Meadows Bank eNewsletter

Volume Issue • April 2020

In This Issue:

Messages to Our Clients Regarding Economic Assistance Programs and Bank Operations

Please see our website for a complete review of all of the communications.

In summary:

Until further notice we have modified our branch hours to 9:00am to 4:00pm daily. We will also keep the lobby and front doors locked to control customer access to the branch to comply with social distancing. One of our branch staff will be monitoring the doors and will allow client access when we can accommodate you in the branch.

Meadows Bank is committed to helping your business through the current economic crisis. We are here to advise you of the options that are presently available for your business from the federal government and Meadows Bank. We hope that by offering you the facts of the two major programs available that you will be able to get the money you need for your business quickly. There are two primary programs that you may want to consider to assist your business:

- The SBA Economic Injury Disaster Loan (EIDL) Program which is a direct loan program through the Small Business Administration (SBA). These are low cost, low interest federal disaster loans for working capital for small businesses.
- The recently approved CARES ACT created the Paycheck Protection Program (PPP) for loans to small businesses impacted by COVID-19 to encourage small businesses to retain their employees during this crisis.

Under the CARES Act, 7(a) Borrowers are relieved of any obligation to pay the principal, interest and any associated fees that are owed on a 7(a) loan for a 6-month period beginning with the first payment due on a loan after March 27, 2020. As such, Meadows Bank has turned off ACH processing for those 7(a) Borrowers who are set up on Autopay for the next six months. The next payment that will be automatically processed will be the October 2020 payment.

To any of our clients who have been impacted by the COVID-19 pandemic, please reach out to your Meadows Bank Loan Officer or Relationship Manager to discuss your challenges and available options.

How to Stay Focused When Working From Home

Ways to stay productive when working from home

Working from home has many perks — zero commute, a comfortable environment and no dress code. Yet, working from home comes with its own set of distractions. Since you don't have your boss looking over your shoulder, it's easy to slack off. Plus, chores around the house will call your name. and if you have furry family members, they will do their best to get your attention. Stay productive working from home with the following tips.

Create a real workstation

Since you may only need a laptop and your cell phone to get your work done, you might not bother creating a real workstation in your home. Working on your couch or from your bed will be comfortable, but those locations will not put you in the proper work mindset. Contributors at Entrepreneur.com recommend you create a home office, complete with a desk, door and business-quality materials.

However, if you relish working from home because you don't enjoy a traditional work space, you can still be productive. "Remove distractions, create a layout that supports efficient workflows and cultivate an environment that keeps you in the zone," McGerr writes.

Dress the part

Your work from home dress code doesn't require the corporate-approved threads your office does, but it's still important to dress for the day. Pajamas, sweats and yoga pants are very comfortable, but they're clothes designed for lounging, the very opposite intent of a productive worker.

"Get dressed every day. It doesn't have to be what other people think you should wear. Are you productive in jeans and a button up shirt? Wear that. Just get out of the clothes you slept in. Let your brain know that you're ready to work," advises Medium.com writer Nicole Peery.

Manage your time

Working remotely tends to offer flexibility with your hours. You can start working the moment you wake up, but if you're not careful, you might find yourself working much later than you want to or should. An office setting typically comes with a set schedule of hours. You clock in, work, take a lunch, work, take a break, work, and then clock out. Your work from home schedule should resemble a typical working day, with breaks, dedicated work time and a hard stop.

Set limits

Your friends and family might interpret your working from home as a day off, so it's important you set boundaries. McGerr advises telling your family and friends the hours you'll be working so they won't distract you. "Setting these boundaries will give you time to work uninterrupted so you don't end up putting in extra hours over the weekend to catch up," according to McGerr.

Ignore social media

Engaging on social media is a fast way to get nothing done during working hours. Don't let social media notifications, messages or emails that are not related to work hog your attention. To keep focused on your work to-do list, Peery recommends using the do not disturb feature on your phone.

Working from home offers a lot of freedom and flexibility. These tips will help keep you productive.

2019 Bank Performance Summary

During these difficult times, we know that our customers continue to rely on Meadows Bank to provide the services they need. That's why Meadows Bank is committed to helping our clients and their businesses through this economic crisis - offering assistance with SBA business loan programs included in the recent federal government stimulus package, as well as all of our regular banking and lending services.

In 2019 Total Assets of the Bank grew over $100 Million and stood at $961.2 million at year end. Growth in other key line items were as follows.

