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

remote workflows, left an opening for fraudsters to take advantage of the chaos. In the September 2020 edition of the Fraud in the Wake of COVID-19 Benchmarking Report, ...

Jan. 08, 2021

Since businesses began moving to a remote environment at the start of 2020, accounts payable teams have spent a significant amount of time ramping-up their ACH payments. Working from home has made it harder to get payments out to suppliers efficiently and securely.

The increased pressure on AP, combined with weak network security and unfamiliar remote workflows, left an opening for fraudsters to take advantage of the chaos. In the September 2020 edition of the Fraud in the Wake of COVID-19 Benchmarking

Report, the ACFE (Association of Credentialled Fraud Examiners) reported that 90

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

While similar in concept to BEC, VEC focuses more on controlling payments through vendor communication. Bad actors hack into vendor emails or business systems and watch the transaction flow for a while. They collect information on the vendor—anything from invoice structures to personal writing quirks. This later enables them to take over communication without raising suspicion.

Once they've identified an opportunity to re-route large ACH payments, they masquerade as the vendor in a spoofed email to the AP team, requesting changes to the account. Depending on the information they've collected, these emails can be quite convincing and ultimately, damaging.

In a successful fraud scenario, the bad actor will have convinced AP to re-route funds to their account. Once they retrieve the funds, the bad actors will close the account. Due to the quick nature of ACH payments, the entire heist can take very little time to pull off—often, mere days. By the time the legitimate vendor asks about their missing payment, it's impossible to retrieve the funds and the buyer is still on the hook for the actual payment.

Building Your Fortress

Many AP departments are not prepared to identify sophisticated, calculating cyberattacks like VEC. For decades, they have grown familiar with identifying check fraud. In those cases, enterprises have developed strong internal controls and combined them with their bank's Positive Pay and Positive Payee capabilities. Now they need to develop the same level of controls for ACH. A comprehensive system would look something like this:

1. Use tools like firewalls, threat monitoring, and multifactor authentication to block attacks on your infrastructure.

2. Put prevention measures in place. Train *all* new hires to identify malware and

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

4. Document your processes and protocols and update them frequently.
5. Never, ever share sensitive data via email.

It's not surprising if these steps sound like a lot; they are. As bad actors grow more proficient in their fraud attempts, it's up to business owners to prepare for when they inevitably become a target. This requires a certain amount of imagination—taking the time to think of how a bad actor might infiltrate your business allows you to shore up your weak points before they become a problem. A single successful attempt has the potential to impact not only the bottom line but also your business reputation.

In the end, the best method for protecting your business is staying vigilant and flexible to changes in fraudulent activity, such as the addition of VEC to the BEC fraud category. Expect the unexpected, and it will be much harder to throw you off guard.

=========

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.

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

Accounting

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved