

REPAY[®]

Realtime Electronic Payments

Fighting Payables Fraud

REPAY WHITEPAPER



Table of Contents

Introduction.....	3
Common Types of Payment Fraud.....	4
Paper Checks.....	4
ACH.....	4
Compromised Data.....	5
Illegitimate Vendors.....	5
Imposters.....	5
The Psychological Impact on Fraud Victims.....	5
Tools to Take on Fraud.....	6
ACH Validation.....	6
Custodial Accounts.....	6
Positive Pay.....	7
Secure Data Storage.....	7
Permission Control & Separation of Duties.....	7
Protect Every Payment with REPAY.....	8



Introduction

From counterfeiters to thieves, money has always been a target of bad actors.

As civilization has evolved, so have our methods of paying for goods and services. The 2020 pandemic expedited the necessity for digital payments and new ways to protect against the fraudsters who evolved just as quickly.

Businesses became prime targets of payment fraud, as many were still using archaic paper processes that didn't offer enhanced security.

There are many reasons for accounts payable (AP) teams to adapt to the digital age, including the time and cost savings it can offer when making vendor payments. However, one essential reason that should be at the top of every business's list is security.

Here, we will cover common fraud schemes and the solutions REPAY has available to protect every payment.



Common Types of Payment Fraud

📍 **Paper Checks:** 40% of businesses still make most of their B2B payments via check. [Source: pymnts.com]

Besides being expensive and slow, paper checks have your account and routing number printed at the bottom. Ripe for the taking!

Common check scams include forgery, kiting, theft, counterfeiting, washing, alteration and more. In fact, 63% of respondents to a JPMorgan study stated they had experienced fraudulent check activity. [Source: JPMorgan.com]

Another consideration regarding paper checks is they must be sent via mail to the vendor or business. Last year, the United States Postal Service issued a warning stating that mail fraud was rising at alarming rates, with 25K reports in early Q1 2023. [Source: CBSNews.com]

📍 **ACH:** A popular alternative to credit cards, ACH offers lower costs and more convenience, but because they involve bank account information, they have gained the unwanted attention of fraudsters.

The percentage of organizations subject to ACH fraud increased by 7% from 2021-2022. [Source: JPMorgan.com] Naturally, that number will increase as more businesses use ACH. However, the fact there is no real-time verification offers fraudsters a prime opportunity.

Fraudsters who infiltrate ACH transactions have a day or two before the business finds out it is an illegitimate transaction, meaning the fraudsters and the funds are long gone by the time the transaction is verified.





•• **Compromised Data:** In 2023, a singular fraud attack breached over 1.5 billion accounts. [Source: [Secureblink.com](https://www.secureblink.com)] Yes, that is billions with a “B.” Cyber-attacks are hitting businesses at high frequencies, gaining access to sensitive account data and costing businesses millions of dollars.

Besides money, compromised data has a long-term impact – damaged reputations. Many businesses find recovery challenging as vendors and customers become skeptical of doing future business with them.



•• **Illegitimate Vendors:** When an AP department pays a vendor or supplier, they must be confident that the funds are going to the correct place. However, this is not always the case. Fraudsters set up fake vendor accounts to gain unauthorized access to invoice systems. From there, they can submit low-value, quickly-approved invoices to themselves as the small amounts aren't likely to raise suspicions.

They may even set up direct payments to send themselves, flying under the radar for months at a time.

•• **Imposters:** Like illegitimate vendors, imposters are criminals who impersonate real people and con businesses and employees into sending them money.

There are many tactics imposters use, including AI, phishing, vishing, voice mimicking, forged signatures and counterfeit documents. You may have even been on the receiving end of a fraudulent text from your CEO urgently requesting you purchase and send them high-value gift cards. It is essential to remain vigilant, and always confirm in the event something appears suspicious.

