THE INFORMER

Quarterly Newsletter for INSOUTH's Business Customers

2nd Quarter

INSOUTH BANK Member FDIC

www.insouth.com

Member FDIC

EQUAL HOUSING LENDER

Bank Holiday Schedule

Juneteenth
Closed
Friday, June 19th

Labor Day
Closed
Monday, September 7th

Need assistance? Call us!

Millington: (901) 872-4545
Atoka: (901) 837-9675
Covington: (901) 476-3330
Brownsville: (731) 772-1201
Memphis: (901) 747-5555
Jackson: (731) 574-2500
Electronic Banking: (866) 348-3614
Debit Card Support: (800) 541-3891
Fraud Prevention Services: (877) 253-8964

INSOUTH Bank is your business partner. If you would like for us to meet with you or your employees to discuss how to protect your money and your information, please do not hesitate to contact us!

IS YOUR BUSINESS ACCOUNT WORKING AS HARD AS YOU ARE?

INSOUTH Bank offers complete treasury solutions to help you protect, manage and grow your business with confidence with our local, dedicated support team. Your business never stops, and neither should your banking. Our Treasury Management Solutions combine Business Checking, Merchant Services, and Positive Pay fraud protection into one seamless, secure platform. Optimize and fuel growth with flexible Lines of Credit* designed Just Right for You and your business.

Self-Service Fraud Protection with Positive Pay & ACH Reporting
Now Offering This Service FREE

- Help business and commercial clients protect their accounts from check fraud.
- Deliver an easy way for business and commercial check writers to review and decision checks.
- Notify commercial ACH Originators of Returns and Notifications of Change in readable reporting formats.
- Verify outgoing ACH credit entries before they are sent to ensure funds are only disbursed to authorized Receivers.
- Provide visibility and insights into incoming and outgoing payments, exceptions, & reporting.
- Add an extra layer of security to Check Positive Pay by confirming the payee name on the presented check matches.

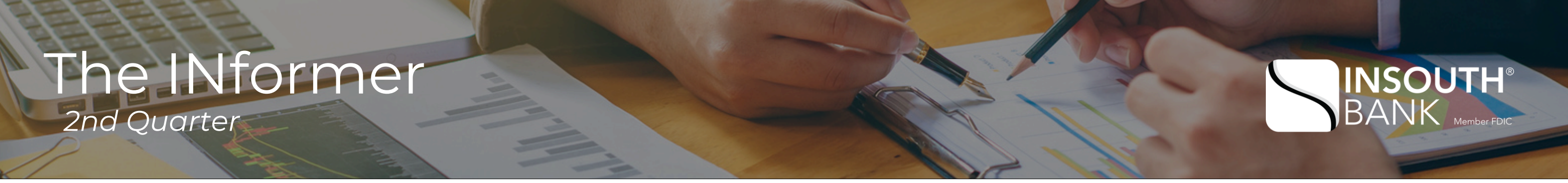
Fraud Protection - Protection That Goes Further

- ACH blocks and transaction filters
- User controls and dual approvals
- Real-time alerts & transaction monitoring
- Fast exception decisioning tools

Cash Management - Know Exactly Where Your Cash Stands

- Manage multiple accounts with ease
- ACH origination (payroll, vendors, collections)
- Custom reporting/QuickBooks export
- Access real-time insights anytime, anywhere

NMLS 400032. *All loans are subject to credit and/or collateral approval.



Fraud Prevention for Small Businesses

If you run a small business, you know how important it is to pay your bills. Scammers know this too and send fake invoices to businesses for products or services they never ordered in the hopes they'll pay up. Invoice fraud happens when scammers impersonate legitimate vendors or executives to trick your business into paying fake invoices or diverting legitimate payments to fraudulent accounts. The lure of large transactions makes invoice fraud very appealing to attackers. According to a 2021 FBI Report, successful business email compromise (BEC) scams (such as invoice fraud) accounted for an average loss of more than $120,000 per incident. These invoice scams cost organizations more than $2.4 billion in 2021.

