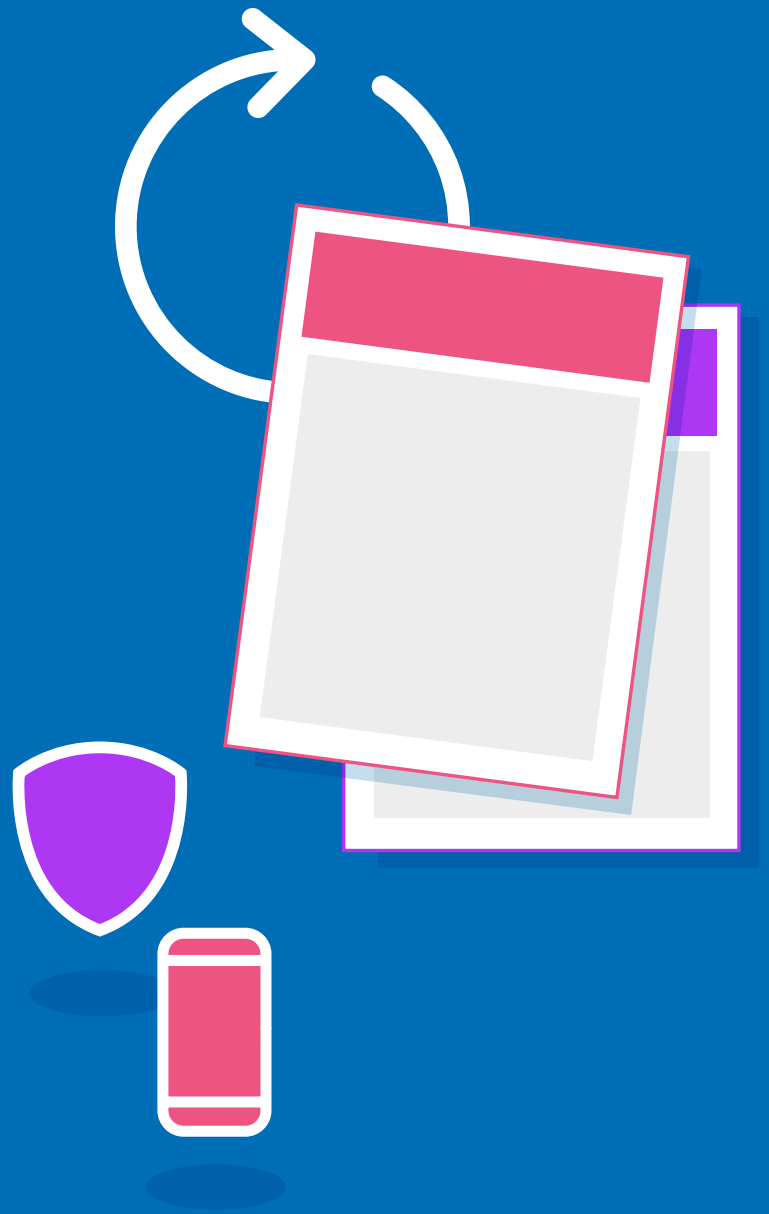
Bottomline

Winning Against B2B Payment Fraud

How AP Can Defeat Emerging Payment Fraud Threats

Table of Contents



The Fraud Quagmire

Payment fraud attacks are coming fast and furious. Accounts Payable (AP) departments are the target.

These attacks are not random attacks, so to speak. They're fraudsters counting on passing go when it comes to your payments. Fraudsters are leveraging increasingly sophisticated strategies to get past defenses. They know their quarry – often, right down to the name and account number. And, in many cases, they are successful.

It is no wonder that not only AP leaders but Chief Finance Officers, Treasury executives, and heads of government have payment fraud on their radar. The reality, however, is that if you avoid one breach, more are already on the way.

