ACH SHOULD NOT BE AUTOMATIC

ACH, or Automated Clearing House, is a convenience of our modern world. Automatic deposit of our paycheck, automatic withdrawals for our mortgages or car loan, and even the ease of paying bills online – it's almost hard to imagine our world without ACH. Unfortunately ACH also provides ample opportunity for cyber theft. Changes to ACH-related information should be anything BUT automatic.

Does the following email look familiar?

> Dear Business Manager,
>
> I changed banks recently and need to update my account information for my automatic deposit. Please send me the form to complete.
>
> Sincerely,
>
> Your employee (not really)

Several M3 school district clients have informed us that they've received a similar request in the latest fraud attempt. While the email appears to be from an employee of the school district, there is one tiny error in the email address which directs correspondence to an illegitimate recipient. In some situations, the business manager might send the form and update the records for the next payroll run. If you didn't notice the error in the email address, would you process the change?

Have a secondary process to verify change requests prior to the next payroll run:

In order to mitigate this fraud risk consider instating a policy which avoids completion of any transaction involving financial information strictly through email. This could be as simple as adding a step to the process for a verification phone call to the employee to confirm the request. If email confirmation is important, make it your practice to start a new email and enter the individual's email address manually so you know it is their correct address.

CASE STUDY ON PROPER PROCESS

One school district shared how their process saved them from incurring a loss. It is their policy that, after a change request, the next payroll check issued is paper while the district processes a $0 pre-note to the new bank account to make sure everything works. This process prevented theft when an employee questioned their paper check. The business manager indicated the paper check was part of the process when changing bank account information. The employee quickly relayed that they had not requested the change.

Sometimes, even with your best risk management strategies, you will still incur a loss. Proactively address this possibility by making sure fraudulent impersonation – also referred to as social engineering or cyber deception – is covered under your crime or cyber liability policy.

Please contact your M3 account executive with questions or for further discussion.