These scams often start when you or someone on your staff gets an unexpected or unfamiliar invoice in the mail. It bills your company for things you didn't order, maybe tech support, domain registration, or search engine optimization services. The invoice might look legitimate and appear to come from a well-known company, or the sender might claim to be from a company you've never heard of before. Adding to the confusion and urgency, some invoices arrive with a "past due" notice. Scammers want your money, and they hope the person handling your company's finances will just pay the invoice by following the sender's instructions. Scammers also sometimes email you fake invoices, but it's really a phishing scam designed to get access to your business's data and networks.

Invoice fraud can come from a fake or a hijacked vendor account. Common tactics may include:

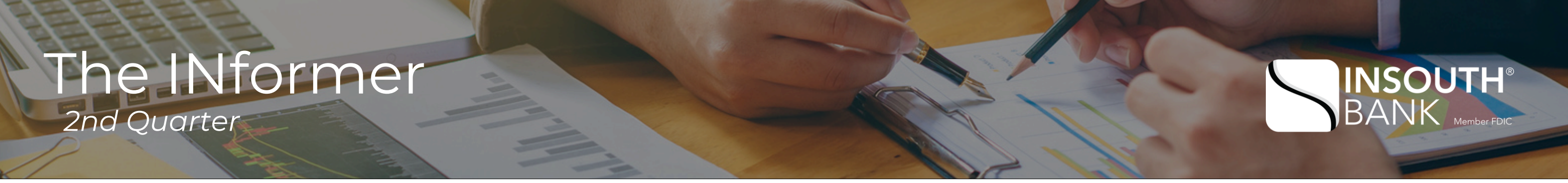
- Account takeovers - Attackers hijack an employee (e.g., accounts payable representative) account to gain access to all clients, vendors, transactions, invoices, and banking information. They use this compromised account to email clients and vendors with new payment details and fake invoices.
- Fake invoices - Attackers mimic a vendor's branding, language, email- and signature-templates they use to generate an invoice.
- Vendor impersonation - Attackers impersonate a legitimate vendor's domain and send an invoice that looks like a valid transaction request.
- Vendor fraud - Vendors that actually perform work for your business may send a duplicate invoice or change the payment amounts, hoping that busy accounting departments don't notice.

Do you know what Positive Pay is?

Check fraud continues to be one of the fastest-growing threats facing businesses today. Even with the increase in electronic payments, criminals are still targeting businesses through stolen, counterfeit, and altered checks. One of the most effective tools available to help protect your business is Positive Pay. Positive Pay is a fraud prevention service that matches checks presented for payment against a list of checks your business has issued. When you issue checks, you provide the bank with information such as the check number, amount, and issue date. As checks are presented for payment, that information is compared to your issued check file. If a check does not match, it is flagged for your review before it is paid. For example, if your business issues a check for $500 and a fraudster alters the amount to $5,000, Positive Pay can identify the discrepancy and allow you to decide whether the item should be paid or returned.

Fraudsters are becoming more sophisticated every day. Taking proactive steps now can help protect your business from costly losses later. If your business writes checks, Positive Pay may be worth considering as part of your overall fraud prevention strategy.

Information provided from: https://consumer.ftc.gov/consumer-alerts/2026/05/run-small-business-pay-your-bills-not-scammers & https://ironscales.com/glossary/invoice-fraud



Is Positive Pay a Good Fit for Your Business?

Positive Pay may be a valuable tool if your business:

- Issues checks regularly
- Has multiple employees authorized to write checks
- Pays vendors by check
- Maintains higher account balances
- Wants an added layer of protection against fraud
- Does not have time to manually monitor every check transaction

What Is Check Washing and How Can You Protect Your Business?

