Meadows Bank eNewsletter

Volume Issue • March 2020

In This Issue:

Meadows Bank eNewsletter

Coronavirus (COVID-19) Notice

We are closely monitoring the evolving COVID-19 situation. The safety of our employees and customers is of the utmost importance to us. At this time, it is especially important we all take seriously the advice of public health experts for maximizing our own health and the health of others. We are monitoring and following all CDC and health department prevention recommendations. And our employees have been instructed to stay home if they feel ill.

Out of an abundance of caution, our branch staff are taking preventative measures against the potential spread of the Coronavirus (COVID-19). Standard procedures include frequent cleaning with health department approved disinfecting products of high-touch surfaces, including counters, door handles and client waiting areas. Our employees may take extra steps to protect themselves and our customers with gloves and hand sanitizer. These are strictly precautionary measures for everyone's safety.

In addition, for our client's safety and the safety of our employees we are reducing the number of weekly courier stops. We will conduct pick-ups and drop-offs on Tuesdays and Fridays for the next several weeks as a preventative measure. If you are sick, please allow us to assist you through our robust online and mobile banking platforms for both individuals and businesses. If you are not already set up with Online or Mobile Remote Deposit Capture, please contact our e-banking team by phone at 702.471.BANK (2265) or email us at hereforyou@meadowsbank.com and we will get you set up with this time-saving and flexible service.

We want to ensure you that we will continue to service our clients through this unprecedented time while at the same time adhering to state and federal health mandates. Meadows Bank is a well-capitalized bank and all deposits are FDIC insured to the maximum limits.

How Contactless Credit Cards Work

Contactless cards could be the future of business transactions

Contactless credit cards, also known as tap-to-pay cards, have begun cropping up all over the country. You may have already seen compatible card readers at your local coffee shop or fast-food restaurant that feature a somewhat familiar graphic resembling that of a volume icon without the speaker, the same associated with NFC (near field communication) technology.

Below, you'll learn more about how these next-generation credit cards work, whether they are secure and how a small business could start accepting them.

How do contactless credit cards work?

Contactless credit cards are chip cards that feature embedded NFC technology, enabling you to pay over a secure radio interface without swiping the magnetic stripe or inserting the chip. "The tech involved is deceptively simple," says Cameron Faulkner in an article for TechRadar. "Evolved from radio frequency identification tech, an NFC chip operates as one part of a wireless link. Once it's activated by another chip, small amounts of data between the two devices can be transferred when held a few centimeters from each other."

This is the same technology used by smartphone-based mobile wallets such as Apple Pay and Android Pay. With mobile wallets, you store your credit card information in an app that then uses the NFC tech to securely send the info to a nearby card reader. Contactless credit cards essentially do the same thing but cut out the smartphone to simplify the process.

How to use contactless credit cards

According to VISA, one of the credit card companies responsible for developing and maintaining NFC technology, the presence of a "Contactless Indicator" — the volume-like icon described above — indicates acceptance. "When featured on a card, it means the card can be used to tap to pay. When featured on a checkout terminal, it means a merchant accepts tapping to pay," VISA says.

Thankfully, just because a card and a reader have a Contactless Indicator doesn't mean they are always busy receiving or sending secret transactions via NFC technology. To make a transaction, you need to tap your contactless-enabled card on the "Contactless Symbol," which looks like the Contactless Icon combined with a pointing hand. Your card needs to be within 1-2 inches of the Contactless Symbol to initiate a payment, which will then take only about one to two seconds to process.

Are contactless credit cards secure?

When you tap your contactless credit card, it creates a cryptographic code unique to the card and to the transaction. This makes it virtually impossible for fraudsters to skim your credit card information, which is one of the vulnerabilities of magnetic stripes. "The cryptogram can only be decoded by your bank to validate your transaction. It cannot be replayed," says Jack Jania, senior vice president of strategic alliances at Gemalto, a leading provider of contactless cards. "The bank decides, 'This is one of my cards, and this is one of my clients' transactions.' It's a handshake between the point-of-sale terminal and the card issuer."

Additionally, credit card networks set a limit for contactless payments. For example, MasterCard has a $100 limit on tap-and-go transactions. If the limit is exceeded, the user must key in their PIN for additional security, preventing someone who has physically stolen your card from making major purchases.

Benefits of contactless credit cards

Using a contactless credit card is potentially faster than any other payment method. It eliminates the small amounts of time lost pulling out cash and returning the change, or making sure a credit card is in the right orientation to swipe or insert. Mobile wallets are also just as fast once payment begins processing, but require the extra step of pulling up an app on a smartphone or smartwatch. For a small business making lots of small transactions, supporting contactless payment can add up to a lot of time saved. In fact, Melanie Gluck, vice president of security solutions at MasterCard, says that's exactly what the technology is best used for. Contactless credit cards are "designed for lower values, for speed and convenience," Gluck says. "It's not meant for major purchases."

