From the desk of:

MARK KESSELRING, SVP
INFORMATION SECURITY OFFICER

STIMULUS CHECK SCAMS

As millions of people around the country eagerly await the arrival of their COVID-19 stimulus check or direct deposit, we want to remind you of the importance of staying vigilant to avoid being a target for fraudsters. There have been reports of attempted fraud surrounding stimulus checks and we want to make sure that you are aware of ways to keep yourself safe.

Stimulus check payments begun to be sent out for those that have enrolled in direct deposit options when filing taxes or those that receive social security. If you do not have direct deposit information currently on file with the IRS, you will receive a paper check via mail over the coming weeks. The IRS is also setting up a secure portal for you to enter direct deposit information if you prefer to not receive a paper check.

Any time fraudsters are aware you will be receiving money from the government, there is a heightened risk for attempted theft. Here are a few things you should be aware of:

- Paperwork scams - People or businesses that offer to fill out paperwork to get your stimulus check faster. There is no paperwork required in order to receive your check, and there is no way to accelerate the amount of time it takes you to receive your check other than setting up direct deposit with the IRS.
- Check advance scams - People or businesses offering a stimulus check advance for a fee. Fraudsters may collect the fee first and then not provide money; or deposit fraudulent checks into customer accounts and asking for funds back before the check charges back. The IRS is doing everything they can to get checks out as quickly as possible.
- Fraudulent websites – The IRS is creating a portal to update your direct deposit information in the coming days. It is important not to click links that you are sent via text or email. Instead, you should go directly to the IRS website for updates on stimulus checks. The IRS portal should ONLY be accessed from the IRS website

Your security is our top priority and we will keep an eye out for potential scams and keep you updated on how to keep yourself safe. For more information on keeping your accounts and personal information safe, visit our page on web safety and security. If you suspect you have received a fraudulent message claiming to

be affiliated with the IRS, you can obtain more information and report the communication on the IRS scam website.

SCAMMERS PASSING AS BANK EMPLOYEES

Criminals often take advantage of uncertain times, leading to an increase in fraudulent activity. Please remember, we will never call you to ask you to provide or verify your full account number, username, password, debit card number, unique PIN or Social Security number. If you receive a call from someone requesting this information, even if the caller ID looks like it is coming from the bank, immediately hang up and report it to our Customer Contact Center, at 1-844-722-6589 (844-RBANKTX).

R Bank is aware of financial institutions who have had customers contacted by a "spoofed" phone number that imitated the bank's number on caller ID. The scammer identified themselves as a bank employee and stated that they were contacting the customer because of fraud associated with the customer's debit card. This fraud was allegedly described that someone was trying to take all of their IRS Stimulus Money out of their account before the customer could spend it. Some customers reported that the fraudster was able to verify their part, or all, of their debit card number, address, and/or their social security number. The fraudster then stated that they will be issuing the customer a new debit card and asked that the customer verify their PIN. Once the PIN was shared, they informed the customer that the PIN from the old card will carry over to the new card.

Never share your debit card number or unique PIN with anyone who calls you, even if the caller ID looks like it is a call from the bank; instead, immediately hang up and contact our Customer Contact Center at 1-844-722-6589. If you have released personal information or if you think you have been a victim of fraud please contact R Bank immediately and notify local law enforcement. You, R Bank customers, are our number one priority.

With COVID-19, the fraudsters are out in force with scams involving a variety of communication channels, including email, phone calls, letters, text messages, faxes and social media.

Please keep updated by checking our COVID19 Response Page for more information on other scams, and how to protect yourself, your personal information and your money.