PAYMENTS NEWS
FOR TREASURY CUSTOMERS

3RD QUARTER 2022

RULES CHANGE ON MICRO-CREDIT VALIDATION

There are some upcoming Nacha Rules ("Rules"} that are important to share with your internal teams. These Rules cover the micro-debit dollar amounts and the increase in the Same-Day ACH item amount. Both of these Rules are significant in the modernization and improvement of the ACH network.

Account Validation: Micro-Credits

Micro-credits are used to test the validity of an account and one of the ways Originators of WEB debits are validating the account as a fraud tool prior to initiating future WEB debits. In addition, micro-credits are also used to test the validity of accounts for online account opening. Nacha approved a Rule that will define and standardize practices and formatting of Micro-Entries. This new Rule defines Micro-Entries as ACH credits of less than $1, and any offsetting debits, for account validation. This Rule will be rolled out in two phases, including:

Phase 1, Effective Sept. 16, 2022:

- Requires that credit amounts must be equal to, or greater than, debit amounts, and must be transmitted to settle at the same time.
- Originators must use "ACCTVERIFY" in the company entry description field.
- Company name must be easily recognizable to Receivers and the same or similar to what will be used in subsequent entries.

Phase 2, Effective March 17, 2023:

- Originators must use commercially reasonable fraud detection. This includes monitoring forward and return Micro-Entry volumes.

For more information on this rule, visit https://www.nacha.org/sites/default/files/2022-03/End_user_Briefing_Micro_Entries_FINAL.pdf

WHY COMPANIES ARE IMPLEMENTING CONTROLS TO MITIGATE ELDER FINANCIAL EXPLOITATION –

Elder financial exploitation (EFE) is one type of elder abuse, which includes physical, emotional, and financial abuse. Elder abuse and EFE definitions vary statutorily by state. The Financial Crimes Enforcement Network (FinCEN) issues advisory warnings on significant fraud that impacts financial institutions, non-financial institutions, and companies that transfer funds. As a treasury customer, it is important to understand this type of crime that continues to increase, as it may impact your own business.

Older adults are targets for financial exploitation and their companies based on the wealth in the elder community (e.g., income and accumulated life-long savings). This wealth is coupled with the inherent nature of elders facing declining cognitive or physical abilities, isolation from family and friends, lack of familiarity or comfort with technology, and reliance on others for their physical well-being, financial management, and social interaction. The COVID-19 pandemic made this type of crime more attractive for fraudsters based on the vulnerabilities for many elder adults.

As a treasury client originating payments for consumers, you may identify red flags of possible elder financial exploitation.

This is not a complete list but brings awareness to your business that could stop potential elder financial exploitation.

Elder Financial Exploitation Red Flag Events

- An older customer appears distressed, submissive, fearful, anxious to follow others' directions related to their financial accounts, or unable to answer basic questions about account activity.

- An older customer mentions how an online friend or romantic partner is asking them to receive and forward money to one or more individuals on their behalf or open a bank account for a "business opportunity."

- During a transaction, an older customer appears to be taking direction from someone with whom they are speaking on a cell phone, and the older customer seems nervous, leery, or unwilling to hang up.

- An older customer is agitated or frenzied about the need to send money immediately in the face of a purported emergency of a loved one, but the money would be sent to the account of a seemingly unconnected third-party business or individual.

- A caregiver or other individual shows excessive interest in the older customer's finances or assets, does not allow the older customer to speak for himself or herself, or is reluctant to leave the older customer's side during conversations.

- The company is unable to speak directly with the older customer, despite repeated attempts to contact him or her.

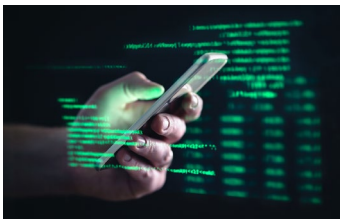
- An older customer's financial management changes suddenly, such as through a change of power of attorney, trust, or estate planning vehicles, to a different family member or a new individual, particularly if changes appear to be under undue influence, coercion, or forgery.

- An older customer lacks knowledge about his or her financial status or shows a sudden reluctance to discuss financial matters.

- Elder adult is seen at Bitcoin ATM on the phone talking with someone and seems confused about how to purchase Bitcoin.

If you feel like your company has identified elder financial exploitation, contact Adult Protective Services for your area. These state and local social service agencies investigate allegations of abuse, neglect, and exploitation of older and disabled adults and work with victims and their families to stop it. For reporting information, contact *The National Association of Adult Protective Services* at https://www.napsa-now.org/aps-program-list/.

Account Takeover: Understanding the Crime and Protecting Your Money - Account takeover is a



type of cybercrime or identity theft where a malicious third-party takes over an online account. This could be taking over an email address, a bank account, or social media profile. Fraudsters obtain security credentials that they can use to access a company or individual's accounts. The criminal can then initiate funds transfers by ACH or wire transfer to bank accounts using money mules to transfer the illicit funds. Examples of sound business practices for financial institutions include:

- Incorporate minimum levels of security on internal computer networks.
- Implement out-of-band payment verification (e.g., call backs, text verification, dual control, etc.).
- Encourage the use of value-added services like positive-pay, debit blocks, and tokens.
- Educate employees on prevention, detection and reporting measures; encouraging daily review of accounts.
- Review procedures for identifying money mules.

Contact your account officer for additional information on how you can protect your money.