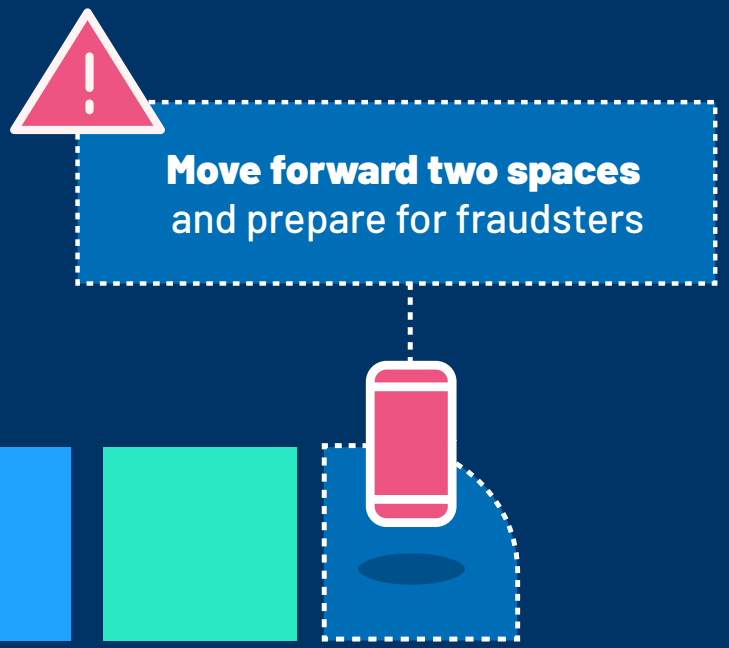
To protect your B2B payments, you need two things. First, a clear understanding of the nature of the threats you are facing. Second, comprehensive defenses that work in real-time to neutralize those threats.

Don't roll the dice. It's time to play your cards wisely and come up with a winning strategy to come out victorious in your battle with payment fraud.

FRAUD TOPS ALL OTHER AP CONCERNS

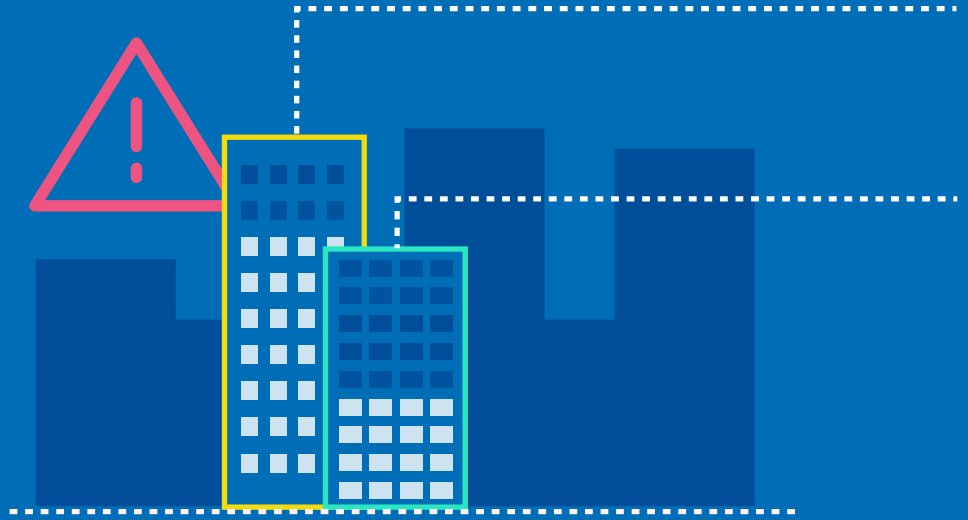
70% of AP leaders believe fraud is their **#1 AP challenge**

58% think their fraud risk has **increased**



Fraudsters Pass Go, Collect $200

Bad actors today are not restricted to lone fraudsters working in their homes. Fraud is big business, and there are international criminal organizations by the hundreds that are investing time and money in technologies and strategies to steal from organizations like yours. ***They are creative, they are well-trained, and they are relentless.***



70%

of businesses were **targets of attempted payment fraud** in the past year

40%

of AP departments have experienced **multiple cases of attempted fraud**

Fraudsters take advantage of every loophole with the latest technology. They commandeer events – including natural disasters, political turmoil, or economic unrest – to find opportunities to slip in under the radar. That is why it is imperative to be familiar with and on guard against their latest schemes.

One particular scheme that tops the list today is business email compromise.

WARNING!

Business Email Compromise Ahead!

Fraudsters are and have been using business email compromise (BEC) – also known as email account compromise (EAC) – to beleaguer AP departments.

The Federal Bureau of Investigation (FBI) states that losses from this scam surpassed $43 billion globally between 2016 and 2021, and that number is rising.

What Is BEC?

When using BEC, fraudsters send your AP department an email that appears to come from a known vendor or internal colleague, containing what looks like a legitimate request. For instance, you might receive a request to update a vendor's banking information, but the "new" banking information actually diverts payments to the fraudster's own bank account.

