MUTUAL FEDERAL
A division of First Bank Richmond
epcor
Electronic Payments Core of Knowledge

# PAYMENTS INSIDER

*The inside scoop on payments for businesses of all sizes*

**INSIDE THIS ISSUE**



## The Perks of Positive Pay: Safeguarding Your Business Against Check Fraud

***by Trevor Witchey, AAP, NCP, Senior Director, Payments Education, EPCOR***

In an era when digital payment methods are gaining popularity, traditional check payments still dominate business transactions. However, the security risks associated with check transactions pose a significant concern for businesses that frequently utilize checks. The prevalence of checks provides an opportunity for fraudsters to create and pass counterfeit checks, resulting in substantial financial losses. As a responsible business owner, it is essential to take measures to protect your company from such criminal activities.

So, what can your financial institution do to help mitigate check fraud? Enter positive pay—a powerful tool that enhances the security of your check transactions. If you're unfamiliar with positive pay, it is a type of automated fraud detection technology designed to detect and prevent counterfeit checks. By leveraging this service, you can add an extra layer of security to safeguard your business. Reach out to your financial institution today to inquire if they offer positive pay services.

Positive pay operates through a meticulous examination of checks presented for payment,

comparing them against the initial company-issued checks. The system scrutinizes various check features, such as the amount, check number and payee name, to identify suspicious items or discrepancies.

There are several positive pay variations that can be employed. Let's explore some of them:

1. **Positive Pay**: This method automatically matches each check presented against a list of issued checks provided by the company. If any discrepancies arise, the system alerts the financial institution and the company.
2. **Payee Positive Pay:** This approach matches the payee names from an issue file to the payee names on the check. If there is any inconsistency, the system raises an alarm.
3. **Reverse Positive Pay:** In this scenario, the financial institution sends a file of presented checks to the company. The company then internally compares these checks to the items they have issued, detecting any potentially fraudulent transactions.

To shed light on the benefits of positive pay, let's explore a couple of real-life scenarios encountered by companies:

**Experience 1:** An ex-employee of a company utilized the account information at the bottom of their payroll check to create counterfeit checks. The ex-employee

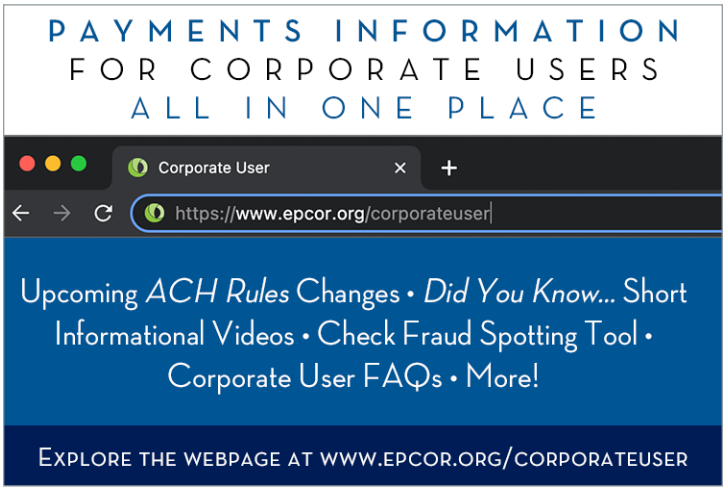
issued these counterfeit checks to various acquaintances who subsequently cashed them at multiple branches. Unfortunately, the company had not implemented the positive pay system offered by their financial institution, and it took them several months to discover the fraud. Total Company Loss: $3,261.27.

