CITIZENS SAVINGS BANK & TRUST CO. WILL NEVER CALL OR TEXT ASKING YOU FOR YOUR USERNAME, PASSWORD, OR ANY OTHER SENSITIVE INFORMATION.

Your safety is our top priority. We want to make you aware of a scan affecting our community.

- Scammers are sending text messages to customers, claiming to represent Citizens Savings Bank & Trust Co. Bank Fraud Department.
- They may try to convince you that fraud has been detected on your account, often by asking you to verify whether you made a recent purchase. If you respond "NO" they will claim that to resolve the issue quickly, you need to follow their instructions.

They may ask you to provide:

- Your digital banking username and password, so they can access your account and dispute/remove the fraud.
- The last four digits of your debit card number, to include the expiration and CVV code.
- **PLEASE NOTE: CITIZENS SAVINGS BANK & TRUST CO. WILL NEVER ASK YOU FOR THIS INFORMATION, NOR WILL WE EVER REQUIRE YOU TO PROVIDE IT TO US!**
- With this information, the scammer can immediately login to your account to make fraudulent transfers or begin using your debit card.

WHAT CAN YOU DO:

- **NEVER** share sensitive information with anyone, especially if they call you claiming to be from Citizens Savings Bank & Trust Co.
- If you receive a call or texts asking for personal information and claiming to represent the bank, please hang up immediately and call the bank at **(888) 438-5579.**
- Citizens Savings Bank & Trust Co. has an active fraud team who will contact you if fraud is ever detected on your account. However, our team will never call or text you to verify transactions, ask you to change your password, or have you read your card number over the phone.

WHEN IN DOUBT, HANG UP THE PHONE AND CALL US DIRECTLY!

To our valued customers,

Citizens Bank has become aware of bad actors performing targeted social engineering attacks against business banking customers of various financial institutions.

What is happening?

Bad actors are using Voice Over IP (VOIP) systems to place calls to business banking customers. These calls spoof the financial institution's phone number, with the caller posing as a Treasury Department employee. Once the pretext is established, the bad actors attempt to obtain sensitive account information to facilitate large, fraudulent ACH transfers.

After reviewing details available from this social engineering effort, we have determined that the bad actors appear to be using information publicly available from the Small Business Administration Payment Protection Program.

What action can you take?

Bad actors recognize that certain time periods—such as holidays or the summer travel season—can present an opportunity to take advantage of added distractions or staff covering unfamiliar roles.

- **Stay vigilant** and be aware of possible fraudulent calls, text messages, or other forms of communication.
- **Never share sensitive information** with anyone who contacts you claiming to be a bank representative.
- **If you receive such a request**, end the call immediately and call us back directly at **(615) 327-9787** extension 300 to verify the request is legitimate.

Your security is our priority. Thank you for your continued partnership.