If you run a business that sees a high volume of small purchases, tap-to-pay cards could make a lot of sense for you. Get in touch with your local financial institution to learn more about how to bring contactless payment solutions to your business.

Coronavirus Scams

The purpose of these fraud alerts is to share information regarding tactics fraudsters use to exploit payment networks and participants. These lessons can be used to strengthen payment controls and prevent similar occurrences, and reduce fraud with other organizations.

Criminals are opportunists, and as seen in the past, any major news event becomes an opportunity for groups or individuals with malicious intentions. The Coronavirus is no different. In fact, the Coronavirus is a much more potent opportunity for enterprising criminals because it plays on one of the basest human conditions…fear. Fear can cause normally scrupulous individuals to let their guard down and fall victim to social engineering scams, phishing scams, non-delivery scams, auction fraud scams, etc.

Numerous international sources from Asia, Africa, Australia, and Europe are reporting a rise in Coronavirus scams, and a rise in the number of incidents in the United States is expected. Brief details of the associated Coronavirus scams being encountered are below:

- Phishing Scams
- Social Engineering Scams
- Non-delivery Scams

Phishing scams have become ubiquitous through email communication and commerce. Cyber criminals are exploiting the Coronavirus through the wide distribution of mass emails posing as legitimate organizations such as the Center for Disease Control (CDC) or World Health Organization (WHO). In one particular instance, victims have received an email purporting to be from the WHO with an attachment supposedly containing pertinent information regarding the Coronavirus. This leads to either unsuspecting victims opening the attachment causing various types of malware to infect their system, or prompting the victim to enter their email login credentials to access the information resulting in harvested login credentials. These incidents enable further instances of cyber-enabled financial crime such as Business Email Compromise (BEC), PII theft, ransomware, account takeovers, etc. Another side effect of the Coronavirus is increased teleworking, which furthers the reliance on email for communication adding yet another multiplier to these email fraud schemes. More of these incidents are expected, and increased vigilance regarding email communication is highly encouraged.

Another emerging fraud scheme exploiting the Coronavirus is using social engineering tactics through legitimate social media websites seeking donations for charitable causes related to the virus. Criminals are exploiting the charitable spirit of individuals, seeking donations to fraudulent causes surrounding the Coronavirus. Increased caution should be exercised when donating to causes tied to Coronavirus relief.

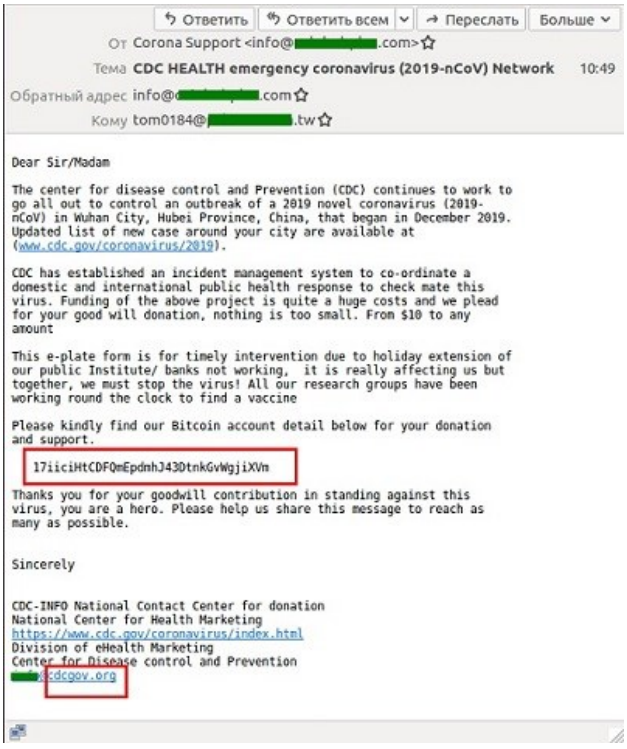
A third fraud scheme surrounds non-delivery scams. Essentially, criminal actors are advertising in-demand medical supplies for sale to be used to prevent/protect against the Coronavirus, i.e. medical masks, gloves, disinfectant, etc. The criminal enterprise will demand upfront payments or initial deposits, then abscond with the funds and never complete delivery.

Please reach out to the Global Investigative Operations Center (GIOC) at GIOC@usss.dhs.gov or 202-406-6009, if you receive any information relating to this Info Alert.

Global Investigative Operations Center Reference #20-004-I

General Disclaimer: Information contained in this Fraud Alert is based on information provided by WesPay. There is no warranty, expressed or implied, in connection with making this information available. Meadows Bank is in no way responsible for any error or omission in this communication.