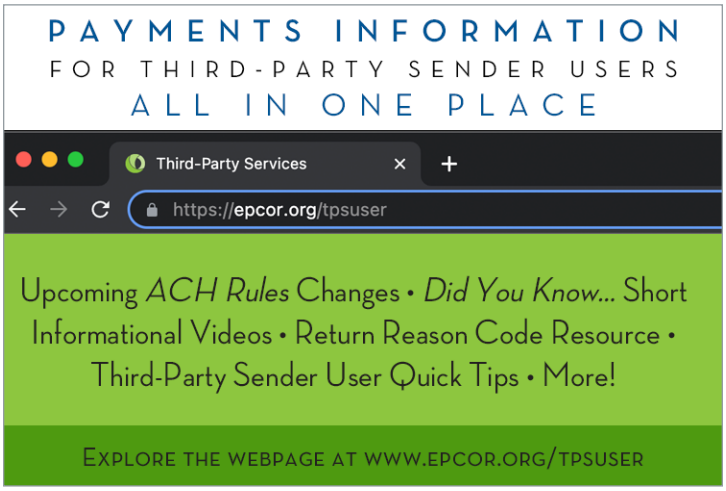
**Experience 2:** A business customer paid a vendor $3,000 for parts. However, the Accounts Receivable person left the check on their desk during their lunch break, allowing another employee of the vendor to record the MICR line information from the business customer's check. This unscrupulous employee then created counterfeit checks on the business customer's account to pay off their personal student loans and car loans, totaling $300,000. Fortunately, the business customer had wisely opted for the positive pay service provided by their financial institution. This service not only verified the dollar amount and check number but also cross-referenced the payee names. Consequently, when the counterfeit checks were presented for payment, they were promptly identified as fraudulent by the positive pay system. Their financial institution immediately contacted the business, and the counterfeit checks were returned as "counterfeit." Total (Potential) Loss: $300,000.00.

The second example vividly illustrates how the implementation of positive pay saved the business from significant financial loss. By utilizing positive pay, the business ensured advanced security for their check transactions. Although check fraud is not uncommon in the United States, companies that heavily rely on check payments can significantly mitigate risks by leveraging protective services like positive pay.

To ensure the effectiveness of your positive pay system and prevent or minimize losses, it is crucial for businesses to maintain accurate records of their check payments. By doing so, you can enhance the security of your transactions and instill peace of mind.

Take proactive steps today by reaching out to your financial institution to inquire about their positive pay service and determine whether its implementation is right for your business. Safeguard your company against check fraud and embrace the perks of positive pay.




# The Rise of Business Email Compromise: Protecting Your Business from Costly Scams

*by Emily Nelson, AAP, APRP, NCP, Manager, Payments Education, EPCOR*

In recent years, business email compromise (BEC) scams have become a significant threat to businesses worldwide. The Federal Bureau of Investigation (FBI) has issued a public service announcement warning about the increasing prevalence of BEC scams, revealing that the total value of redirected funds has exceeded a staggering $12 billion. This article aims to shed light on the evolving nature of BEC scams and their impact on various industries, providing valuable tips to safeguard businesses from falling victim to these costly frauds.

## The Growing Scope of BEC Scams

BEC scams have shown no discrimination, targeting businesses of all sizes, personal transactions and even global markets. Reports indicate that these scams have been documented in all 50 states of the United States and across 150 countries worldwide. It is a clear indication that the threat is widespread and affects businesses regardless of their location or scale of operation.

## Understanding How BEC Scams Happen

BEC scams can occur in different variations, but they all share the common goal of manipulating victims into transferring funds to fraudulent accounts.

Here are two common versions:

- **Version 1:** Scammers gain access to a legitimate account, often through malware or phishing attacks, and utilize it to conduct unauthorized transfers of funds or direct others within an organization to do so. For example, a fraudster may pose as the CEO and instruct the CFO to wire funds to an account immediately, claiming an urgent need for the transaction. In some cases, scammers create email domains that closely resemble legitimate business addresses to deceive recipients.
- **Version 2:** The fraudster assumes the identity of a legal entity and contacts a business, either through phone calls or emails, regarding an "important matter." Victims are often pressured into wiring money immediately and discreetly.

## Tactics and Red Flags

To protect your business from falling victim to BEC scams, it is crucial to be aware of common red flags indicating potentially fraudulent activities. These include:

- Exclusively email-based communication that seems urgent or out of the ordinary.
- Poorly crafted emails, incorrect email signatures or the use of formal language that is atypical for the sender.
- Transactions involving new vendors or contacts.
- Transfer requests made when senior officials are out of the office.
- Large fund transfers to unfamiliar recipients.
- Requests made near the end of the day, weekends or holidays.
- Funds being sent to personal accounts when the company typically only deals with business accounts.
- Receiving accounts with no prior history of large fund transfers.