	12/31/19	12/31/18	Annual Growth
Total Assets	$961.2 Million	$858.7 Million	12%
Total Loans	$805.2 Million	$752.9 Million	7%
Total Deposits	$838.2 Million	$745.8 Million	12%
Total Capital	$118.0 Million	$99.0 Million	19%
Net Income After Tax	$18.4 Million	$15.8 Million	16%

Following are other key financial ratios for 2019:

- Return on Average Assets of 2.01%
- Return on Average Equity of 16.9%
- Net Interest Margin of 4.85%
- Efficiency ratio of 48.83%
- Book Value per Common Share of $27.67 as of 12/31/2019

In 2019, The National Association of Development Companies (NADCO) named Meadows Bank “Most Active Community Lender of the Year” for the SBA 504 loan program following similar recognition the prior year. Also, in fiscal 2019, Meadows Bank placed second among Statewide and Regional Banks in 7(a) lending according to the U.S. Small Business Administration office.

BauerFinancial, Inc., an independent bank research firm gave us a Five Star “Superior” rating in 2019. The “superior” rating indicates the Bank is financially sound and is operating well above its regulatory capital requirements. This rating is issued after analyzing the financial information at the end of each quarter and is current through December 31, 2019. Also, SNL Financial, a financial institution rating company affiliated to S&P Global, has notified us that we were one of the top 100 best-performing community banks under $3 Billion in assets in 2019.

As the current crisis passes over the country, the big question is what we should expect on the other side. How soon businesses will be able to rebound from mandatory closings, employee layoffs and business disruption will depend on the pace at which consumer confidence returns.The retail and service industries are critical components of the national and local economies and consumers’ willingness to resume normal activities at pre-crisis levels will undoubtedly dictate the pace of the recovery as well as the Bank’s performance in 2020.

We hope this summary of our performance reiterates the strength of the bank and reassures any concerns about our ability to ride out the current crisis. Meadows Bank is here to work with our neighbors to make sure our community is strong and standing tall when this crisis passes. Together we will make it through - because together, we are stronger.

Coronavirus (COVID-19) Cybercrime Alert

Governments around the world are working diligently to slow the spread of the Coronavirus (COVID-19). Measures such as frequently washing your hands, refraining from touching your face, quarantining as much as possible and aggressively practicing social distancing all help in flattening the curve of new cases of the disease.

Amid the effort to keep people healthy, there is a sector of human society that use catastrophic events, such as the current global pandemic, to exploit others for their own selfish gain.

This month's article sheds light on some cybercrime taking place that employs the terms Coronavirus or COVID-19.

The information below was provided by the United States Computer Emergency Readiness Team (US-CERT). The information came from a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC).

This alert provides information on exploitation by cybercriminals and Advanced Persistent Threat (APT) groups of the current Coronavirus (COVID-19) global pandemic. It includes a non-exhaustive list of Indicators of Compromise (IOCs) for detection as well as mitigation advice.

Both CISA and NCSC are seeing a growing use of COVID-19 related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19 related scams and phishing emails. This alert provides an overview of COVID-19 related malicious cyber activity and offers practical advice that individuals and organizations can follow to reduce the risk of being impacted. The IOCs are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this alert does not seek to catalogue all COVID-19 related malicious cyber activity. Individuals and organizations should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves.

APT groups are using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using Coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and "hack-and-leak" operations.

Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cybercriminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats observed include:

- Phishing, using the subject of Coronavirus or COVID-19 as a lure,
- Malware distribution, using Coronavirus or COVID-19 themed lures,
- Registration of new domain names containing wording related to Coronavirus or COVID-19, and
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

Malicious cyber actors rely on basic social engineering methods to entice a user to carry out a specific action. These actors are taking advantage of human traits such as curiosity and concern around the Coronavirus pandemic in order to persuade potential victims to:

- Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.
    - For example, a malicious Android app purports to provide a real-time Coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install "CovidLock" ransomware on their device.
- Open a file (such as an email attachment) that contains malware.
    - For example, email subject line contains COVID-19 related phrases such as "Coronavirus Update" or "2019-nCov: Coronavirus outbreak in your city (Emergency)"

To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with "Dr." in their title. In several examples, actors send phishing emails that contain links to a fake email login page. Other emails purport to be from an organization's Human Resources (HR) department and advise the employee to open the attachment.

Malicious file attachments containing malware payloads may be named with Coronavirus or COVID-19 related themes, such as "President discusses budget savings due to Coronavirus with Cabinet.rtf."

Mitigations

Malicious cyber actors are continually adjusting their tactics to take advantage of new situations, and the COVID-19 pandemic is no exception. Malicious cyber actors are using the high appetite for COVID-19 related information as an opportunity to deliver malware and ransomware, and to steal user credentials. Individuals and organizations should remain vigilant. For information regarding the COVID-19 pandemic, use trusted resources, such as the Centers for Disease Control and Prevention (CDC).