•• **The Psychological Impact on Fraud Victims:** The fraud types mentioned above cost businesses more than just money; they often negatively impact victim's mental health. 53% of respondents of a recent survey who experienced social engineering fraud blame themselves. [Source: [aarp.org](https://www.aarp.org)] Victims often cite feelings of embarrassment, anxiety, shame, fear and hopelessness, which need to be taken seriously. [Source: [Stories.td.com](https://www.stories.td.com)]



Tools to Take on Fraud

Fraud tactics are ever-changing, making it nearly impossible for businesses to take on payment security themselves. They often lack the resources, funds and expertise to fight back against them.

REPAY enlists several security tactics to help protect B2B payments so businesses don't have to go it alone.

🔗 **ACH Validation:** Nacha, the governing body of ACH, requires companies like REPAY to screen debit transactions.

REPAY screens transactions for account status, payment/NSF/chargeback history, ownership and personal identifying information (PII) consistency.

Catching fraudulent ACH transactions before they go through helps you:

- Reduce ACH return ratios
- Expedite unsuccessful payment responses
- Learn more about your customers

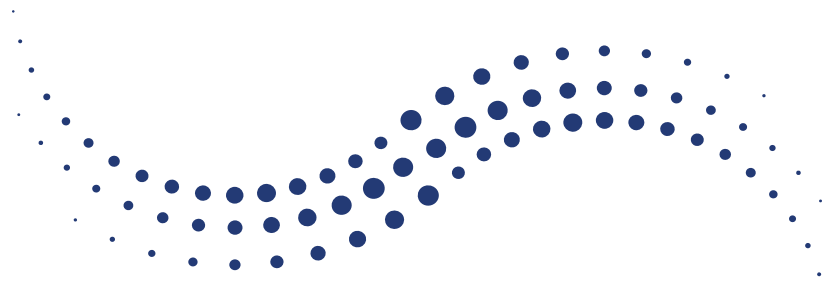
Implementing ACH validation requires a heavy development lift and is time-consuming to maintain, making REPAY an obvious choice to partner with.

🔗 **Custodial Accounts:** Sending paper checks or ACH for payment leave bank account numbers vulnerable. REPAY can help you set up a custodial account where you can “sequester funds.” This means you have a separate bank account that is used solely for making vendor payments, so fraudsters can't access your main accounts.

Funds are only transferred to the custodial account when it is time to pay.

- Eliminates access to business account and routing numbers
- More control over credits and debits

If you have multiple bank accounts, maintaining a custodial account can be tedious. REPAY can help with setup and management.





••• **Positive Pay:** Positive pay is a service where banks register and confirm the validity of checks before they are processed. Issuers can stop a fraudulent payment before the money goes missing.

In 2022, one company's positive pay solution prevented \$791M in check and ACH fraud.

[Source: q2.com]

However, positive pay can be very expensive for SMBs. See the following example:

Bank charges \$50 per account per month fee for validation

X Client has 500 accounts to verify

\$25,000 cost per month to the client

Positive pay from REPAY validates checks without high fees.

••• **Secure Data Storage:** Compliance and regulatory changes can be difficult to keep up with.

Store data off your server and on REPAY's, where we use the following mechanisms to protect every payment.

- Gateways
- Tokenization
- Encryption
- Firewalls
- AVS / CVV
- And more!

••• **Permission Control & Separation of Duties:** Not every payment platform can support custom permissions. When it comes to access and approvals of sensitive data such as payment information, it is never a good idea to put the responsibility on one person.

REPAY's secure platform lets you:

- Set up permission hierarchies
- Enable "dual control"
- Implement contingency plans



Protect Every Payment with REPAY

As fraudsters become more sophisticated, businesses don't need to worry about falling behind. Don't let cost concerns, headcount or technology restrictions prevent you from protecting data.

From ACH and check fraud to invoice spoofs and compromised data, REPAY's secure solutions – mentioned in the above section – arm you against attacks.

Our [automation platform](#) simplifies the vendor payment experience for more efficient and better protected payments.

- Reduce risk using virtual cards
- Approve payments from anywhere
- Track transactions in real time
- Dedicated vendor enablement team

Schedule a demo today!



REPAY[®]

Realtime Electronic Payments

repay.com • info@repay.com