27% of all cyber crime-related financial losses reported by businesses in 2022 were due to BEC

Losses to BEC are approximately **80x greater** than losses to ransomware

$124,000 is the average cost of each incident in 2022

The BEC "market" is expected to grow from **$1.1 billion in 2022 to $2.8 billion** by 2027

FBI's IC3 2022 Internet Crime Report
FBI's IC3 2022 Internet Crime Report
FBI's IC3 2022 Internet Crime Report
MarketandMarkets, 2023

Two Roads to BEC

There are two main types of BEC scams that frequently breach AP defenses:

THE COMPROMISE

The Compromise.
A compromise situation is even worse; in this case, the fraudster has hacked into your own or your vendor's email system and is literally emailing your AP department using the correct email address. If the fraudster makes a normal payment-related request, there is nothing to raise a red flag. And, of course, any tools that IT has put in place to monitor incoming emails and block bad attachments or malicious links will not filter these emails out, since they are the correct email address.

THE SPOOF

The Spoof.
Fraudsters pretend to be a vendor or colleague by using an email that is almost the same – but not quite – as the actual person's email address. For example, if the email is ted.hinny@company123.com, the fraudster will send an email from ted.hinney@company123.com. Catching the added "e" is very difficult, and if the email sounds like "business as usual," an AP employee will not be suspicious. Also, be mindful of bad actors switching the letter l for a capital I, and vice versa, because that is almost impossible to detect unless you slow down.

The Social Engineering Play

Fraudsters using BEC make heavy use of social engineering. This includes:

EARNING TRUST.

BEC fraudsters are very patient. They may send innocuous emails to an AP employee for days or even weeks in the guise of a vendor, engaging in conversation to establish their bona fides before finally slipping in the request or submitting the false invoice that was their goal all along. Watch for odd phrasing, uncharacteristic language, and typos.

TAKING ADVANTAGE OF CURRENT EVENTS.

Situations that cause turmoil and promote a sense of urgency are ripe for BEC fraudsters. For example, when Silicon Valley Bank collapsed, a huge number of vendors needed to update their banking information because they were quickly changing or establishing new bank accounts. Fraudsters stepped in and leveraged the emergency for their own ends. When there is a major situation, be suspicious of both new emails and emails relating to the topic.

IMPERSONATING INTERNAL LEADERS.

Fraudsters will pose as AP leaders or business executives and make requests of AP employees, such as asking for a vendor payment to be sent on a rush basis to a new bank account or requesting confirmation of a vendor's bank account data. These emails are often timed when AP employees will be tired or flustered, such as at 4:30 p.m. on a Friday. It is worth an extra cup of coffee to stay vigilant at the end of the workweek.

BEC scams are often not "one and done." Once they experience initial success such as a diverted payment or updated bank account, fraudsters may ramp up their efforts. Consequently, you can be defrauded multiple times before you discover and shut down the fraudster. By that point, you might be out large sums of money.

Problems on the Board

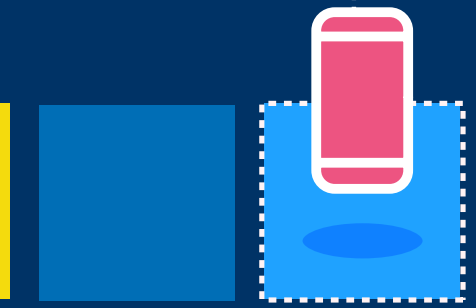
SIM Swap Fraud

Fraudsters are zeroing in on cell phones. The reason? Through them, they can intercept multi-factor authentication (MFA) codes and log in to bank accounts, emails, and payables systems. By gaining access to your or your vendors' accounts, they can steal payments outright and/or practice scams that leverage impersonation. It is essentially a skeleton key for bad actors.

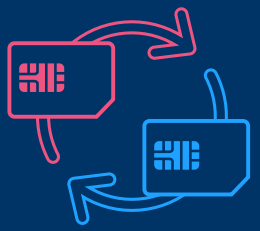
Cell phones are breached through a SIM swap fraud. This is where a fraudster tricks a mobile provider into activating a SIM card in their possession for the victim's cell phone number.

Once activated, any calls or texts go to the fraudster's phone rather than to the victim's phone – including, for example, the MFA codes that are used to verify identity before logging into a bank account.

Breach Detected!
Move back one space.



2018-2020:
320 SIM swap complaints were received by the FBI with losses of approximately **$12 million**



2021:
1611 SIM swap complaints were received by the FBI with losses topping **$68 million**

Check Your Checks: Positive Pay Fraud

Positive Pay, often referred to as Payee Positive Pay, has been considered a robust defense against a stolen check being turned into a fraudster's windfall. With Positive Pay, a bank will only pay out the check to the business named on the check. Unfortunately, this security measure is now being compromised across the United States by a relatively simple fraud.