Phishing Guidance for Individuals

The NCSC's suspicious email guidance explains what to do if you've already clicked on a potentially malicious email, attachment, or link. It provides advice on who to contact if your account or device has been compromised and some of the mitigation steps you can take, such as changing your passwords. It also offers NCSC's top tips for spotting a phishing email:

- Authority – Is the sender claiming to be from someone official (e.g., your bank or doctor, a lawyer, a government agency)? Criminals often pretend to be important people or organizations to trick you into doing what they want.
- Urgency – Are you told you have a limited time to respond (e.g., in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- Emotion – Does the message make you panic, fearful, hopeful, or curious? Criminals often use threatening language, make false claims of support, or attempt to tease you into wanting to find out more.
- Scarcity – Is the message offering something in short supply (e.g., concert tickets, money, or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

Phishing Guidance for Organizations and Cybersecurity Professionals

Organizational defenses against phishing often rely exclusively on users being able to spot phishing emails. However, organizations that widen their defenses to include more technical measures can improve resilience against phishing attacks.

In addition to educating users on defending against these attacks, organizations should consider NCSC's guidance that splits mitigations into four layers, on which to build defenses:

- Make it difficult for attackers to reach your users.
- Help users identify and report suspected phishing emails (see CISA Tips, Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams).
- Protect your organization from the effects of undetected phishing emails.
- Respond quickly to incidents.

CISA and NCSC also recommend that organizations plan for a percentage of phishing attacks to be successful. Planning for these incidents will help minimize the damage caused.

Communications Platforms Guidance for Individuals and Organizations

Due to COVID-19, an increasing number of individuals and organizations are turning to communications platforms—such as Zoom and Microsoft Teams— for online meetings. In turn, malicious cyber actors are hijacking online meetings that are not secured with passwords or that use unpatched software.

Tips for defending against online meeting hijacking (Source: FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI press release, March 30, 2020):

- Do not make meetings public. Instead, require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a meeting on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. Change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications.
- Ensure telework policies address requirements for physical and information security.

We are here to help keep you protected. Meadows Bank has a robust platform of sophisticated tools to protect you from cybercrime and bank fraud. To learn more, visit www.meadowsbank.bank or send an email to hereforyou@meadowsbank.com.

Right Now - More Than Ever Before - It's All About Online/Mobile Banking

Treasury Management Online Banking Platform

Our Treasury Management online banking platform is a sophisticated, yet easy to use, program for our business customers. It provides additional security enhancements, a customizable dashboard, the ability to set up recurring ACH and Wire transactions, an impressive number of reporting tools and much more.

The new Treasury Management platform has multiple features:

- Dashboard Access; a quick view of key information – account information, Positive Pay exception items, outgoing wires, ACH batches, resource links and favorite reports, just to name a few.
- Accounts Access; accounts in this product – view a list of accounts or search for a specific transaction.
- Payments; work with transfers, wires, ACH, Positive Pay, and stop payments.
- Reporting View; reports and define favorite reports.

Remote Deposit Capture

Remote Deposit Capture (RDC) and its mobile companion mRDC allows your small business to deposit checks without going to the bank. You can quickly and easily deposit checks to your business checking account using either a personal computer along with a unique scanning device or via a compatible smartphone or tablet. RDC and mRDC offer you a convenient way to make anytime, anywhere deposits, allowing you to receive funds faster and improve working capital.

- Make deposits at your convenience – no more traveling to a bank branch or scheduling a courier pick up.
- Accelerate cash flow with same day depositing.
- Deposit checks into multiple accounts.
- Deposit more than one check at a time.
- Consolidate banking from various regions since proximity to the bank is no longer an issue.
- Maintain the controls necessary for your daily cash management operations – you assign individual login credentials for multiple authorized users and set account restrictions and criteria levels.
- Transmit deposits through a secure internet connection with the latest security protocols.
- Reduce check fraud by allowing returned items to be identified sooner and minimizing lost/stolen checks.
- Track deposit activity and obtain detailed reporting.

Online/Mobile Banking

Manage your finances more efficiently in a secure, simple-to-use environment. Meadows Bank's Online and Mobile Banking allows you 24/7 access to check your balances, browse transactions, transfer funds, set up bills to be paid automatically, and much more.

- View balances and account activity.
- Monitor transactions in real time.
- Set up one-time and recurring fund transfers between Meadows Bank accounts.
- Transfer money between Financial Institutions.
- Make mobile deposits using your mobile device's camera.
- Pay bills quickly and easily - variable or recurring.
- Make person-to-person payments.
- Set up personalized account alerts.
- Receive electronic statements.
- Integrate with Quicken and other personal accounting software.

Bill Pay

Simplify your life with online bill payments - no more writing checks, stuffing envelopes and searching for stamps.
Meadows Bank Bill Pay makes it easy to pay bills to individuals or businesses:

- Pay bills from multiple accounts.
- Send single or recurring payments.
- Pay bills now or schedule future payments.
- Make person-to-person electronic payments quickly and easily.
- Send money to individuals via text and/or email.
- Initiate expedited payments.
- Track your account balances and payment history quickly.
- Get helpful text alerts and payment reminders.

To learn more about any of these products or for technical support, please contact us at 702.471.BANK (2265) or email us at hereforyou@meadowsbank.com.