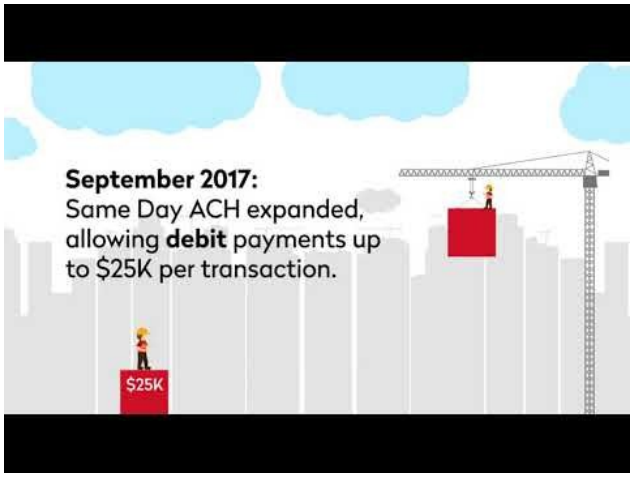
Treasury Management Newsletter

Same Day ACH Item Threshold Increases to $1 Million Per Payment

Nacha passed a rule that will go into effect March 18, 2022. This rule will increase the Same Day ACH dollar limit to $1 million **per payment** to allow network users the capability of expediting an ACH payment based on their need. While this rule allows a Same Day ACH amount of $1 million per payment, there is an exposure limit set for each Originator (e.g., daily file limit) that is currently in place. If you have a business need to send a larger Same Day ACH payment up to the $1 million per payment amount, please contact us prior to the effective date.



Wire Transfer Fraud Awareness

Training Your Employees to Identify and Prevent Fraud in your Business

As a small business, fraud prevention is likely a significant area of concern. While fraud is probably not on the mind of a business during the course of the day as there are many other tasks to complete for the business to be successful. To ensure your employees are aware of wire fraud trends and how to prevent fraud, training and fraud prevention procedures are important. Rather than fraud protection being one more task to add to your list, just include it as part of your business strategy based on external fraud threats and fraudsters attempting to steal your money.

Each year, fraud takes a toll on companies large and small, but in recent years, criminals are increasingly targeting local small businesses. The key trends along with action items for business owners to follow in an effort to prevent fraud are identified below. No matter how prevalent you think fraud is among small businesses, this information offers an opportunity to put in place the safeguards necessary to protect you and your customers.

Consumers and businesses are periodically conned into wiring money to infamous actors most often via licensed money transmitters like Western Union and MoneyGram. Once a consumer sends money to a

scammer, it is often impossible to find the fraudster or retrieve the money. What complicates matters is the reality that wire fraud criminals are located both inside and outside of the United States. As a business owner, it is necessary to recognize the most common wire fraud scams which include:

Business Email Compromise/Email Account Compromise: Imagine a typical day at the office. An employee receives a friendly reminder email from a vendor they've known for years about an invoice coming due. The email is conversational, asks about the employee's recent vacation, and then reminds the employee that a late payment for the invoice could result in a surcharge if not handled immediately. Communications like these may be the work of a wire fraud criminal.

Vendor Payment: A fraudster will email someone in a business informing them that their payment is late and will result in an additional late fee or removal of services._

Debt Collection: Posing as a debt collector, a wire fraud criminal uses threats to make the consumer settle a fake debt.

Advance Fee Loans: A scammer poses as an online lender and after the consumer submits a loan application, they are directed to wire processing payments to the lender. Once the consumer wires the money, the loan is never received.

Action Items for Businesses to Prevent and Mitigate Fraud

Several strategies can be put in place to make it more difficult for criminals to commit wire fraud. Small businesses may consider the following action items:

- Avoid free web-based email systems to transact business.
- Require employees to select unique and strong passwords or pass phrases.
- Require employees to change email passwords frequently.
- Require multi-factor authentication (e.g., email and telephone call) when receiving initial payment information or a request to change payment information.
- Send a confirmatory letter or email (not using the "reply" feature in email) concerning any request to change payment information.
- Delay payment in connection with any request to change payment accounts or a request to make payment to a foreign bank account.
- Provide clear instructions to business partners concerning how payment information should be communicated.
- Keep account authorizations up to date and notify the bank when an authorized signer or online banking user leaves.

- Review any request received by email to change payment accounts for signs that the email may be from a third party.

- Tightly limit access on who can manage recipient information to prevent changes to key fields like beneficiary account information and monitor changes to these fields, paying close attention to payroll files.

- Run background checks and credit checks on all new employees who have access to your finances and continue to reinforce not sharing your online credentials via training.

Procedures you can follow if you are the victim of wire transfer fraud

1. Notify us immediately to communicate the fraud so we can terminate online banking access and/or freeze the account.

2. Notify law enforcement.

3. Investigate whether your email system may have been compromised.

4. Ask business partners to investigate whether their email systems may have been compromised.

HAVE A SAFE AND HAPPY HOLIDAY!