HERE'S HOW IT WORKS:

1. The fraudster registers a business name with the state.
2. The fraudster opens an account at a bank for the business.
3. The fraudster steals one of your checks on its way to your vendor.
4. The fraudster adds your vendor's name as a fictitious name or Doing Business As (DBA) name to their business's profile on the state business registration website.
5. The fraudster adds that fictitious name or DBA to their bank account.
6. The fraudster deposits the stolen check without any problem since the payee name and the name on the bank account match.

Because check reconciliations take a long time, ***it is not uncommon for three months to go by before the real vendor wonders where their check is and reaches out to you –*** only for both of you to suddenly realize that the check has been cashed and the money is long gone. ***That's a huge reputational and monetary hit for your company.***

ChatGPT: Fraud in the Cards

Like any technology, artificial intelligence (AI) can be used for good or ill. Fraudsters, unfortunately, are finding ChatGPT and other forms of AI to be extremely useful for carrying out their scams.

CHATGPT ENABLES FRAUDSTERS TO:

IMPROVE SOCIAL ENGINEERING.

AI can generate emails that are grammatically, socially, and culturally appropriate – a far cry from the often-parodied and easily-identified "I am a prince" scams. This lets scammers who are not fluent in a certain language effectively target victims who speak that language, boosting their success rate.

CREATE DEEP FAKES.

It is possible to create deep fakes using any type of content: written, audio, images, and video. Doing so enables fraudsters to impersonate colleagues and vendors with a new level of realism. As the technology improves, so will the results.

MULTIPLY MALWARE.

Coding malware is a breeze when fraudsters can instruct ChatGPT to make hundreds or thousands of iterations based on stated specifications. This new, AI-generated malware can slip through existing security filters and deceive colleagues and vendors into revealing sensitive information.

As ChatGPT and other AI tools increase the breadth and depth of fraudsters' capabilities, ***the ramifications for protecting B2B payments will only become greater.***

STOPPING *Sophisticated Fraud from Gaming You*

In the current economic environment of "do more with less," AP departments feel under the gun – and rightly so. They have fewer resources yet greater responsibilities because of the sophisticated nature of the fraud attacks that are targeting them. Nevertheless, despite the apparently overwhelming odds, AP can win the day against fraudsters galore.

Prioritize Training

Success begins with rigorous training. For AP, that means providing in-depth education and training on the common types of payment fraud and how to counter them. This enables AP teams to work smarter and keep your company safer. Payment partners such as banks and financial organizations frequently offer training and education programs that you can take advantage of.

Bear in mind that security training should take place on an ongoing basis since fraud schemes are continually being refined and invented, with ChatGPT and check fraud being recent examples. Your AP team needs to be consistently provided with current information in order to identify subtle fraud attempts.

The goal of education and training is not simply to equip AP with information; it is to create a culture of awareness. That means making awareness part of your DNA so that any time an email, request, phone call, or transaction is even the slightest bit "off," your AP team instantly pauses to investigate further.

Draw again
to begin your training

When you have an attempted or successful fraud attack at your company, incorporate it into your training. **A real-life example of how fraudsters have targeted your organization will drive home the importance of security policies and procedures.**

Establish the Right Rules

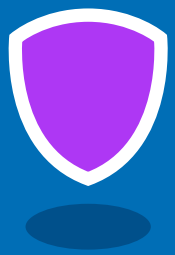
Every game has its rigid set of rules to prevent bad behavior and cheating. So should your AP department. Well-considered and well-executed policies and procedures are one of your greatest defenses against B2B payment fraud.

For example, rules should be established for:

- Adding new vendors to your portfolio
- Authenticating vendors when they reach out via email or phone
- Specifying how bank account changes can be submitted
- Auditing vendor bank account changes
- Reporting and escalating incidents for investigation

Rules should incorporate layers of protection. The more layers of protection you have instituted, the safer you and your vendors are. For instance:

- Employ multi-factor authentication (MFA) across all online portals
- Have each AP employee protect their cell phone SIM card by putting a separate PIN on it
- Use secure portals for vendor communication rather than email
- Never take payment instructions or bank account changes through email or phone calls



"There is one piece of advice that is worth repeating 100 times: Put multi-factor authentication everywhere you possibly can to limit your exposure to a breach."

Chris Gerda, Risk and Fraud Prevention Officer, Paymode-X, Bottomline

Partner Up

You and your AP team are not alone in this high-stakes game. You have the opportunity to engage with banks, financial organizations, and other B2B payment experts to dramatically increase your odds of winning.

