The Regulatory Alchemist

A Publication of Alchemetric Solutions, Inc.

In this issue: ACH Suspicious Activities

May 2021

ACH Suspicious Activities

Recently a Tennessee newspaper, the Morristown Citizen Tribune, published an article pertaining to an indictment of an office manager of a local company.

As reported by the paper, investigators believe the office manager paid herself an extra $44,104 without the knowledge of the company's owner.

The newspaper reported that the individual manipulated payroll data and records to conceal her theft and that in some cases she altered payroll software to make it appear that she had issued direct deposits to a fictitious employee, whereas such funds were actually deposited into the office manager's bank account.

This item can serve as a training reminder that various types of suspicious activities can occur through the use of automated clearing house (ACH) items. For example:

- In the summer of 2020 national headlines were made relating to criminal activities involving inappropriate COVID-related unemployment insurance claims being made and distributed via direct deposits. In addition, these claims may have been made on behalf of fictitious individuals and were sometimes deposited into bank accounts of other individuals located in different states.

- Tax refund scams may also involve the use of direct deposits of inappropriately submitted tax refunds. Frequently such scams result in multiple tax refunds being deposited into an account where the recipients are not the account owners.

Given the increasing occurrences of such types of inappropriate activities, financial institutions need to implement internal controls to identify potential ACH transactions which may require the submission of a Suspicious Activity Report.

As a starting point for determining what internal controls may be needed by your institution, take a look at what ACH system reports are available. If your system has the capability to produce reports comparing ACH recipient names to account holder names, then processes should be implemented to make sure that this report is being regularly reviewed and that when appropriate, suspicious activity notifications are made to designated staff members.

However, it is recognized that some computer systems utilized by financial institutions offer more robust monitoring and reporting than other systems. If your system is one that is lacking in robust reporting, then at a minimum, staff members whose regular duties involve working with ACHs should be trained on the various types of ACH frauds that could be encountered and that such employees should be mindful of such activities while they are performing normal, recurring ACH activities - such as posting, reconciling, working with rejects, etc.

Finally, policy and procedure documents should be updated to reflect whatever ACH monitoring processes have been implemented at your institution.

And the Really Fine Print....