Same Day ACH Considerations

Phase 2 of same day ACH will begin September 15, 2017 and we believe it is important for you, our customer, to understand how this could affect incoming ACH credits and debits to your account (e.g. payroll/overdrafts).

Payments moving faster and the impact it could have on you:

If you currently have an automatic withdrawal from your account, or you make check payments to a business that converts your check to an electronic payment (ACH), the payment could now potentially be deducted from your account the same day. So it is important to ensure your account balance is sufficient enough to cover any checks or withdrawals to your account prior to authorizing the deduction.

CHECKS & DEBITS – As an example, you go online or make a phone call on Tuesday morning at 9:00 AM and you authorize an ACH payment to XYZ Cable, with a payment date of Tuesday, utilizing your routing number and account number. If XYZ Cable utilizes same day ACH, that payment could potentially be deducted from your account late in the day on Tuesday. If you were not anticipating this debit same day, it could potentially overdraw your account.

If you write a check to a business and they utilize same day ACH, the business would convert your check to an ACH transaction therefore, giving the deduction the potential to post to your account the same day. An indication of this conversion would include the business giving you your check back at that same time or the business has you sign an authorization form informing you of this process.

DEPOSITS & CREDITS – As an example, prior to same day ACH - your employer submitted a payroll file in advance so the funds would be made available by the opening of the business day. After September of 2016, if your employer were to choose to perform a same day ACH, your funds would not be available until later in the day.

Suspicious Activity

Payments moving faster means faster fraud:

Customers are required to report suspicious activity to the bank immediately after it is identified in order to mitigate potential losses to the consumer or business and to ensure the bank can address the unauthorized activity in the timeframe dictated by the ACH Rules.

Best Practices to Avoid ACH Fraud

Business

- Secure your tokens and passcodes separately at all times
- Utilize the dual control feature within Business PC Banking for all transmissions
- Review transaction history daily to confirm transaction activity
- Utilize limit restrictions for ACH transactions at multiple levels: per transaction, daily, weekly, or monthly limits
- Set up 6 day pre-notifications for transactions
- Take advantage of ACH Template Alerts
- Do not conduct online banking over wireless that you don't own
- Do not use your account number, social security number or other personal information when establishing your passcode
- If you receive an email from someone asking you to verify your personal information contact the bank immediately as the bank would never ask for this information
- Install anti-virus and spyware detection software on all computer systems

Consumer

- Review transaction history daily to confirm transaction activity
- Do not conduct online banking over wireless that you don't own
- Create a strong password that does not include using your account number, social security number or other personal information
- If you receive an email from someone asking you to verify your personal information contact the bank immediately as the bank would never ask for this information
- Install anti-virus and spyware detection software on all computer systems
- Never share your password or username information
- Do not use an automatic login feature that saves usernames and passwords
- Do not use the same password on all the websites you visit. Do not use the same passwords at home that you use at work.