Meadows Bank eNewsletter

Volume Issue • June 2020

In This Issue:

Recent Uptick in Check Fraud - Help Protect Your Accounts

With a recent uptick in fraud, especially counterfeit checks, we wanted to share some of the measures we take to help prevent fraud as well as some services you can take advantage of to better protect your accounts. We realize that these measures may seem intrusive and at times irksome, but please remember that it is all done for the safety of your business.

Below are a couple measures we take to protect your accounts against fraud:

- On all wire transfers, whether initiated online, through email or fax, a member of our team will call our client to verify the validity of the wire transfer, amount and to whom it is made payable.
- On large checks presented at one of our branches to be cashed, a member of our team will call our client to assist in identifying fraud and unauthorized transactions.

Below are a couple measures you can take advantage of to protect your accounts used for your accounts payable:

- Maintain control of your outgoing mail until in the hands of the USPS. Remind your vendors to maintain control of the receipt of their mail. Much of the recent fraud is due to the break-in of mailboxes, whether individual of community mailboxes.
- Take advantage of our Positive Pay service.

What is Positive Pay?

Positive Pay is a fraud prevention tool for business customers attached to our Treasury Management Online Banking System. It assists in the prevention of fraud by adding a layer of protection against forged, altered, counterfeit and unauthorized checks.

How does it work?

When a check is presented for payment against your account, that item is automatically run through our Positive Pay system to compare the account number, check number, issued date and dollar amount against a list of items you have issued and provided to the bank. If the check being presented is not included on the list of items you have given to us, it is automatically flagged by our system as an “exception” and you will be alerted through a computer generated notification sent to you by our Treasury Management System. Upon receiving this notification, you will log in to your Treasury Management dashboard to review the item and determine whether the bank should allow it to be paid, or if it should be returned. Upon making your decision, our system will either honor the item and allow it to be cashed, or return the item per your instructions.

How does the bank know which checks are issued by me?

You or a member of your company will upload a list of your authorized checks directly through your Meadows Bank Treasury Management portal. This is the file our system will check any items presented for payment against. Most accounting software is capable of creating a compatible file that can be uploaded into our system with no additional work on your part; the majority of our Positive Pay customers upload their files from the same file that they use to issue their checks. If you do not use any outside software to manage your check register, we also offer the ability to manually input your issued checks directly into our system.

How can I sign up for Positive Pay?

Inform your Account Officer, a member of your local branch or your Relationship Manager that you’re interested in learning more about Positive Pay and we’ll take it from there! A member of our team will reach out to you to discuss the product, and answer any questions you may have. If you determine that Positive Pay would be beneficial to you and your company, we will assist you with getting the proper agreements signed, setting up the system for you and providing training to you and your staff on how to use Positive Pay.

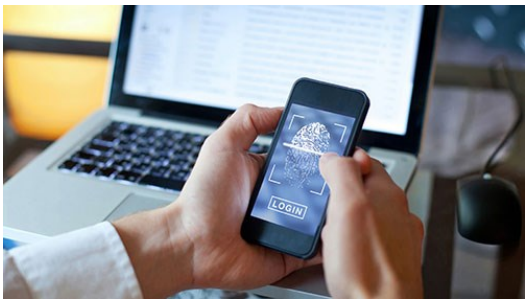
REAL ID and Employee Verification

What the REAL ID is and how it relates to your small business

If your employees regularly enter federal buildings or use air travel, you'll need to make sure that they're carrying up-to-date REAL ID cards — otherwise, they'll be turned away from security checkpoints. Here's what you need to know to determine whether your employees need to obtain REAL IDs, when they should do so and whether or not you can use REAL IDs to verify their I-9 eligibility.

What is a REAL ID?

According to the Department of Homeland Security, the REAL ID originated with the REAL ID Act, which Congress passed back in 2005 based on the 9/11 Commission's recommendation. This legislation gave the federal government permission to "set standards for the issuance of sources of identification, such as driver's licenses."



When will the government enforce REAL IDs?

October 1, 2021 is the enforcement date for REAL ID, as the DHS confirms. While the REAL ID is not required, employees will need to obtain one if they plan on flying domestically, purchasing firearms and ammunition or setting foot on a military base or federal facility after this date.

If a person doesn't have a REAL ID and needs to travel via plane, they'll have to show TSA an alternative acceptable document such as a passport, passport card or state-issued Enhanced Driver's License. If an employee doesn't have a REAL ID or one of these alternative acceptable documents, TSA has the right to prohibit them from passing through security and boarding the flight. Head to the DHS website, for more information about the REAL ID and to browse the list of TSA Acceptable Documents.

How do employees get a REAL ID?

If some of your staff travel frequently for work, encourage them to obtain a REAL ID. This will prevent any delays or sabotaged travel plans for your business, which can result in a loss of time and money.

To obtain a REAL ID, the employee will need to check out their state's driver's licensing agency website to find out what documents to bring with them when they visit their local DMV office in person. According to the DHS, the minimum documentation they'll need must prove the following: social security number, date of birth, full legal name, lawful status and two proofs of address of principal residence.

