to change bank account information. According to our internal data, these requests are common, with suppliers changing bank accounts roughly every four years.

Mar. 16, 2021

2020 was an eventful year for business payments. We saw expansive leaps in digitization, accompanied by new challenges. Remote work forced accounts payable departments to pay more suppliers electronically, primarily by ACH or direct deposit.

In many cases, companies began making ACH payments before they could adequately secure remote networks and environments and without new protocols and

procedures to ensure the secure handling of supplier bank account information. The

(Vendor Email Compromise). In this type of attack, criminals hack into supplier systems, monitor invoice flow, identify a potential weak spot among the supplier's customers and then reach out to someone in accounts payable to request a bank account update.

Often, they time this sort of change just ahead of a large payment. If successful, they route the payment to an account they've set up only to close it once they receive the funds.

AP teams stay vigilant when they receive requests to change banking information. But really, they always need to handle bank account data securely. If this data is intercepted, it gives fraudsters fuel to make their schemes more credible. IT departments need to secure company networks and environments. AP departments need to have stringent, repeatable processes for collecting, validating, and storing the information.

Collecting the data

Start with identifying the information you need to store. In addition to the routing, account numbers, and other remittance information, you may want to add security questions or other uniquely identifying information.

This information should never be transmitted via email, which is extremely unsafe. It's shocking how open people are with the information they share using that communication method. There's a lot of naivete surrounding the notion of business email compromise, or BEC. The FBI documented over $26 billion in *reported* losses from BECs between June 2016 and July 2019. According to the 2020 AFP Payments and Fraud Control Survey Report, BEC schemes were the most common type of fraud attack last year, with 75 percent of organizations experiencing an attack and 54 percent reporting financial losses.

With such attacks on the rise, banking data really should be sent via a secure portal

or fraud attempts. Make sure your team is well trained, so alarm bells go off in that scenario.

It's not just during the supplier enablement process that this information needs to be protected. Suppliers routinely send invoices that include bank routing and account information via email. Again, this is well-intentioned—the aim is to make it easier for the customer to pay them, but it's also risky. Using a secure portal is the best solution.

When accepting sensitive information over the phone, be sure to have phone validation procedures in place to ensure the person you're talking to is an authorized representative of the supplier.

Validating and securing

When you're setting up a relationship with the supplier for the first time, AP should work with procurement to validate all the contract information. They may also want to use a third-party tool or service provider that connects into banking networks to validate and authenticate account identity and ownership. There are many such tools on the market.

If you're switching an existing supplier from check to ACH, you may already have some visibility into their banking data as another way you can cross-check their information before making changes.

Once validated, information must be securely stored. Where housed on paper, companies should implement a level of physical protection such as locked in a file cabinet, but we know files are often kept in a folder on someone's desk or—in the age of remote work—someone's car or home. Many companies keep supplier data in spreadsheets. If someone were to intercept that information, it would be in peril.

When storing supplier banking information in an ERP system, ensure access is

With the pace of change and new security threats upon us, focus on worse-case scenarios may leave you feeling helpless and overwhelmed. Preparation is key to successfully managing change. Identifying these scenarios will help you predict and prepare for the challenges and pitfalls ahead as you safely transform your accounts payable flow.

========

Angela Anastasakis is the SVP of Operations and Customer Success for Nvoicepay, a FLEETCOR Company. She has more than 30 years of leadership experience in operations and product support. At Nvoicepay, Angela has been instrumental in leading Operations through rapid growth, while maintaining their 98% support satisfaction rating through outstanding service.

Accounting • Auditing • Security