CPA
Practice Advisor

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

by ACH. That, in turn, accelerated another trend: fraud.

Nov. 10, 2020

Forced to work from home during COVID-19, accounts payable departments have accelerated plans to move away from paper checks and pay more of their suppliers by ACH. That, in turn, accelerated another trend: fraud. Through social engineering, fraud attacks on ACH credits are most commonly known as Business Email Compromises or BECs.

According to the 2020 AFP Payments and Fraud Control Survey Report, for the first

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Three-quarters of respondents said that preventing and detecting fraud has become more difficult in the current environment, and more than 90 percent expect attacks to increase. Organizations are under siege, and nearly one-third have received no guidance from banking partners about mitigating ACH credit risks.

What can organizations do?

Defeating BECs requires a multi-pronged approach. Ongoing anti-fraud training is important because these emails are getting more convincing every day. Fraudsters have become experts in user data and A/B testing, which reduces elements that alert their victims of illegitimate changes to their accounts. Strong internal controls are also important and network security, which prevents parties from gaining access to internal systems.

Here are four ways to help reduce your risk of ACH credit fraud.

1. Handle with Care

Thwarting ACH credit fraud is all about handling supplier banking data securely, which accounts payable must have on hand to transmit their payment file to the bank. This data is often stored in the ERP system, or sometimes on an Excel spreadsheet, where AP staff has been recorded during supplier onboarding. Sometimes it's stored when a supplier updates their information. Fraudulent change requests are one of the most frequent avenues of attack.

Let's say you've got a new person in accounts payable who isn't fully trained yet. This person gets an email from a supplier, asking to update their bank account information.

Your new hire, eager to please, fulfills the request, inputting a new routing number

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

You should never use an unsecured email for banking information updates, although a surprising number of companies still do. It's too easy for a hacker to intercept one of those emails and use the information within it for their own means. If they get contact or bank account information, they can pose as legitimate suppliers and circumvent internal controls. Some businesses even keep information in spreadsheets or their ERPs, but systems like those aren't designed to store data securely.

Some companies allow suppliers to update their own information in supplier portals. That might work, provided that companies manage secure portal access and verify all updates. However, if suppliers can log in and update information, it's likely that hackers can access the same information with very little resistance.

The most sophisticated approach that I've seen so far includes a trained procurement team, who verifies and validates all changes that come through.

There are a couple of drawbacks to this approach. It's a big IT investment with plenty of labor asks. Even then, it's still prone to internal fraud. At the end of the day, even the best systems will still have their risks. The goal is to minimize them.

3. Look at Fees

Companies often try to shift the risk and time burden to others, with some success. For example, they may choose to pay their suppliers by card., which puts the risk on credit card networks. In cases of card fraud, it's more likely that payments can be canceled or refunded.

Virtual cards offer even more security because they provide unique numbers, which can only be used by a specified supplier for a specified amount. The big drawback is that not all suppliers accept cards—there are fees to consider.

An organization I'm familiar with pays many of its suppliers with PayPal. Their

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

rise in tandem with the rise in ACH payments. But there is a perfect way to shift the risk to companies that are built to withstand the verification and validation burdens. Today's payment automation providers manage supplier information, so individual companies no longer have to spend valuable time on it. It's similar to handing the reins to IT and procurement departments to lock down the database and institute controls. The difference is that working with a provider removes the time investment and liability.

Think of payment automation providers as a means to outsource risk. Their sole focus is to ensure secure, on-time payments to your suppliers without causing costly overhead. They have perfected the systems and processes for hundreds of thousands of AP departments across the United States, and in ways that businesses would be hard-pressed to replicate.

Businesses used to worry about check fraud above all else. While they still have to pay attention to that aspect, it's become a low-tech form of fraud that's easy to understand and plan for. As companies shift to electronic payment means, they're increasingly experiencing sophisticated cyberattacks, which target much larger sums and are harder to defend against. With such attacks growing, businesses may find that outsourcing professionals is the best defense.

==============

Josh Cyphers is the President of Nvoicepay, a FLEETCOR Company. For the past 20 years, Josh has managed successful growth for a variety of companies, from start-ups to Fortune 100 companies. Prior to Nvoicepay, Josh held leadership roles at Microsoft, Nike, Fiserv, and several growth-stage technology companies. Josh is a lapsed CPA and has a BS in Economics from Eastern Oregon University.

Accounting • Technology

Hello. It looks like you’re using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us