## Protecting Your Business from BEC Scams

Mitigating the risks associated with BEC scams requires a proactive approach and robust security measures. Here are some tips to help safeguard your business:

- Establish a secondary means of communication for verification purposes, especially when dealing with urgent or suspicious requests.
- Implement a policy for identifying and reporting BEC and similar email scams within your organization.
- Exercise caution during phone conversations and avoid disclosing sensitive information.
- Verify any changes in payment type or location mentioned in legal documents before distributing funds.
- Educate your internal staff and key financial officers about the risks and characteristics of BEC scams.
- Implement filters at your email gateway to detect and block emails with known phishing indicators and consider blocking suspicious IP addresses at your firewall.
- In the event of discovering a fraudulent transfer, act swiftly by contacting your financial institution, reporting the incident to your local FBI office and filing a complaint at ic3.gov or bec.ic3.gov.

As the value of funds redirected through BEC scams continues to rise, it is vital for businesses to be proactive in protecting themselves from these fraudulent activities. By understanding the evolving tactics employed by scammers, recognizing red flags and implementing effective security measures, businesses can mitigate the risk of falling victim to BEC scams and safeguard their finances and reputation in an increasingly digital landscape. Stay vigilant and take the necessary steps to protect your business from the costly consequences of BEC scams.

# Why FedNow® Isn't a Payments App

***The following information originally appeared on July 10, 2023, on IndependentBanker.org. This an abbreviated version.***

Apple Pay, Cash App, FedNow®, PayPal, Venmo, Zelle and more. These solutions have become household names, creating an alphabet soup of desired faster payments functionality for consumers and businesses alike.

In fact, the Federal Reserve reports that 83% of consumers use payment apps or digital wallets at least occasionally, and nearly two-thirds of businesses indicate they would factor access to faster payments into future decisions on whether to switch financial institutions.

To respond to this interest in faster payments, community banks are working them into product plans and offerings with increasing urgency. Research supports this observation: The 2023 Faster Payments Barometer from the U.S. Faster Payments Council found 88% of organizations plan to introduce FedNow® by 2025, and 77% have implemented or are in the process with Zelle today.

## One of These is Not Like the Others

While each of these solutions provides a faster payments experience, one of them distinguishes itself by the nature of what it is: FedNow®. It's the only one on the list at the start of this article that is a payments rail unto itself.

"It is so infrequent that new infrastructure or payment rails are created to move money that it is only natural to think of interfaces that might feel similar," says Kari Mitchum, Vice President of Payments Policy at ICBA. "But FedNow® is not going to be like Apple Pay. FedNow® is not an app."

In fact, when it comes to instant payments, the only comparable solution on the market today is the Real Time Payments Network (RTP®) from The Clearing House. Having launched just over five years ago, it offers a similar real-time payments infrastructure as a foundational rail.

## Combating FedNow® Confusion

But as one of only two new payments systems to launch in more than 40 years, FedNow® as an infrastructure payment type can be a difficult concept to grasp. Add to that the confusion that emerges because faster payments have become a hot market commodity, and misinformation can feed into that lack of clarity.

"In April, we had presidential candidates, media personalities and podcasters talking about FedNow® and creating additional confusion about what FedNow® is and what FedNow® isn't," Mitchum says. "We were hearing from our financial institutions with questions on how they should talk to their customers, and ICBA pulled together some FAQs. I expect that to continue as consumers become more aware of FedNow® happening in their financial institutions."

"When people think of new payment capabilities today, they naturally think of the end-user experience and apps, not underlying technology or networks," summarizes Nick Denning, Senior Vice President of Payments Industry Relations at ICBA Bancard. "It's easy to mistake instant wallet transfers for instant bank transfer payments, but they are very different."

## The FedNow® Difference

So, what sets FedNow® apart? At a high level, three key attributes differentiate it from app-based solutions:

### 1. FedNow® is a payments rail.

Perhaps the most straightforward way to distinguish FedNow® from app-based solutions is to consider it as a complement to existing payments rails: ACH, check, credit and debit cards, RTP® and wire. In short, FedNow® offers a backbone for payments to flow.

To draw a parallel, Denning likens payments rails, including FedNow®, to the operating systems iOS and Android. In this scenario, the underlying operating system fuels the functionality of the mobile device, just as the payments rail enables money movement. Carrying the analogy further, Zelle, Venmo and others act like the apps that are deployed on mobile devices, using the operating system infrastructure to perform distinct tasks.

"The operating system would be the network level [ACH, card, RTP®, FedNow®], and then all of the apps [Zelle, Venmo, etc.] are riding on top of that operating system," Denning says.

### 2. FedNow® does not offer a customer-facing solution.

As the background payments rail, FedNow® will integrate with existing customer-facing offerings, such as a financial institution's own digital or mobile app or new solutions designed around new experiences or use cases.

