half of the survey respondents, up from 46% in 2017. Wire transfers are still the most common target for BEC scams, probably because they're usually one-off requests...

Aug. 20, 2019

Earlier this year, AFP (Association of Finance Professionals) published its annual "Payments Fraud and Control Survey," which looks at trends in business payments fraud and what companies are doing to combat them.

The news wasn't particularly good. Even though companies are finding some success with increased fraud-prevention efforts, they're having trouble keeping pace. Eighty-two percent of the survey's 628 respondents said their organizations experienced attempted or actual payments fraud in 2018. That represents a nearly a 20% rise in

the past five years. We're at a point where it's no longer a question of whether your

Business email compromise (BEC) is a top tactic for external attacks, impacting over half of the survey respondents, up from 46% in 2017. Wire transfers are still the most common target for BEC scams, probably because they're usually one-off requests, so it's less noticeable when something is out of the ordinary. Checks are the second most common target because they're still the most common payment method.

The good news is that with heightened awareness and defenses, the number of companies experiencing BEC wire payments fraud has dropped 17%, from 60% to 43%.

The number of companies hit by BEC fraud targeting checks has dropped as well. Nearly 90 percent of organizations now report using Positive Pay. Roughly 70% say they have instituted internal controls such as segregation of accounts and daily reconciliation to fight check fraud. These measures appear to be working. Just 20% of companies reporting said BEC scams targeted paper checks, a 14% decline from the previous year. That far outpaces the decline in use of paper checks, which remains stubbornly stuck at about 50%.

The bad news is that one-third of companies reporting said fraudsters accessed ACH credits via BEC, up from 12% in 2017. According to the report, that means that criminals are now more able to invade internal systems through account takeovers (ATOs), and access harder-to-reach payment methods. This has caught companies off guard; 56% of survey participants said they aren't taking any additional steps to protect ACH payments.

Going After Bigger Fish

Another ominous trend: although monetary losses haven't increased significantly on a per-company basis (scams are typically designed to evade red flags by requesting ordinary amounts of money), fraudsters have stepped up attacks on large enterprises

where bigger payments are more common. And they're successfully stealing larger

What can companies do to protect themselves? They must fight this battle on many fronts. They should set up training, protocols, and controls to address different schemes, payment methods, and associated processes.

Education, training, and internal controls that prohibit payment initiation based on emails or other secure messaging systems are the top means to guard against BECs. Verification policies and minimum two-factor authentication are both important too, because scams are getting more and more convincing.

Positive Pay is a good first step against check fraud. You can take it a step further with Payee Positive Check, which adds the payee name to the data fields that are cross-checked.

Companies that actively protect themselves against ACH fraud use a variety of measures, including:

- reconciling accounts daily to identify and return unauthorized debits,
- blocking all ACH debits except on a single account set up with ACH Positive Pay and a debit filter, and
- blocking ACH debits on all accounts, and creating a separate account for ACH debits initiated by third parties such as taxing authorities.

Daily reconciliations are also a common way of protecting against attacks on security credentials. Other protections include restricting access to company networks to company-issued devices; dedicating a PC with no access to email, web browsers, or social networks to payment origination; and instituting disaster-recovery plans.

On the card payment side, single-use virtual cards are the most secure way to pay invoices, because the card number can only be used once, and only for a specified amount and payee.

Adding another layer

for them. The customer tells us whom they want to pay and how much, and sends us the invoices. We pull the funds needed to do the payment run into the account, then move that money to pay the suppliers, insuring and bonding all payments to ensure that they get to where they need to go. Our customers don't need to send us any bank account information, or even tell us how to pay the supplier—we keep all that information in our secure, cloud supplier payment network. We locate the vendor and find out how they want to be paid—print check, ACH payment, card (we use virtual cards exclusively), or a wire.

That system creates separation of duties, a key tactic in fighting internal fraud. We are the payor, so nobody internally is going to be cutting a check or authorizing a wire. Because we pay the same suppliers on behalf of many customers—and engage directly with those suppliers to collect and store their banking and payment data—it's nearly impossible to set up and pay a fake supplier, which is another common internal fraud tactic. Our practice of not collecting supplier bank account data from our customers also eliminates the opportunity to redirect payments to a different account.

We are also SOX- and SSAE-certified, and we leverage the latest and greatest cybersecurity techniques and technologies. We also have insurance coverage in case of losses due to an attack, which most companies don't have. A payment provider will, because their business rests on it.

No Signs of Stopping

As this year's report makes clear, payment fraud has become a game of whack-a-mole that the moles are winning. Companies have battened down the hatches on some fronts, only to find fraudsters popping up elsewhere with an even more insidious scheme. Despite some success in the battle, overall fraud continues to rise as

criminals deploy more stolen data and sophisticated technology in support of their

Jim Wright is Vice President, Enterprise Sales at Nvoicepay, working with companies with more than a billion in annual revenue. He is a veteran of the enterprise procurement and accounts payable space, having served in senior sales roles at Zycus, Corcentric and Ariba prior to joining Nvoicepay.

Accounting • Technology