

CIBM Bank is providing this newsletter to inform our clients of important banking regulations, fraud prevention tips, and general information.

Non-Consumer ACH Stop Payments Rule:

A written stop payment order regarding any debit entry initiated or to be initiated to a non-consumer account will remain in effect until the earliest of: (a) the withdrawal of the stop payment order by the receiver; (b) the return of the debit Entry; or, (c) six months from the date of the stop payment order, unless it is renewed in writing. (NACHA Operating Rules, 3.7.2.1)

Please contact your local CIBM Bank Personal Banker or Treasury Management Officer to review the ACH stop payment orders that are currently on your account and to make arrangements to renew any orders, if deemed necessary.

Be aware of new IRS Scams

Source: <https://www.consumerfinance.gov/about-us/blog/tax-season-protect-yourself-irs-imposter-scams/>

IRS imposters love to take advantage of tax season by telling people they owe money to the IRS, and they claim the consequences of not paying will be harsh and immediate. To make things worse, the scammers are now armed with phone number masking - your caller ID might say "Internal Revenue Service" or the number may actually be the real IRS phone number. The Consumer Financial Protection Bureau (CFPB) asked officials at the IRS how consumers can spot the phony messages and report them to the proper authorities.

Pass the message on to your customers/members. According to CFPB, the IRS will never:

- Call to demand immediate payment with a prepaid debit card, gift card, or wire transfer.
- Threaten to bring in local police or other law enforcement groups to have you arrested or deported for not paying.
- Demand payment without giving you the opportunity to question or appeal the amount they say you owe.
- Contact you by email, text message, or through social media to request personal or financial information such as PINs, passwords, credit card, bank, or other account information.



Report Scams

Report possible IRS scams to the Treasury Inspector General for Tax Administration at 1-800-366-4484 and to [FTC.gov/complaint](https://www.ftc.gov/complaint). If you get an email from someone claiming to be from the IRS, don't open any attachments or click on any links contained in the message. Instead, forward the e-mail to phishing@irs.gov.

Product Spotlight: Employee Services

Our goal is to help. One of the ways we can do that is to provide you with added benefits for your employees. We offer options where we do the work, and allow you, the employer, to provide something additional of value to your team.

Bank of Choice: This employee benefit banking program is offered at no cost to you. It includes our premier Acceleration checking account, a bonus for account opening, and so much more. Our team will visit your location and allow your team to enroll onsite. You fund the accounts with direct deposit, and your team benefits from the relationship you have with us as an institution. Contact your treasury management representative or local branch for more information.

Health Savings Accounts: As a business owner a high deductible health plan may be right for your company and lower your insurance costs. Offering HSAs is a way to help your employees supplement high deductible costs. We can help you provide your employees with an added benefit and value. Many employers simply provide the account option to their employees, while others offer funding to the employees on an annual, monthly or per pay basis as an additional benefit. A member of our team would be available to come set up accounts at your location making this a convenience service as well. Contact your Treasury Management representative or local branch for more information.

Upcoming CIBM Bank Holiday Closing - Memorial Day

Monday, May 27, 2019: All branches of CIBM Bank and the Federal Reserve Bank will be closed in observance of Memorial Day.

CIBM Bank takes your security seriously: CIBM Bank is committed to protecting your personal and account information. We have account monitoring systems and other controls in place to recognize and help prevent fraud. We will never attempt to gain your personal or account information via email, text message or automated phone calls. Attempts such as these should be considered fraud. If you are contacted in this manner or believe you are the victim of bank fraud, contact us immediately.