CORE BANK

ISSUE #02 | Q1 2022

Contents

NACHA Rules Updates

Same Day ACH Limit Increase: *Effective Date March 18th, 2022*

What does this do? Increases the per-payment maximum from the current $100,000 to $1 million. It will apply to all eligible Same Day ACH payments, including credits and debits for both businesses and consumers.

The $1 million limit will be beneficial for many types of payments, from insurance claim payments and payroll funding, to business-to-business and tax payments, and many more.

> "NACHA has made a significant enhancement to Same Day ACH every year since it was introduced in 2016. This enhancement reflects our commitment to see that the modern ACH network meets the nation's needs for fast and efficient payments." – Jane Larimer, President, and CEO NACHA

Interested in sending Same Day ACH? Contact our Treasury Services team today!

Third Party Sender Requirements *Effective Date Sept 30, 2022*

What does this do?

1) Defines a Nested Third-Party Sender (TPS)- A Nested Third-Party Sender is a Third-Party Sender that has an agreement with another Third-Party Sender to act on behalf of an Originator and does not have a direct agreement with the ODFI.
2) Establishes the agreements and responsibilities in a Nested TPS arrangement- Nested Third-Party Senders must be addressed in the ODFI's ACH Origination agreements and the TPS must have an Origination agreement with its Nested TPS(s)
3) Updates ODFI's TPS registration requirements- An ODFI must identify all Third-Party Senders that have Nested TPS relationships in Nacha's Risk Management Portal and must provide Nacha with the Nested TPS relationships for any of its TPSs upon request
4) Requires TPS to conduct an initial risk assessment and update as needed.

Helpful Hints and Reminders: **What is a TPS?**

A TPS is an entity that has a contractual relationship with an Originating Bank (ODFI) to transmit debits or credits to the account of a Receiver on behalf of the Originator. A TPS has a contractual relationship between the Originator and the Third-Party and there is not an agreement between the Originator and the ODFI. A third-party sender sends payment on behalf of its client, originating the transaction through its own financial institution (bank) as opposed to the financial institution of the client. Example: If the Originator has a contractual relationship with a payroll processor and the payroll processor sends the ACH file to the payroll processor's financial institution for introduction into the ACH Network, the payroll processor is considered a Third- Party Sender.

Heads up: Failure to report TPS or Nested TPS can result in Nacha Rules violations. Unsure if you are a TPS or what category you may fall into? Visit the Third-

CORE BANK

ISSUE #02 | Q1 2022

Party Sender Identification Tool from NACHA (Link can be found in the Additional Resources section). The tool uses questions to help understand your role.

If you think TPS applies to you, or you would like additional information, please reach out to our Treasury Services Team for assistance.

Payment Industry Trends

Focus on Fraud: Per the 2020 AFP Payments Fraud and Control Survey, 81% of Organizations experienced attempted or actual payments fraud.

How do the fraudsters do it? One method to be aware of is Business email Compromise (BEC). BEC is a big win for fraudsters and continues to be successful based on the absence of training and assumed safe and sound procedures. Fraudsters can obtain access to business email and begin conversations with bank personnel. More detailed information on BEC can be found in the Additional Resources section.

Some numbers on BEC per 2021 AFP Payments Fraud and Control Report: Highlights:

76% of organizations were targeted by BEC in 2020.

Most Prevalent Types of Business Email Compromise (BEC) Fraud
(Percent of Organizations)

	LESS THAN 25 INSTANCES ANNUALLY	26-100 INSTANCES ANNUALLY	101-200 INSTANCES ANNUALLY	200+ INSTANCES ANNUALLY
Emails from other third parties requesting changes of bank accounts, payments instructions, etc.	88%	9%	2%	1%
Emails from fraudsters pretending to be senior executives using spoofed email domains directing finance personnel to transfer funds to fraudsters' accounts	87%	9%	2%	2%
Emails from fraudsters impersonating as vendors (using vendors' actual but hacked emails addresses) directing transfers based on real invoices to the fraudsters accounts	87%	11%	1%	1%

Another method is by Corporate Account Takeover (CATO). CATO is a form of corporate identity theft where a business' online credentials are stolen by fraudsters using malware. Criminal entities can then initiate fraudulent banking activity. Templates built in online banking can also be updated to include beneficiary account numbers for money mules or the fraudsters themselves.

How can you prevent fraud? The best safeguard is you and your employees. With training, recognizing signs of suspicious activity can help prevent your funds from getting into the wrong hands.

Security Tips:

- Verbally confirm payment instructions
- Use trusted phone numbers on record
- Establish dual control
- Be suspicious of urgent payment requests with changes
- Require payment instruction forms
- Utilize a secure email system
- Watch for address changes

Core Bank offers multiple fraud prevention products/tools such as ACH positive pay and security tokens. Contact a Treasury Sales Representative to find out more.

Notes from the Bank

COMING SOON…

ACH Stop Payments Effective for 2 years

Currently, ACH stop payments are effective for 6 months or 1 year which often doesn't give enough time for those annual fees and subscriptions. Core Bank will soon be increasing the expiration date on ACH stop payments to 2 years. Watch for additional communication on a go live date.

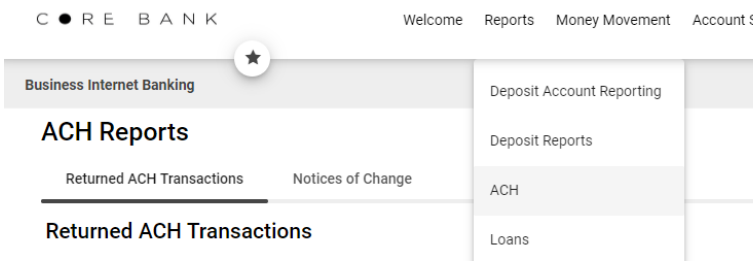
NOW OFFERING…

ACH Reporting for Returns and Notices of Change

Accuracy. Automation. Efficiency. Accessing ACH Return notices and correcting outdated ACH information is now a whole lot easier! No more waiting for calls from the Bank and more manually having to edit templates.

Core Bank went live with our ACH Reporting module and now ACH Return Notices and ACH Notices of Change are available online via our portal.

If you need any assistance in accessing these reports, please contact Treasury Services Support.



REMINDER…

Core Bank will send emails containing links to Risk Assessments as part of annual reviews. Be on the lookout for those emails and let one of our team members know if you have any questions. It is important to complete the assessments timely as delays might cause an impact to services.

Additional Resources

Third-Party Sender Identification Tool | Nacha

https://www.nacha.org/content/ach-rules-resources-corporates

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

Contact Information

Treasury Services can be reached at 402-898-3397 or treasuryservices@corebank.com.