# HOW TO MITIGATE THE RISK OF PAYMENT FRAUD IN THE NEW REALITY


IOFM Institute of Finance & Management

Sponsored by Corpay

# HOW TO MITIGATE THE RISK OF PAYMENT FRAUD IN THE NEW REALITY

Accounts payable (AP) departments of all sizes are under siege by fraudsters.

The increased risk of payment fraud is the biggest challenge that AP leaders say they face as their teams work remotely[1]. Fifty-eight percent of AP leaders believe their department's risk of payment fraud has grown since the start of the pandemic[2]. Twenty percent of AP leaders admit that their department's risk of payment fraud is "significantly" higher compared to before the pandemic[3]. Forty percent of AP departments have experienced "multiple" fraud attacks within the past year[4].

The operational disruption caused by both the prolonged shift to remote working and the growth in the adoption of Automated Clearing House (ACH) payments to suppliers has given rise to increasingly sophisticated cyberattacks that target larger sums of money and can be harder to defend against.

ACH fraud is increasing as fraudsters target accounts payable teams by impersonating suppliers via telephone and email, and tricking AP staff into diverting funds into banking accounts they control[5].

These cyberattacks are both harder to detect than low-tech check fraud, and difficult to plan for. And the fraud mitigation measures employed by most businesses were designed to prevent ransomware attacks and other software-based schemes—not scams that exploit human weakness. As a result, businesses must rethink their approach to mitigating the risk of payment fraud.

This white paper provides an action plan.

## The Downside of ACH Growth

The shift to remote working has resulted in the dramatic growth of electronic payments to suppliers. It's hard to chase down check approvals and print and mail checks to suppliers when payables staff are working at home.

The ACH Network moved 1.5 billion business-to-business ACH payments in the second quarter of 2022, a 12.3 percent increase compared to the same quarter the previous year[6].

Many industry observers have argued that the pandemic has done more to push businesses away from paper checks than the combined sales efforts of electronic payment solutions over the past decade.

But the growth of electronic payments also has created new fraud risks for businesses. By relying on email to collect and manage supplier banking information and approve invoices for payment, businesses have unwittingly increased their risk of falling victim to Business Email Compromise (BEC)—fraud schemes that use phishing attacks and social engineering to target ACH credits.

**75% of organizations experienced a BEC attack in 2019[7].**

BEC attacks were a growing problem before the start of the pandemic. In 2019, BEC schemes surpassed check fraud to become the most common type of fraud attack that businesses experience[8].

But remote working and the growth of ACH during the pandemic have resulted in more fraud attacks. Bad actors have adapted their tactics to leverage the disruption caused by the shift to remote working. They use operational disruption as an opportunity to confuse users into interacting with fraudulent content like clickbait articles and requests to change supplier banking information.

It's not a stretch to say that B2B ACH fraud could grow in tandem with ACH payment volumes.

**Three-quarters of organizations say that preventing and detecting payment fraud has become more difficult since the start of the pandemic[9].**

1 Institute of Finance and Management (IOFM) online survey, March 2021
2 Institute of Finance and Management (IOFM) online survey, March 2021
3 Institute of Finance and Management (IOFM) online survey, March 2021
4 Institute of Finance and Management (IOFM) online survey, March 2021
5 Association for Financial Professionals (AFP), *2020 AFP Payments and Fraud Control Survey Report*
6 NACHA press release, August 2, 2022
7 Association for Financial Professionals (AFP), *2020 AFP Payments and Fraud Control Survey Report*
8 Association for Financial Professionals (AFP), *2020 AFP Payments and Fraud Control Survey Report*
9 Association of Certified Fraud Examiners (ACFE), *Fraud in the Wake of COVID-19 Benchmarking Report*

BEC attacks also are typically better planned and more sophisticated than the phishing schemes of yesteryear. Fraudsters will use social engineering to research a buyer, members of its finance team, and its suppliers. Some criminals may even gain visibility into a buyer's AP approval processes.

Bad actors will use the insights that they gather to pose as suppliers, trusted coworkers or senior executives. A thiefr will send a spoofed email message to a buyer's AP department requesting a change in the bank account details that the buyer has on file for the supplier. It's not uncommon for these spoofed emails to include a long email thread that includes names, details, and even documentation that the bad actor uncovered during their social engineering. In some cases, a bad actor takes control of the email account of payables or finance professional to launch the BEC attack. Otherwise, the bad actor will spoof the email from another mail server.