Can REAL ID be used to verify employees' I-9 eligibility?

Some have suggested that because REAL ID requires two forms of documentation, it's a valid List A document that your business can use for I-9 purposes. Per Jennifer Jacobus PHRca, SHRM-CP, SDEA Director of HR Services, you won't be able to use the REAL ID in this way. However, an employee can use the REAL ID as an acceptable List B document for employee verification.

Even though you can't use an employee's REAL ID as a List A document, it's still a useful item for them to obtain. By encouraging staff members who travel frequently to obtain a REAL ID sometime before October 1, 2021, you're one step closer to ensuring that future work trips are smooth and successful.

PPP Flexibility Act - Update to Borrowers

Paycheck Protection Program (PPP) Flexibility Act*

The President signed the above Act into law on June 8, 2020. The Act provides additional flexibility in the PPP program for borrowers. Many of the provisions in this Act will make it easier for businesses to achieve the requirements for loan forgiveness.

- Extend the covered period for loan forgiveness from eight weeks after the date of loan disbursement to 24 weeks after the date of loan disbursement, providing substantially greater flexibility for borrowers to qualify for loan forgiveness. Borrowers who have already received PPP loans retain the option to use an eight-week covered period.
- Lower the requirements that 75 percent of a borrower's loan proceeds must be used for payroll costs and that 75 percent of the loan forgiveness amount must have been spent on payroll costs during the 24-week loan forgiveness covered period to 60 percent for each of these requirements. If a borrower uses less than 60 percent of the loan amount for payroll costs during the forgiveness covered period, the borrower will continue to be eligible for partial loan forgiveness, subject to at least 60 percent of the loan forgiveness amount having been used for payroll costs.
- Provide a safe harbor from reductions in loan forgiveness based on reductions in full-time equivalent employees for borrowers that are unable to return to the same level of business activity the business was operating at before February 15, 2020, due to compliance with requirements or guidance issued between March 1, 2020 and December 31, 2020 by the Secretary of Health and Human Services, the Director of the Centers for Disease Control and Prevention, or the Occupational Safety and Health Administration, related to worker or customer safety requirements related to COVID–19.
- Provide a safe harbor from reductions in loan forgiveness based on reductions in full-time equivalent employees, to provide protections for borrowers that are both unable to rehire individuals who were employees of the borrower on February 15, 2020, and unable to hire similarly qualified employees for unfilled positions by December 31, 2020.
- Increase to five years the maturity of PPP loans that are approved by SBA (based on the date SBA assigns a loan number) on or after June 5, 2020.
- Extend the deferral period for borrower payments of principal, interest, and fees on PPP loans to the date that SBA remits the borrower's loan forgiveness amount to the lender (or, if the borrower does not apply for loan forgiveness, 10 months after the end of the borrower's loan forgiveness covered period).
- In addition, the new rules will confirm that June 30, 2020, remains the last date on which a PPP loan application can be approved.

SBA, in consultation with Treasury, will promptly issue rules and guidance, a modified borrower application form, and a modified loan forgiveness application implementing these legislative amendments to the PPP.

*Excerpts from the SBA Press Release

For additional information and other updates related to the COVID-19 pandemic and banking operations, please visit our website at www.meadowsbank.bank

Mobile Banking App Exploitation

Let's start this article by letting you know that you can find a link to our official mobile banking app on the homepage of our website.

Now to the FBI's alert.

As the public increases its use of mobile banking apps, partially due to increased time at home, the FBI anticipates cyber actors will exploit these platforms. Americans are increasingly using their mobile devices to conduct banking activities such as cashing checks and transferring funds. US financial technology providers estimate more than 75 percent of Americans used mobile banking in some form in 2019.

Studies of US financial data indicate a 50 percent surge in mobile banking since the beginning of 2020. Additionally, studies indicate 36 percent of Americans plan to use mobile tools to conduct banking activities, and 20 percent plan to visit branch locations less often. With city, state, and local governments urging or mandating social distancing, Americans have become more willing to use mobile banking as an alternative to physically visiting branch locations. The FBI expects cyber actors to attempt to exploit new mobile banking customers using a variety of techniques, including app-based banking trojans and fake banking apps.

App-Based Banking Trojans

The FBI advises the public to be cautious when downloading apps on smartphones and tablets, as some could be concealing malicious intent. Cyber actors target banking information using banking trojans, which are malicious programs that disguise themselves as other apps, such as games or tools. When the user launches a legitimate banking app, it triggers the previously downloaded trojan that has been lying dormant on their device. The trojan creates a false version of the bank's login page and overlays it on top of the legitimate app. Once the user enters their credentials into the false login page, the trojan passes the user to the real banking app login page so they do not realize they have been compromised.

Fake Banking Apps

Actors also create fraudulent apps designed to impersonate the real apps of major financial institutions, with the intent of tricking users into entering their login credentials. These apps provide an error message after the attempted login and will use smartphone permission requests to obtain and bypass security codes texted to users. US security research organizations report that in 2018, nearly 65,000 fake apps were detected on major app stores, making this one of the fastest growing sectors of smartphone-based fraud.

