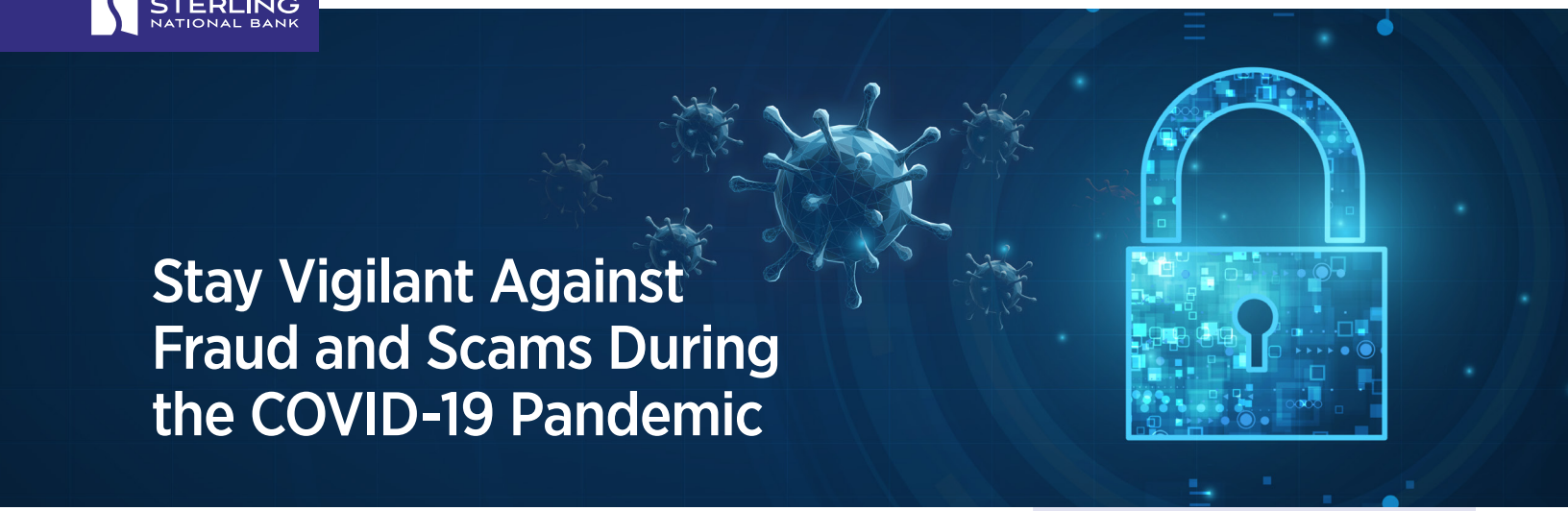
STERLING NATIONAL BANK



Stay Vigilant Against Fraud and Scams During the COVID-19 Pandemic

At Sterling National Bank, now more than ever, we urge our customers to be vigilant and aware of the potential for fraudulent activity, since the unfortunate reality is that successful attempts to compromise accounts and/or information are on the rise amid the COVID-19 crisis.

Attempts have taken on a variety of forms—from unsolicited phone calls and text messages to sophisticated email and web phishing attempts—and fraudsters are using consumers' vulnerability during this time of great uncertainty to their advantage. With such rampant illicit activity being observed nationwide, it is critical to understand what the most common types of fraud being practiced look like and the steps you can take to protect yourself and your organization.

According to the Federal Trade Commission (FTC), more than 18,000 instances of fraud related to COVID-19 have been reported since January 1, 2020—with losses exceeding $13 million[1] and counting.

The Many Faces of COVID-19 Fraud

- **PHISHING EMAILS** appearing to be from reputable sources like the Centers for Disease Control (CDC) or World Health Organization (WHO), financial institutions, or popular retail/e-commerce companies that ask you to share personal information or that contain links that could lead to malware being downloaded to your computer. Phishing emails may also appear to come from within your organization, such as from executive leadership or from the IT department.

- **MALICIOUS WEBSITES** offering maps or statistics related to COVID-19 that ask you to share personal information to register or download malware to your computer.

