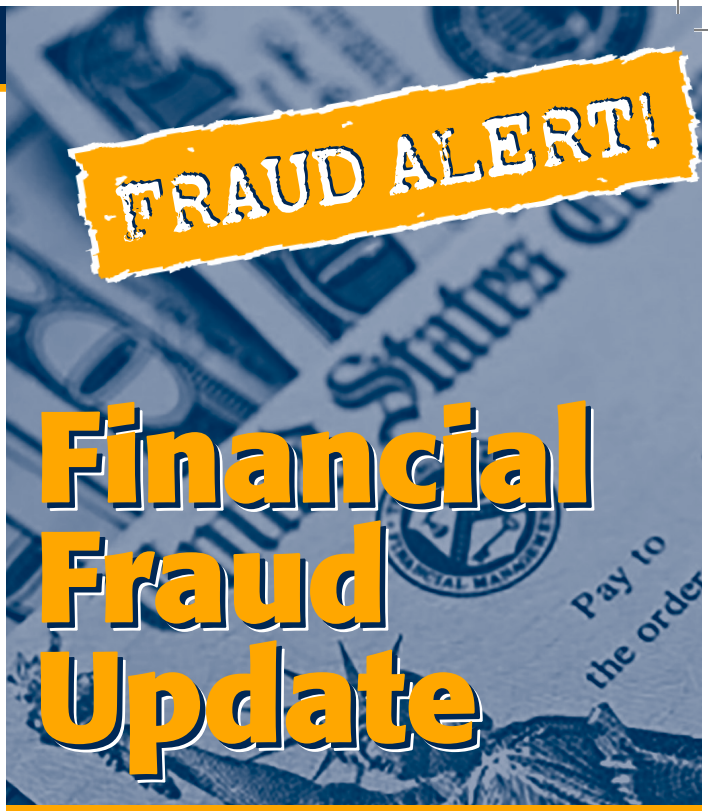
REPORT THE ATTEMPTED THEFT

- Federal Trade Commission
  www.ftc.gov
- Federal Bureau of Investigation
  www.fbi.gov
- Internet Crime Complaint Center
  www.ic3.gov
- Federal Deposit Insurance Corporation
  www.fdic.gov
- National Credit Union Association
  www.ncua.gov

HAB BANK

www.habbank.com



COVID-19 PAYMENT SCAMS

- **Payment Facts**
- **Impostor Scams**
- **Scam Prevention**

Covid-19 Relief Payments

The U.S. Congress has enacted a massive relief package for Covid-19 disease to help individuals and businesses.

The Federal Trade Commission (FTC) and the Federal Bureau of Investigation (FBI) have raised concerns about *scammers and fraudsters that impersonate federal employees* and ask you to verify personal account information in order to receive a payment.

HERE ARE THE PAYMENT FACTS

The relief package passed by the U.S. Congress mandates the following.

- Direct cash payments of up to $1,200 for individuals and $2,400 for couples.
- There is an additional benefit of $500 for every child.
- The payments are based on 2019 U.S. Tax Returns for those who filed them and 2018 U.S. Tax Returns if they have not filed yet for 2019.

NOTE: All the payment rules and restrictions are available at U.S. Treasury website **www.treasury.gov.**

HERE ARE THE SECURITY FACTS

- The U.S. Government will not contact you about these payments—period.
- The U.S. Government will not ask you to verify payment information of any kind.
- The U.S. Government will not ask you to pay any fee or charge to receive payment.
- The U.S. Government will not offer to expedite your payment for a fee.

WHAT SHOULD I DO TO PROTECT MY PERSONAL INFORMATION

Your personal information is secure with your financial institution. The scammers are very convincing con artists … good at what they do.

- Hang up if you receive a telephone call from someone who claims to be from a government agency asking for verification of personal information.
- Ignore or delete it if you get a pop-up message, email or text that directs you to call a certain number or visit a website to verify personal information.
- Never reply to a phone number or use a website that is part of a suspicious call, pop-up or text message to verify personal information.
- Phishing emails are near-replica websites of a trusted or well-known institution such as your financial institution or a government agency. When in doubt, you should initiate contact through a known telephone number or website.

Just ask yourself the question: Why would your financial institution or the government need to contact you for personal information to make or receive a payment—they already have it!