CHECK$ and BALANCE$

Quarterly Newsletter

Legence Bank

What's Inside:

POSITIVE PAY

Get ahead of fraud with Smart POSITIVE PAY! This amazing service allows you to easily and quickly verify checks that have cleared your account with Legence Bank, ensuring they are checks you have written.

FEATURES OF SMART POSITIVE PAY

- Accessible within Smart Cash Management
- Easily configure and upload check files from your current accounting/check printing software
- Receive notifications if checks don't match checks you have written
- Quick and simple notifications to Legence Bank to return items that you didn't write
- Easily identify and mark any checks that were valid written checks, but did not process properly

UPCOMING HOLIDAYS

Columbus Day
All locations will be closed **Monday, October 9** in observance.

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

by 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 Legence Bank 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 Legence Bank to inquire about 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 and components offered. 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.

To shed light on the benefits of positive pay, let's explore a couple of real-life scenarios encountered by one of EPCOR's financial institution members:

Experience 1: An ex-employee of a company utilized the account information at the bottom of their payroll check to create fraudulent or 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, during lunch break, the Accounts Receivable person left the check on their desk, 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. Fortunately, the business customer had wisely opted for the Positive Pay service provided by XYZ Bank. 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. XYZ Bank immediately contacted the business, and the counterfeit checks were returned as "counterfeit." Total (Potential) Loss: $300,000

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 bank transactions and instill peace of mind.
Take proactive steps today by reaching out to Legence Bank to inquire about positive pay and determine whether its implementation is right for your business. Safeguard your company against check fraud and embrace the perks of positive pay.

The Check's in the Mail... Or Is It?

by Marcy Cauthon
AAP, APRP. NCP, Senior Director, On-Demand Education, EPCOR

How many of us have ever put an outgoing bill/invoice in our home/business mailbox or a blue U.S. Postal mailbox? It is true that Americans have decreased their use of check payments, however; cases of check fraud continue to soar. Criminals are targeting USPS blue collection boxes, unsecured residential mailboxes, privately owned cluster box units at apartment complexes and highdensity commercial buildings to gain access to funds to perpetrate a scam.

After stealing checks from a mailbox, fraudsters will alter or "wash" the check, replacing the Payee name with a fraudulent consumer or business name and deposit the checks into fraudulent accounts they have set up. They often will wash and alter the amount of the check as well. Fraudsters have also gotten crazy at stealing business checks and creating authentic-looking counterfeit checks that are utilizing real account and routing numbers but are deposited using fake identities.

Well, there are numerous ways checks may be deposited in today's environment that give immediate availability but have less monitoring, such as image-enabled ATMs and remote deposit capture.

What can consumers and businesses do to combat this type of fraud?

Be vigilant in reviewing your transactions online with your financial institution daily if not more often.

Why is remaining vigilant so important?

Financial institutions only have a 24-hour window to return a check after it has been posted to your account. That is a very quick turnaround. Outside of that timeframe, your Financial institution may be able to deal directly with the depositing Financial institution to try and recover funds for altered checks or forged endorsements. With the number of these claims flowing through the financial system today, it could take months up to a year to get the issue resolved, but it is not guaranteed that funds will be reimbursed. Reviewing your transactions daily is imperative, especially if you are a business that has had your checks counterfeited. Again, your financial institution only has 24 hours from when the item posts to your account to get it returned. Your financial institution will have a timeframe specified within their deposit agreement of how long they give you to review your account statement and report that an item is altered or counterfeit. It is important that your business is aware of that timeframe, as the loss could fall on you if you don't notify your financial institution in a timely manner.

Another major issue that could impact your organization is when a check payment sent to you by your client is intercepted by a fraudster. This scam causes issues for the business and the consumer. The consumer believes they paid their bill/invoice on time, and the business is sending out late notices as they never received the payment. My advice to your business in this situation is to work with your consumer to resolve the error. The consumer will need to contact their financial institution and notify them that the check cleared their account but that the named Payee (your business) didn't receive the funds as intended. The financial institution will then need to file a claim to the depositing financial institution on the consumer's behalf, which often requires a written statement from your business stating you never received the funds.

