Meadows Bank eNewsletter

Volume Issue • April 2022

In This Issue:

Out and About in Our Communities

Chris McQuattie - VP/Branch Relationship Manager in Reno has been nominated to sit on the Board of Directors for the Boy Scouts of America in Northern Nevada. Confirmation is expected at the May 2022 BOD meeting. In addition, he will have the role of VP of Finance.

Kari Golden - VP/Branch Relationship Manager in Henderson took over her duties as President of the Board of Directors for CREW Las Vegas - the industry's premier business networking organization, working to advance women in all aspects of commercial real estate, and to support our members through education, leadership, partnership and networking.

Todd Russell - VP/Commercial Loan Office in Arizona has been elected to the Board of Directors for Hunkapi - an independent non-profit organization based in Scottsdale, Arizona that offers therapeutic riding, emotional regulation, equine assisted psychotherapy and other services for both children and adults.

Weighing the Costs of Opening a Second Store

Deciding if it’s the right time to expand

If you’re an entrepreneur who’s worked hard to build a flourishing business, it may be tempting to open a second location in hopes of serving more clients and earning more profit. However, the process of opening and maintaining a second brick-and-mortar can add a wealth of complications to running your operation. Here’s a look at a few factors to consider before you take the plunge.

Consider your first location

Before you shop around for a new space to rent, consider the age, growth curve, and state of your current location. According to business consultant Lisa Starr, if your business is under three years old, it’s hard to judge whether its growth curve will be sustainable or indicative of your second location’s success. Starr also suggests looking at your current lease. If you’re coming up on the end of your lease, is it possible that your lease won’t be renewed? If you were forced to relocate your first location, could you handle the time, energy, and financial cost of managing your fledgling second store? If not, it may be a good idea to hold steady and continue strengthening your first location until a better time for growth arises.

Location is everything

Your second brick-and-mortar’s fate is heavily tied to its location. If your new store is too close to your first shop, the second location could leech business away. To ensure that both locations have plenty of room to attract customers and grow, Starr suggests drawing a 10-mile-radius circle around your current location, and scouting for a second location outside of that bubble. It’s also important to consider whether your second store is conveniently located in an area that’s accessible to your target demographic.

How long will it take to break even?

After you’ve signed on the dotted line for the lease, hired and trained new employees, and promoted your new store, you may be serving customers and receiving cash — but that doesn’t mean your new location is profitable yet. Startup costs are sizable for a second store, so consider how long it will take your shop to break even. In most cases, the profits and savings from the first store will go to support the second one until the newer location can support itself. Entrepreneur contributor Thomas Smale recommends having a backup plan in place if your second shop doesn’t break even as soon as projected due to slow growth or unforeseen economic circumstances. Consider seeking out additional financing to make sure your second store can stay afloat, but be aware of how much debt you’re taking on.

Alternatives to a second location

Instead of opening a second location to grow your enterprise, Starr suggests that you consider the goals you have for your second location and see whether you could accomplish those goals with your first location. If you’re looking for higher profits, you may be able to achieve this with a slight price hike on your best-selling products or services. You could also boost profits through expanding your operating hours, optimizing the way you schedule staff, or managing clients more efficiently.

Opening a second store could reap significant rewards, but it comes with a fair share of risks. Before you change the way you do business, hash out your ideas with your business partner or a professional consultant.

Recently Funded Loans

Whether you want to acquire land for development, start or expand your business, purchase equipment, hire employees, finance a franchise or expand your office space, we offer a range of loans with varying terms, rates and requirements.

Here are just a few of our recently funded Commercial and SBA loans:

NEVADA

$2,785,000

Commercial Bridge Loan

The Huntridge Theater Renovations

$2,200,000

SBA 504 – Construction

Medical Office

ARIZONA

$850,000

SBA 7a – CRE Purchase

Auto Repair

$13,125,000

Construction Loan

WaterWalk Phoenix – Deer Valley

UTAH

$2,471,000

SBA 504 – Purchase Building

Engineering Firm

CALIFORNIA

$900,000

SBA 7a – Purchase CRE

Cabinet Manufacturer

Reporting Cybercrime

In this 'Protect Yourself' section of our newsletter, we provide information and tips to help you spot tools, techniques and procedures that criminals use to launch cyberattacks and/or other fraudulent schemes, in order to help you avoid becoming a victim.

Periodically, we also provide practical steps you can take if you have become a cybercrime victim. That is the focus of this month's article. Below are steps outlined by the National Cybersecurity Alliance that you can take to help you with reporting cybercrimes and evidence collection.

Cybercrime can be particularly difficult to investigate and prosecute because it often crosses legal jurisdictions and even international boundaries. Additionally, an offender may disband one online criminal operation – only to start up a new activity with a new approach – before an incident even comes to the attention of the authorities.

The good news is that federal, state and local law enforcement authorities are becoming more sophisticated about cybercrime and are devoting more resources to responding to these threats. Furthermore, over the past several years, many new anti-cybercrime statutes have been passed that empower federal, state and local authorities to investigate and prosecute these crimes. However, law enforcement needs your help to stop the nefarious behavior of cybercriminals and bring them to justice.

