BANKERS' BANK
OF KANSAS

SCAMS ON THE RISE – INCREASING CARD FRAUD

COVID-19 has provided the perfect opportunity for scammers to obtain debit and credit card information from unsuspecting victims. To help you keep your customers aware and protected, we have compiled important information from the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Attorney Steven McAllister of the District of Kansas and various state Attorney Generals. Feel free to pass this information along to your customers.

Examples of known scams:

- **Government Aid scams:** Claims that you need to provide bank account, debit account or PayPal account information to receive your stimulus check are a scam. The IRS will deposit checks into the direct deposit account from previously provided tax return information.
- **Treatment scams**: Offering to sell testing, cures, vaccines, and advice on unproven treatments for COVID-19.
- **Supply scams**: Fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand.
- **Provider scams:** Scammers are contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.
- **Charity scams:** Donation solicitations for those affected by COVID-19.
- **Phishing scams:** Scammers posing as national and global health authorities, such as World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC).
- **App scams:** Scammers are creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that compromises users' devices and information.
- **Investment scams:** Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result. These promotions are often styled as "research reports," make predictions of a specific "target price," and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited publicly available information.

Tips to protect consumers from scams:

- Do not click on links in unsolicited emails and be wary of email attachments.
- Independently verify and research the identity of any company, charity, or individual that contacts you regarding COVID-19. Check websites and email addresses and beware of only slight differences like cdc.com and cdc.org versus cdc.gov.
- Ignore offers for a COVID-19 test, vaccine, cure or treatment. Legitimate health organizations will not send unsolicited emails with information on COVID-19.
- Check online reviews of any company offering COVID-19 products or supplies.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Carefully research investment opportunities using the SEC website.

Helpful links:

CISA - https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

SEC - https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus

FTC - https://www.consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams

IF YOU BELIEVE YOU ARE A VICTIM OF A COVID-19 SCAM, REPORT IT TO WWW.INYOURCORNERKANSAS.ORG AND DISASTER@LEO.GOV