The Financial Crimes Enforcement Network (FinCEN) issued an alert earlier this year to financial institutions with tips on how to detect, prevent and report suspicious activity associated with mail theft-related check fraud. Some of the red flags that financial institutions are looking for are:

1. Non-characteristic large check withdrawals on accounts with a new Payee.
2. Account holder claims a check they put in the mail was never received by the recipient, however; the check cleared their account.
3. Checks clearing on accounts appear to be a different color or not within the check range of other checks issued.
4. Account holders with no history of check deposits start experiencing large check deposits followed by a rapid withdrawal or transfer of funds.
5. Checks have appeared to have been washed using chemicals and Payee and/or amounts have been altered.

Combatting this type of fraud begins with account holders being diligent in reviewing their account history via their institution's online banking or utilizing a positive pay service that your institution may be offering to your business. If you have any questions about your responsibilities as an organization, contact your financial institution.

Fast, Faster or Instant: What's Your Payment Preference?

by Shelly Sipple
AAP, APRP, NCP, Senior Director, Certi cations & Continuing Education, EPCOR

When it comes to making a payment, a payment is a payment is a payment, right? Yes, in the sense that a consumer or business intends to pay for goods or services. And while your financial institution likely offers a variety of options, how might your organization choose one payment means over another? Perhaps one consideration is whether your organization wants to fund the purchase out of current income or with borrowed funds. Some other reasons may include ease of use, familiarity, convenience and cost. Or your organization may prefer to use a payment method that is safe and secure or universally accepted. However, in today's ever-changing (and rapidly) payments ecosystem, consumers and businesses may also make the decision based on how quickly the payment needs to be in the payee's account—fast, faster or instantly. But what payment options are considered fast? Faster? Instant? Cash would be considered fast when compared to bartering as are checks, debit cards and next-day ACH. However, Same Day ACH and wire transfers fall into the faster category. And that leaves RTP® and FedNowSM, which are instant payments. While fast payment options are good and still serve a purpose, faster and instant payments are what many organizations are interested in these days. So, let's further define them!

Faster Payments
With faster payments, a payee's deposit account is credited or debited a few hours after a payment order has been initiated. Same Day ACH allows credit and debit payments to be originated, processed and settled all on the same day. Same Day ACH payments are accumulated throughout the day and then offset against each other, with only the net differential transferred between financial institutions (known as deferred net settlement). A wire transfer is also a faster payment; however, individual transactions settle as they are processed (known as real-time gross settlement). Both Same Day ACH and wires may only be processed during certain hours Monday through Friday, excluding federal holidays. This is one key feature that keeps them from being instant payments.

Instant Payments
With instant payments, clearing and settlement occur in real-time for each individual credit transaction, and funds can be sent and received around the clock, any day of the year. fee transfer of funds between the payer and payee's accounts at financial institutions occurs within seconds and funds are final and irrevocable. RTP®, which was implemented November 2017, and FedNowSM, which goes live July 2023, are examples of instant payments. RTP® and FedNowSM are different from ACH in the fact that the systems operate on a 24/7/365 basis. Gone are the constraints of normal banking hours. Along with a completely wide-open timeframe, RTP® currently can be, and FedNowSM will be, utilized by consumers, businesses and financial institutions. Anyone anywhere can participate in instant payments (as long as they have connection to the given network). These benefits of speed, convenience an accessibility are what set RTP® and FedNowSM apart from traditional payment methods. Interested in utilizing some form of faster or instant payments at your organization? Reach out to your financial institution to learn more and discuss your options.

Meet Our Team

Matt Simmons
Business Services Manager

Office: (618) 658-3249
Cell: (618) 841-0513
Office Fax: (618) 658-1613
Toll Free: (800) 360-8044 (3249)
Email: msimmons@legencebank.com

Sean Lasley
Business Services
Relationship Specialist

Office: (618) 998-4168
Cell: (618) 841-2019
Office Fax: (618) 969-8307
Toll Free: (800) 360-8044 (3249)
Email: slasley@legencebank.com

Allison Browning
Business Services Representative

Office: (618) 658-3249
Office Fax: (618) 658-1613
Toll Free: (800) 360-8044 (3249)
Email: abrowning@legencebank.com

Niky Navarro-Gamboa
Business Services
Administrative Specialist

Office: (618) 524-6743
Office Fax: (618) 519-9194
Toll Free: (800) 360-8044 (3249)
Email: nnavarro-gamboa@legencebank.com