Who to Contact

- **Local law enforcement:** Even if you have been the target of a multijurisdictional cybercrime, your local law enforcement agency (either police department or sheriff's office) has an obligation to assist you, take a formal report and make referrals to other agencies, when appropriate. Report your situation as soon as you find out about it. Some local agencies have detectives or departments that focus specifically on cybercrime.
- **The Internet Crime Complaint Center (IC3):** IC3 will thoroughly review and evaluate your complaint and refer it to the appropriate federal, state, local or international law enforcement or regulatory agency that has jurisdiction over the matter. IC3 is a partnership between the Federal Bureau of Investigation and the National White-Collar Crime Center (funded, in part, by the Department of Justice's Bureau of Justice Assistance). Complaints may be filed online at ic3.gov.
- **Federal Trade Commission (FTC):** The FTC does not resolve individual consumer complaints but does operate the Consumer Sentinel, a secure online database that is used by civil and criminal law enforcement authorities worldwide to detect patterns of wrong-doing, leading to investigations and prosecutions. You can file a complaint at reportfraud.ftc.gov. Victims of identity crime may receive additional help through the FTC hotline at 1-877-IDTHEFT (1-877-438-4338); identitytheft.gov provides resources for victims, businesses and law enforcement.
- **Your local victim services provider:** Most communities in the United States have victim advocates ready to help following a crime; these providers offer information, emotional support and advocacy as needed. Find local victims service providers at ovc.ojp.gov/directory-crime-victim-services/search.

Collect and Keep Evidence

Even though you may not be asked to provide evidence when you first report the cybercrime, it is very important to keep any evidence you may have related to your complaint. Keep items in a safe location in the event you are requested to provide them for investigative or prosecutive evidence. Evidence may include, but is not limited to, the following:

- Canceled checks
- Certified or other mail receipts
- Chatroom or newsgroup text
- Credit card receipts
- Envelopes (if you received items via FedEx, UPS or U.S. Mail)
- Facsimiles
- Log files, if available, with date, time and time zone
- Social media messages
- Money order receipts
- Pamphlets or brochures
- Phone bills
- Printed or preferably electronic copies of emails (if printed, include full email header information)
- Printed or preferably electronic copies of web pages
- Wire receipts

In addition to the above, Meadows Bank strongly encourages you to immediately notify us about incidents of cyber theft, suspicious account activity, or any attempts to gain access to your accounts by unauthorized individuals. You may call us directly at 702.471.BANK (2265) or by emailing hereforyou@meadowsbank.bank.

Beware of Two-Factor Authentication Scams!!

Two-Factor Authentication (2FA) also referred to as Multi-Factor Authentication (MFA), utilizes a combination of verification methods to secure your online banking profile. 2FA combines something you know, such as your username and password with something you have, such as your phone (text verification code) or email (emailed verification code) and/or something you are, such as your fingerprint or facial recognition to confirm your identity prior to allowing access to your online accounts.

Meadows Bank requires our customers to have the following information in order to access any of our online products:

- Your user ID and password.
- An authentication code which is sent to your phone or email address on file, either by text message (SMS) or secure email.

If you are logged in to your online banking profile with Meadows Bank and request access to a new service such as Bill Pay, Mobile Deposit or Zelle, Meadows Bank will again send you a verification code by text or email prior to allowing you to enroll in that new product. For example, as you create new payees within our bill payment system, add new users within our Treasury Management platform, or create new Zelle recipients, you will again be required to input a new verification code before proceeding. Our system is designed to prompt you every step of the way to help protect your accounts if your user name and password have fallen into the wrong hands. These passwords are for you and you alone and should never be shared with anyone, not even a bank representative. Would be scammers often portray themselves as being from your bank to convince you to provide this information to them. Do not fall for it!! Meadows Bank (or any other bank) will never ask you for your user name, password or verification codes.

As Two-Factor Authentication has become more and more the norm, and fraudsters are no longer able to compromise your online account(s) by stealing your user ID and password, they have stepped up their game in an attempt to trick you into sharing that information with them. Here's how it works:

You receive a text from someone claiming to be from your bank. They inform you that in order to verify your identity, they need you to provide them with the verification code that they are about to send to you. What is really happening behind the scene is, the fraudster has entered your user ID and password but can't get pass the entry of the required computer-generated verification code without your help. If you fall for their scam and provide them with the verification code you received, they can immediately enter that code, login to your online banking profile and take over your account by changing your password, security questions and the phone numbers associated with that account. Once they've changed your personal information, they begin accessing your account and send your money to their accounts at different banks.

Since you participated in the fraud by providing the fraudster with the secure information they needed to access your account(s), you often are left with no recovery rights and are left to deal with the fall out.

Below are some reminders on how to protect yourself from 2FA scams:

1. Never reply to a text or email asking you to send your verification code.
2. If you receive texts or emails from your bank containing verification codes that you were not expecting or did not request, your online profile may have been compromised. Log in to the banking website or online app directly. **Do not click on any links from your texts or emails.** Immediately change your password. Once completed, call your bank to report the potential incident. The bank will take the appropriate steps to protect you and your account(s). **DO NOT** provide any information to anyone calling claiming to be from your bank. Hang up and dial a trusted bank phone number or stop in to your local branch for assistance.
3. Remember, your bank will never call you and ask you to provide your user name, password, authentication information, etc. That information is yours and should never be shared. If you feel you may have fallen victim to a scam, immediately call your bank and let them know.
4. Listen to your gut. If it doesn't feel right, it's probably not right.