TIPS TO PROTECT YOU AND YOUR ORGANIZATION

Obtain Apps from Trusted Sources

Private sector companies manage app stores for smartphones and actively vet these apps for malicious content. Additionally, most major US banks will provide a link to their mobile app on their website. The FBI recommends only obtaining smartphone apps from trusted sources like official app stores or directly from bank websites.

Use Two-Factor Authentication

Since 2016, surveys of application and website users have identified that a majority of users do not enable two-factor authentication when prompted. These users cite inconvenience as the major reason to avoid the use of this technology. Cybersecurity experts have stressed that two-factor authentication is a highly effective tool to secure accounts against compromise, and enabling any form of two-factor authentication will be to the user's advantage

Do:

- Enable two-factor or multi-factor authentication on devices and accounts to protect them from malicious compromise.
- Use strong two-factor authentication if possible via biometrics, hardware tokens, or authentication apps.
- Use multiple types of authentication for accounts if possible. Layering different authentication standards is a stronger security option
- Monitor where your Personal Identifiable Information (PII) is stored and only share the most necessary information with financial institutions.

Don't:

- Click links in e-mails or text messages; ensure these messages come from the financial institution by double-checking e-mail details. Many criminals use legitimate-looking messages to trick users into giving up login details.
- Give two-factor passcodes to anyone over the phone or via text. Financial institutions will not ask you for these codes over the phone.

Use Strong Passwords and Good Password Security

Cyber actors regularly exploit users who reuse passwords or use common or insecure passwords. The FBI recommends creating strong, unique passwords to mitigate these attacks. The National Institute of Standards and Technology's most recent guidance encourages users to make passwords or passphrases that are 15 characters or longer.

Do:

- Use passwords that contain upper case letters, lower case letters, and symbols.
- Use a minimum of eight characters per password.
- Create unique passwords for banking apps.
- Use a password manager or password management service.

Don't:

- Use common passwords or phrases, such as "Password1!" or "123456."
- Reuse the same passwords for multiple accounts.
- Store passwords in written form or in an insecure phone app like a notepad.
- Give your password to anyone. Financial institutions will not ask you for this information over the phone or text message.

If a Banking App Appears Suspicious, Call the Bank

If you encounter an app that appears suspicious, exercise caution and contact that financial institution. Major financial institutions may ask for a banking PIN number, but will never ask for your username and password over the phone. Check your bank's policies regarding online and app account security. If the phone call seems suspicious, hang up and call the bank back at the customer service number posted on their website.

The Official Meadows Bank Mobile App

On the front page of our website we provide a link to the official stores (App Store and Google Play Store) where our official Meadows Bank Mobile App can be downloaded.

Electronic Banking Security Measures

We wanted to take a minute to highlight the security measures we utilize with our electronic banking products in order to protect you, our customers, from compromise.

Multi Factor Authentication

Multi Factor Authentication is an integral part of the Meadows Bank identity and access management process. MFA is a security mechanism in which individuals are authenticated through more than one validation procedure before being allowed to access a system or program. Meadows Bank utilizes multiple combinations of verification techniques within our various electronic products to ensure your accounts are protected. While these methods may vary by system or product, their purpose remains the same: to protect you and your assets by adding additional layers of security to your online or mobile banking experience.

There are three recognized types of authentication factors:

TYPE 1- Something You Know - This includes passwords, pin numbers and security phrases, or security questions and answers that you retain and can recall and input upon request.

TYPE 2 - Something You Have – Items in this category are strictly physical objects such as your smart phone or tablet or PC. The system can identify patterns of access on these devices which become flagged as “trusted”.

Type 3 - Something You Are – Included in this group are parts of the human body that can be used for verification, such as your finger print, facial recognition, retina scans, iris scans and other forms of Bio-Metric identification.

When attempting to access your account information with Meadows Bank, or when utilizing our electronic banking products, you will automatically be processed through MFA. In the event that the system deems anything to be out of the ordinary for your personal pattern of behavior, such as logging in from a new device, or attempting to access the system while out of town in a location you aren’t typically known to be in, our system will add an additional verification requirement to confirm your identity, such as prompting you to answer security questions, or inputting an SMS code from the phone number we have on file, before granting access.

If we are unable to confirm your identity via MFA, out of an abundance of caution and in the interest of protecting your financial information, your account will automatically be locked and no further access can occur until you contact the bank directly. Upon speaking with a bank representative, additional security questions may be asked in order to positively confirm your identity. Afterwards we will unlock your profile and you can proceed with your online or mobile banking activity.

If at any time, you feel your information may have been compromised, please contact us right away by calling 702-471-2265. This will ensure that steps are taken immediately to protect your accounts and identity from any further fraud.

To report lost or stolen debit/ATM cards call 702-471-2265 during normal business hours and 888-297-3416 after business hours or on holidays.