While digital fraud often makes headlines, check fraud remains a significant threat to businesses and consumers. One of the most common forms of check fraud is check washing. Check washing occurs when criminals steal a legitimate check and use chemicals to remove the ink, allowing them to alter the payee, amount, or both. The check is then deposited or cashed, often before the account owner realizes it has been compromised. For example, a business may issue a check for $250 to a vendor. After being stolen, the check is "washed" and rewritten for $2,500 payable to someone else. If not caught in time, the altered check could clear the account.

Even businesses that issue only a moderate number of checks can benefit from the peace of mind Positive Pay provides.

Benefits of Positive Pay:

✔️ Helps detect counterfeit and altered checks
✔️ Reduces the risk of fraud losses
✔️ Provides an additional layer of account security
✔️ Allows you to review suspicious items before payment
✔️ Helps protect your business's finances and reputation

How to Protect Your Business

- Use Electronic Payments When Possible. ACH payments, online bill pay, and other electronic payment methods reduce the number of paper checks that can be intercepted and altered.
- Avoid Leaving Outgoing Mail Unsecured. Instead of placing checks in an unsecured mailbox, consider dropping them off inside a post office or handing them directly to a postal employee.
- Use Permanent Gel Ink Pens. Gel ink is more difficult for criminals to remove than standard ballpoint ink, making checks harder to alter.
- Monitor Your Accounts Regularly. Review transactions frequently and report suspicious activity immediately. The sooner fraud is identified, the better the chance of minimizing losses.
- Consider Positive Pay. Positive Pay compares checks presented for payment against checks your business has issued. If information such as the check number or amount doesn't match, the item is flagged for review before payment is made.
- Reconcile Accounts Promptly. Regular account reconciliation helps identify unauthorized or altered checks before additional fraud occurs.

Additionally, here are some common red flags to recognize in order to prevent business email compromise:

- Urgent requests for wire transfers or ACH payments
- Vendor payment change requests
- Slightly altered email addresses
- Requests to change employee direct deposit information
- Emails creating a sense of urgency or secrecy

SCAM ALERT

URGENT PHISHING ALERT

Fake "automatic credit limit exceeded" emails are targeting business checking accounts.

We're warning you about phishing emails currently being sent to INSOUTH Bank business customers. These emails claim that the automatic credit limit on your checking account, or the total amount allowed to be originated for the day, has been exceeded — often citing a specific dollar amount to create urgency.

These messages are designed to look like routine account or ACH notifications, often signed with addresses that resemble payment processors. They are not from INSOUTH Bank, and any link they contain should not be clicked.

WARNING SIGNS TO WATCH FOR

- **Urgent "credit limit exceeded" language**, often referencing a specific dollar figure for ACH origination or daily credit totals.
- **Sender addresses that don't match INSOUTH Bank**, including ones that look like they belong to a payment processor or third-party system.
- **Links to an unfamiliar "secure portal,"** sometimes with instructions to copy and paste the link if it doesn't open — INSOUTH Bank will never ask you to do this.

What to do right now

1. **Don't click any links** in the email, and don't reply to the sender.
2. **Don't copy or paste the link** into any browser.
3. **Delete the email.**
4. **Verify account activity directly** by logging into online banking or your treasury management portal, not through any link from an email.

Example of this scam email & text message — do not tap any links:

The credit total allowed to be originated today has been exceeded by $215,000.55

Thank you,
ACH_NOR_6@fiserv.com

INSOUTH Bank:

To review the check payment that was initiated, please access the secure portal provided. The portal will allow you to view real-time alerts and updates related to your banking account.

https://websecureinsouthbank.secure-s529i.com/258

Please note, if there's any trouble with going to secure portal please copy & paste portal on mobile browser.

If anyone on your team has already clicked a link or entered credentials, contact us immediately so we can help secure your account.

Call us now: 866-348-3614
This is our trusted, official number — save it to your contacts. Our Customer Service email is customer.service@insouth.com.