- **SOCIAL ENGINEERING SCAMS** asking you to send money or provide personal information over the phone or by email or text message. Specifically, fraudsters are calling to schedule Coronavirus tests and collecting credit or debit card and other personal information for copays or other out-of-pocket expenses.

- **"MONEY MULE"** schemes in which people are inadvertently roped into money laundering or check fraud schemes under the pretense of a work-at-home job offer.

[1] https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers

Sterling is Committed to Your Security

We know you do your best to protect your information, but if we spot an issue, we want to reach out as soon as possible. Make sure your phone numbers and email addresses on file with Sterling are up to date. You can update your information through the Sterling Mobile Banking App or through Sterling online banking.

These are convenient ways to check account status, pay bills at any time, and manage and track your budget.

- **TO DOWNLOAD** Sterling's secure Personal Mobile Banking app on your iPhone or Android device, visit www.snb.com/personal-mobile-banking.
- **TO ACCESS** your accounts via our secure online portal, visit snb.com and choose Personal, Commercial, or Business Online Banking under "My Account."

Protect Your Funds

Rest assured that the best place for your money is in a safe, sound financial institution, where it is insured by the Federal Deposit Insurance Corporation (FDIC). You have easy access to the money in your account by using your Sterling National Bank Debit Card, which provides protection in the event of a loss or unauthorized transaction. Please visit **FDIC.gov** for more information regarding how your deposits are protected.

To learn more about how Sterling National Bank is supporting its clients through the ongoing health crisis, please contact your Relationship Manager or visit our COVID-19 Resource Center at snb.com/coronavirus.

- **ATM "BUST-OUT"** schemes in which fraudsters use multiple stolen or fictitious debit cards to make continuous withdrawals. **Because such attempts to access accounts often occur without ever engaging directly with the fraudster, it's important to monitor your accounts regularly and to report any suspicious activity you may see immediately, particularly for multiple small and unfamiliar transactions in a short period of time.**
- **ILLEGAL ROBOCALLS** pitching a variety of in-demand goods and services, including medical treatments and work-at-home schemes. Alternatively, callers may also state that they are from a government agency, such as the Internal Revenue Services (IRS) or the Department of the Treasury (DOT), regarding assistance funds.
- **CHARITY SCAMS** asking for donations to unknown but seemingly legitimate groups. For your security, when donating, we recommend to give only to established, well-known organizations.
- **SUPPLY SCAMS** claiming to have essential items, such as personal protective equipment (gloves, masks, etc.), testing kits, and other critical supplies. These scams often arrive unsolicited via an unfamiliar website.

How to Protect Yourself and Your Business

- Remember that banks, including Sterling and government agencies will never call, text, or email to request money or personal information (Social Security Number, bank account information, or credit card numbers) or to engage you in any official business related to the COVID-19 crisis. This includes Small Business Administration (SBA)/Economic Injury Disaster (EID) loans, which are administered by your financial institution via secure channels within the bank
- Never click on any links (email, text, or web) that you don't expect or trust. This is particularly true for any links asking you to reset user information such as a username, email address, password, or security question(s).
- Whenever possible, only trust information from official and secure sources such as secure local, state, and federal government (.gov) websites and local healthcare officials.
- Take proactive measures to secure your accounts, such as updating and strengthening your passwords, updating your operating systems and security software, and enabling multi-factor authentication for online account logins wherever available.
- Know that anyone offering to pay you for goods or services via wire transfer, certified check, gift card, or cryptocurrency (BitCoin) is most likely a scammer and should not be trusted.
- Recall the old adage "anything that sounds too good to be true probably is." It's important to keep your guard up and not let a fraudster take advantage of fear, emotions, or uncertainty. When in doubt, assume that you are dealing with a fraudster and do not engage.
- Support your community and fight fraud by reporting any suspicious activity to the proper authorities, such as the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center at ic3.gov or your local law enforcement agency.
- Stay informed about the latest scams related to the COVID-19 pandemic by visiting the FTC's coronavirus page at ftc.gov/coronavirus.

WHITE PAPER

Expect Extraordinary.

snb.com | 855.274.2800