could avoid taking more significant action with respect to such claims.

Return Reason Code R10 will be defined as "Customer Advises Originator is Not Known to Receiver and/or Originator is Not Authorized by Receiver to Debit Receiver's Account" and used for:

- Receiver does not know the identity of the Originator
- Receiver has no relationship with the Originator
- Receiver has not authorized the Originator to debit the account
- For ARC and BOC entries, the signature on the source document is not authentic or authorized
- For POP entries, the signature on the written authorization is not authentic or authorized

Return Reason Code R11 will be defined as "Customer Advises Entry Not in Accordance with the Terms of the Authorization." It will be used by the RDFI to return an entry for which the Originator and Receiver have a relationship, and an authorization to debit exists, but there is an error or defect in the payment such that the entry does not conform to the terms of the authorization. This includes:

The debit Entry is for an incorrect amount

The debit Entry was debited earlier than authorized

The debit Entry is part of an Incomplete Transaction

The debit Entry was improperly reinitiated

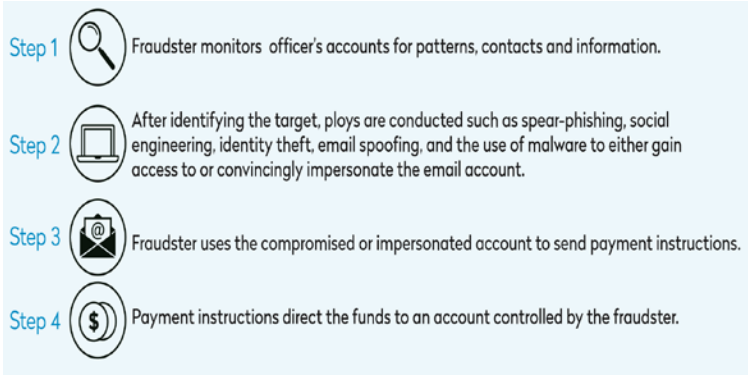
For ARC, BOC, or POP entries: The source document was ineligible, notice was not provided to the Receiver, and the amount of the entry was not accurately obtained from the source document.

DON'T BE THE VICTIM OF FRAUD SCHEMES

Fraud schemes continue to grow, evolve and target legitimate businesses, nonprofits, government and other public sector organizations. The FBI monitors schemes like Business Email Compromise and Vendor Impersonation Fraud along with other types of attacks. Below are some popular forms of fraud attacks on corporate customers. It is important to train management and your employees on these schemes to further protect against these types of events.

Business Email Compromise: What Is It and How Can It Impact You?

With Business Email Compromise, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise one of the business' officers and monitor his or her account for patterns, contacts and information. Using information gained from social media or "out of office" messages, the fraudster will often wait until the officer is away on business to use the compromised email account to send payment instructions.



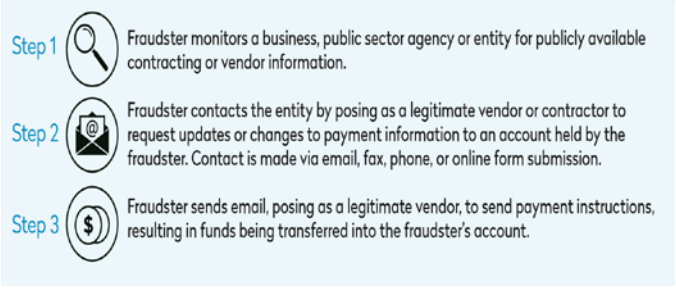
Strong internal controls are key to guarding against these scams.

Source: NACHA Protecting Against Fraud

- Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume it's a cybersecurity problem.
- Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, requests for secrecy, or pressure to act quickly.
- Authenticate requests to make a payment or to change payment information.
- Review accounts frequently.
- Initiate payments using dual controls.
- Never provide password, username, authentication credentials, or account information when contacted.
- Don't provide nonpublic business information on social media.
- Avoid free web-based email accounts for business purposes. A company domain should always be used in business emails. To make impersonation harder, consider registering domains that closely resemble the company's actual domain.

- Do not use the “reply” option when authenticating emails for payment requests. Instead, use the “forward” option and type in the correct email address or select from a known address book.

Vendor Impersonation Fraud: What is It and How Can it Impact You?



Vendor Impersonation Fraud can occur when a business, public sector agency or entity, such as a municipal government agency or a public university/college, receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payment along with routing and account information. This type of request could come from fraudsters and not the contractor. Although any business entity could be the target of this type of social engineering attack, public sector entities seem to be specifically targeted because their contracting information is oftentimes a matter of public record.