WesPay is a payments association dedicated to building and sharing knowledge to guide members through their payments journey, from concept to operation. They work with financial institutions, third-party payment providers and organizations supplying payment services related to operations and compliance, risk management and fraud, and payments strategy and planning.



Warning Signs of an Online Tax Scam

Tax season is in full swing, which means criminals will go to great lengths to separate you from your money, your identity, or anything of value that is within their reach. They may offer seemingly legitimate "tax services" that are actually designed to steal your identity and your tax refund. Often, criminals will lure you in with an offer of larger write-offs or refunds. Such scams might include fake websites and tax forms that look like they belong to the Internal Revenue Service (IRS) in order to trick you into providing your personal information.

Due to the rise in data breaches, you should always take steps to minimize your risk of identity theft and other online-related crimes; this is especially important this time of the year. Below are some warning signs to look for and basic precautions you can take to minimize risk and avoid becoming the next victim!

Warning Signs of an Online Tax Scam

- An email or link requesting personal and/or financial information, such as your name, social security number, bank or credit card account numbers, or any additional security-related information.
- Emails containing various forms of threats or consequences if no response is received, such as additional taxes or blocking access to your funds.
- Emails from the IRS or federal agencies. The IRS will not contact you via email.
- Emails containing exciting offers, tax refunds, incorrect spelling, grammar, or odd phrasing throughout.
- Emails discussing "changes to tax laws." These email scams typically include a downloadable document (usually in PDF format) that purports to explain the new tax laws. However, unbeknownst to many, these downloads are almost always populated with malware that, once downloaded, will infect your computer.

Never Send Sensitive Information in an Email: Information sent through email can be intercepted by criminals. Make sure to consistently check your financial account statements and your credit report for any signs of unauthorized activity.

- **Secure Your Computer:** Ensure your computer has the latest security updates installed. Check that your anti-virus and anti-spyware software are running properly and receiving automatic updates from the vendor. If you haven't already done so, install and enable a firewall.
- **Carefully Select the Sites You Visit:** Safely searching for tax forms, advice on deductibles, tax preparers, and other similar topics requires great caution. NEVER visit a site by clicking on a link sent in an email, found on someone's blog, or in an advertisement. The websites you land on might look like legitimate sites but can also be very well-crafted fakes.

Avoid Being the Victim

- **Be Wise with Wi-Fi:** Wi-Fi hotspots are intended to provide convenient access to the internet, however, this convenience can come at a cost. Public Wi-Fi is not secure and is susceptible to eavesdropping by hackers, therefore, never, never use public Wi-Fi to file your taxes!
- **Look for Clear Signs:** Common scams will tout tax rebates, offer great deals on tax preparation, or offer a free tax calculator tool. If you did not solicit the information, it's likely a scam.
- **Be on the Watch for Fake IRS Scams:** The IRS will not contact you via email, text messaging, or your social network, nor does it advertise on websites. Additionally, if an email appears to be from your employer or bank claiming there is an issue that requires you to verify personal information, this is most likely a scam as well. Don’t respond to these types of emails; always contact the entity directly.
- **Always Utilize Strong Passwords:** Cybercriminals have developed programs that automate the ability to guess your passwords. To best protect yourself, make your passwords difficult to guess. Passwords should have a minimum of nine characters and include uppercase and lowercase letters, numbers, and symbols.

If you receive a tax-related phishing or suspicious email at work, report it according to your organization’s cybersecurity policy. If you receive a similar email on your personal account, the IRS encourages you to forward the original suspicious email (with headers or as an attachment) to its phishing@irs.gov email account, or to call the IRS at 800-908-4490. More information about tax scams is available on the IRS website and in the IRS Dirty Dozen list of tax scams.

- IRS | Taxpayer Guide to Identity Theft
- IRS | Report Phishing
- IRS Dirty Dozen

In addition to the tax scams noted above, unscrupulous individuals are taking advantage of the Coronavirus COVID-19 outbreak to defraud individuals of their funds and steal their identity.Following the precautionary measures noted above can help you protect your personal data from tax and health care scams that are in full swing. See article in "The Latest" section of this newsletter for more information.

Meadows Bank eNewsletter

Remote Deposit Anywhere Through Our Mobile App

Maximize convenience and minimize trips to the branch — our Remote Deposit Anywhere™ lets you deposit checks from wherever you are, 24/7.Download our mobile banking app – Meadows Bank Mobile –from the iPhone App Store or the Android Google Play Store, and access Remote Deposit Anywhere to start making deposits at your convenience.

Here are instructions to enroll once you have the mobile app downloaded:

Click Here for Instructions