ACH Rule Changes

ACH is becoming much more popular since the uptick in mail fraud in recent years along with the technology to alter paper checks. Also, ACH fraud is increasing. As a result, many banks are looking at their liability. Historically, if there was a fraudulent ACH, the bank would cover it for a good customer. Now they are trying to back down on this, even though they have insurance for this type of fraud. So they focus on the controls and procedures side of the process.

The key to this is having a strong banking relationship and getting your bank to stand up for the customer if something happens. ACH fraud is still fairly small as far as I know. And don't forget the "positive pay" feature where your customers send a list of checks they printed with verification data (payee, amount, etc.) for the bank to use when the checks are presented. This may carry a fee, but it puts the onus on the bank to do the job.

I agree that your customer should meet with the bank and review their procedures to show how they do have good controls and maybe get some good suggestions.

One of the key vulnerability controls is over changes to banks and accounts for ACH payments. Fraudsters will pretend to be a vendor and often know information that should be private and secure about that vendor's accounts. If they impersonate that vendor and send your customer a request to change the ACH bank routing info and the account, that is a red flag of a possible fraud attempt. Your customer needs to have a procedure for processing any request to change banking information that verifies with well-known vendor contacts that this is real and not a scam. If it is a scam, ask the bank how to report the attempt.

One PBS user failed to check and did a wire transfer for $500K to a fraudster bank account and did not recover the money. The Secret Service wrote a report and told them to forget it, the money was long gone.

John Miller