"FedNow® does not have a user interface that financial institution operations staff or their customers will be using," Denning says.

### 3. FedNow® has the potential to support a wide variety of transactions.

While payments apps like Venmo and Zelle are expanding their scopes into more than person-to-person (P2P) payments, they still don't offer the full range of instant payments functionality a payments rail provides.

Consider possible FedNow® use cases like early wage access, payroll, disbursements, bill pay, account-to-account (A2A) transfers, real estate settlements and so much more. The instant payments rail opens up a wide variety of potential development opportunities for strengthening the payments landscape.

If you're interested in FedNow®, reach out to your financial institution.

*Source: Independent Banker*

# Exchange Framework Validated for E-remittance Information

***The following article originally appeared on FedPaymentsImprovement.org.***

A key step in the business-to-business (B2B) payments process is the retrieval and reconciliation of the remittance information, or the details that describe what is being paid, with the payment and the order status in the accounts receivable system. Today, this is a largely manual and time-consuming process, involving emails and/or portals.

The Business Payments Coalition (BPC) and Federal Reserve have been collaborating with industry experts on a work effort to solve for this challenge and modernize the exchange of electronic remittance (e-remittance) information using an exchange framework ecosystem. An exchange framework is an electronic delivery network based on a set of technical standards and policies that allows businesses to securely share electronic supply chain documents with one another.

As a result of this collaboration, the Remittance Delivery Work Group completed a validation phase in the summer of 2023, where they successfully demonstrated it is operationally feasible for an exchange framework to cost-effectively deliver e-remittance information. The work group published their findings in the *Remittance Delivery Validation Report.*

To reach this current validation phase, the industry had to first understand whether it is possible to establish an e-remittance ecosystem on an exchange framework.

## Feasibility Assessment Phase: Is an Exchange Framework Feasible for Delivering E-remittance Information?

In September 2021, more than 40 industry organizations joined the Remittance Delivery Assessment Work Group where they unanimously determined it is feasible to establish a remittance exchange framework, similar to the e-invoice exchange framework, with some minor adaptations. Work group participants found the exchange framework provides a standard, secure way to deliver e-remittance information that will minimize the need for businesses to make changes to their account payable and account receivable systems.

With feasibility established, an immediate next step for the work was identified: proceed to a validation phase and test the framework's operational abilities for e-remittance exchange. Many participants from the Remittance Delivery Assessment Work Group progressed to this validation phase, inspired by the vision of a modern remittance delivery system.

## Validation Phase: Can an Exchange Framework Deliver E-remittance Information?

Early in the validation phase, work group members voted to use the E-invoice Exchange Market Pilot's exchange framework infrastructure, which is now overseen by the Digital Business Networks Alliance. This electronic exchange framework became available for use by all businesses to exchange electronic invoices in early summer 2023, following the successful completion of the BPC's E-invoice Exchange Market Pilot.

Through extensive validation testing, the work group participants demonstrated an exchange framework can both facilitate the exchange of e-remittance information and enable straight-through processing, regardless of accounting system used. This is a major breakthrough as it moves the industry closer to a completely automated payments process from start to finish.

The successful testing confirmed an exchange framework can help businesses of all of sizes implement consistent cash application processes for all payment types, while minimizing changes to accounting systems. Further, the exchange framework will also help reduce exceptions because it standardizes remittance information. This will greatly lessen the current manual processes involved with the exchange of remittance information between businesses.

The success of the validation phase increases industry confidence that an exchange framework can support both the sending and receiving of e-remittance information. This has the potential to greatly improve the efficiency of B2B payments and enhance the end-to-end value proposition for electronic B2B payments.

## Upcoming Pilot Phase: What's Next for E-remittance?

With the validation phase now complete, the work group unanimously recommends moving to a pilot phase using the DBNAlliance's exchange framework. This pilot will build on the momentum of the validation phase and focus on the following:

- Piloting a fully operational exchange framework.
- Finalizing the ISO 20022 remittance data model.
- Preparing for the establishment of a production remittance exchange framework.

At the recommendation of the work group, the BPC, with support from the Fed, will proceed with facilitating an E-remittance Exchange Pilot supporting all electronic B2B payment methods. This pilot phase will be the final test before market adoption of an exchange framework for e-remittance information.

*Source: The Federal Reserve*

epcor®

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

**The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.**


www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665