By the time an organization realizes that an ACH payment is fraudulent, the thieves have already moved the money to offshore accounts, leaving little chance that the funds will be recovered.

**90% of organizations experienced an increase in the frequency of BEC attacks and other cyber fraud after the start of the pandemic[10].**

BEC attacks are so insidious partly because technology alone cannot stop them. Every employee should be aware of how bad actors can use legitimate information in nefarious ways. But they're not—and that's where many businesses are leaving themselves at risk.

## New Ways of Working, New Risks

Businesses must adapt the way they mitigate their fraud risk.

**The pandemic has made it easier for bad actors to execute payment fraud attacks.**

Bad actors used to focus cyberattacks largely on ransomware and other schemes designed to exploit vulnerabilities in code that wasn't secure enough to operate in the hostile internet environment.

Now that technology providers have hardened their systems, bad actors have shifted to schemes that exploit human weakness. Bad actors are capitalizing on the fact that many businesses focus their fraud-mitigation efforts solely on technology, without addressing vulnerabilities in human behavior.

For instance, bad actors have become nimbler in customizing their phishing schemes. Bad actors can use phishing campaigns to leverage their way into a laptop or home network. A common scheme in the past was to send spoofed emails from a major technology provider telling recipients that they need to update their passwords to avoid running out of drive space or having their email boxes fill up. Now that employees are working remotely, finance pros are more likely to receive spoofed emails from a delivery company instructing the recipient to update their password and other details.

These types of phishing campaigns can be hard to detect.

**Sophisticated cyberattacks have emerged over the past 24 months.**

Similarly, one common BEC attack sends a hyperlink to a finance professional via email. Clicking the hyperlink routes the recipient to a web server where a seemingly harmless greeting is presented. No malicious code. No nefarious scripting. While nothing may seem out of the ordinary, clicking on the hyperlink provides the bad actor with the source IP for their machine, compromising its security.

**BEC attacks are the highest source of security risks11.**

## How to Mitigate Your Risk

Cyberattacks shouldn't scare businesses from migrating to electronic supplier payments.

Taking a multi-pronged approach to fraud mitigation will help businesses mitigate their risks.

10 Association of Certified Fraud Examiners (ACFE), *Fraud in the Wake of COVID-19 Benchmarking Report*
11 Association for Financial Professionals (AFP), *2020 Payments Fraud and Control Report*

**More than 90 percent of organizations expect fraud attacks to increase[12].**

Ongoing training. Phishing emails are more convincing these days. The web makes it easy for fraudsters to uncover the names of legitimate suppliers and finance executives. Corporate letterhead can be recreated within minutes. Spoofed email addresses can fool staff who don't critically scrutinize requests to change bank accounts. And some fraudsters conduct A/B testing to determine which fraudulent emails are the most effective in duping unsuspecting businesses. The ultimate defense against payment fraud is creating an organization-wide security mindset. Staff needs to know the tactics employed by bad actors, and how to stop them. Employees should learn how to reduce the risk that they will fall victim to bad actors. Teach staff to suspect unsolicited emails and never click on hyperlinks unless they trust them. Urge employees to hover over hyperlinks to review the authenticity of URLs before clicking on them. Instruct employees to never open email attachments unless they trust the sender and are expecting the file. Impress upon employees that they should never provide credentials to anyone over the phone or via email. And they should lock their laptop or PC every time they step away from it. By taking a programmatic approach, businesses can foster a culture of fraud mitigation and increase engagement from staff on the frontlines of thwarting fraud.

**Employees must be aware of potential security threats when they work remotely.**

Strong internal controls. Securing hardware, laptops, and software is the table stakes in the fight against payment fraud. Bad actors can do as they please once they gain unfettered access to a company's hardware or software. Firewalls and other network security also are critical in preventing bad actors from gaining access to internal banking and payment systems. But businesses must also implement and enforce processes to help ensure that they aren't leaving the proverbial back door unlocked. For starters, businesses must establish processes for securely handling supplier banking data and validating requests to change bank account details. New employees who haven't been fully trained but are eager to please may be tempted to fulfill a fraudulent request to update a supplier's bank account information. Businesses also should leverage the experience and expertise of payment solutions providers. Some providers hold continuous operational threat briefings. They dissect every fraud attack and pass along their learnings to frontline staff, uncover potential vulnerabilities in the payment processes employed by businesses, and develop effective security measures.