There are two key areas where strategic partnerships are especially valuable: ***converting checks to virtual cards and practicing business identity authentication.***

1. Convert Checks to Virtual Cards

Virtual cards enable you to pay your vendors electronically through an existing payment card network such as Visa or Mastercard. **They provide coveted security through:**

SINGLE-USE PROTOCOLS.
Virtual cards use a unique 16-digit, randomly-generated number, expiration date, and CVV that can only be used once.

TRANSACTION-LEVEL CONTROL.
You issue virtual cards for a specific payment amount and set controls to decline the authorization if the vendor pulls a different amount.

SECURE ACCOUNT DETAILS.
Virtual card account details are securely stored and can only be obtained by authorized users.

VENDOR DATA PROTECTION.
Virtual cards eliminate the need for you to hold vendor bank account information.

ROBUST CARD NETWORKS.
Virtual cards leverage the built-in security and controls of the card networks, making them a highly-secure form of payment.

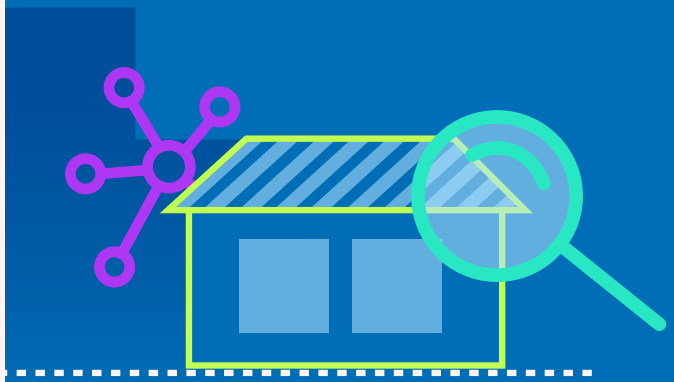
These security measures minimize the risk of payment fraud associated with data breaches and other attacks, not to mention completely eliminating the risks that are inherent to paper checks. Plus, some solutions provide comprehensive reporting, user behavior monitoring, and payment risk scoring to allow you to identify red flags or anomalies that could indicate possible fraud attempts before they actually occur.

2. Don't Roll the Dice. Use Business Identity Authentication

In the realm of B2B payments, business identity authentication is the act of validating that a vendor is who they say they are before inputting their business information, changing their bank account information, or submitting a payment. It is, in effect, "the moat around the castle" that protects you from attack.

Robust business identity authentication is an ongoing and never-ending process that incorporates data from every touchpoint with the vendor. For example, within the Paymode-X network, user, behavioral, and device data is generated every time a vendor looks at a payment report, draws down a virtual card, receives an ACH transaction, or logs in to do automation reporting. This data is used to authenticate the next vendor interaction which, in turn, generates further data. Each cycle makes the vendor profile that much more detailed, and the security that much stronger.

Ultimately, business identity authentication eliminates worries about payments and even the need for payment monitoring because the vendor is known at such a deep level that payments can be sent with complete confidence.



"Big data equals big fraud protection. Therefore, any ability that you have to utilize a larger network or partner to help you authenticate a vendor is to your advantage because they are looking at a much broader attack surface, which is very meaningful to mitigating your risk."

Chris Gerda, Risk and Fraud Prevention Officer, Paymode-X, Bottomline

A Winning Strategy

Nearly every week, your AP department will face a new attack by fraudsters. Yet even the most sophisticated ambushes can be thwarted by prioritizing basic training, establishing standard operating procedures, and engaging in strategic partnerships. Business email compromise, SIM swaps, Positive Pay loopholes, and even ChatGPT-facilitated frauds all fall before this robust, winning strategy.

Take the time to assess your vulnerability to payment fraud, and take action to mitigate any risks that currently exist.

You can win!

Paymode-X: Your Get-Out-of-Fraud Card

With the tips we've offered, you're well on your way to protecting yourself from fraudsters trying to game your systems. If you're looking to take payment fraud prevention to a whole new level, we can help.

With 550,000+ businesses exchanging over $400 billion in payments annually, Paymode-X is the largest electronic payment network in the world. We pride ourselves on providing vendor authentication, protecting payments with layered security using more than 300 data points to identify bad actors, and multi-factor authentication to keep your payments safe. That's how we exchange those payments with zero fraud every year, and how we go beyond the moves you can make yourself to give you true payments peace of mind.

Corporate Headquarters
100 Internetional Drive,
Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
Fax: +1-603-436-0300
info@bottomline.com