**Criminals now rely on people-centered tactics like weaponizing email.**

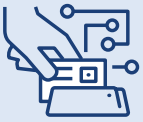
Data security. Organizations should never exchange sensitive banking information via email. It's too easy for hackers to intercept emails and use contact details and bank account information for nefarious purposes, such as posing as legitimate suppliers to circumvent internal controls. Spreadsheets and ERP applications also weren't built to securely store bank account details and other sensitive data. Even supplier portals are not without risk. Sophisticated thieves can hack into portals and access bank account information with little resistance. Similarly, few businesses can afford the IT investment required to prevent bad actors from infiltrating their firewalls and accessing supplier banking information. All these are reasons for businesses to shift the responsibility of collecting, storing, and updating supplier banking information to payment solution providers that can withstand the verification and validation burdens. Some solution providers have data-security experience developed over years of working with thousands of finance departments.

**Many businesses never considered the vulnerabilities of remote working when developing their security infrastructure.**

Virtual cards. Virtual cards are the most secure way to pay suppliers. Virtual cards aren't the same as the plastic purchasing cards that many businesses use to buy office supplies and other small ticket items. Unlike physical cards, virtual cards cannot get lost or stolen, and they offer several layers of protection that make them resistant to fraud. The 16-digit number created for each virtual card can only be used once. Each virtual card number created is associated

12 Association of Certified Fraud Examiners (ACFE), *Fraud in the Wake of COVID-19 Benchmarking Report*

with unique amount or amount range, a merchant ID number, and a date or date range. Transactions are declined if each piece of information does not match. Businesses can further reduce their risk of fraud loss by using virtual cards through a payment solution provider with proven fraud controls in place. Not every supplier will agree to get paid with a virtual card, but those that do can help mitigate the risk of fraud.



**Virtual cards offer level of fraud protection not found in ACH payments.**

These measures will help a business reduce its fraud risk while achieving operational efficiencies.

## Thrive in the New Reality

The shift to remote and hybrid working environments has created new operational challenges and new risks for AP departments. Bad actors are seizing upon the operational disruption to adapt their tactics and exploit human weaknesses. Increasingly sophisticated BEC and phishing schemes and other cyberattacks divert supplier payments and compromise financial activities. To reduce their risk of payment fraud losses in this new reality, businesses need a multi-pronged strategy that combines ongoing employee training, strong internal controls, data security, and virtual cards.

## About Corpay

Corpay is a global leader in business payments, helping companies of all sizes better track, manage and pay their expenses. Corpay provides customers with a comprehensive suite of online payment solutions including Bill Payment, AP Automation, Cross-BorderPayments, Currency Risk Management, and Commercial Card Programs. As the largest commercial issuer of Mastercard in North America, Corpay handles over a billion transactions each year. Corpay is part of the FLEETCOR (NYSE: FLT) portfolio of brands.

To learn more visit www.corpay.com.

## About the Institute of Finance & Management

Accounting and finance professions have each undergone nothing short of a complete transformation since the Institute of Finance and Management (IOFM) was founded in 1982 and since then our mission has been, and continues to be, to align the resources, events, certifications, and networking opportunities we offer with what companies need from the accounting and finance functions to deliver market leadership. IOFM empowers accounting and finance professionals to maximize the strategic value they offer their employers.

Our enduring commitment to serving the accounting and finance professions is unmatched. IOFM has certified over 25,000 accounting and finance professionals and serves several thousand conference and webinar attendees each year.

IOFM is proud to be recognized as the leading organization in providing training, education and certification programs specifically for professionals in accounts payable, procure-to-pay, accounts receivable and order-to-cash, as well as key tax and compliance resources for global and shared services professionals, controllers, and their finance and administration (F&A) teams.

Learn more at IOFM.com

IOFM Institute of Finance & Management