

Fraud Alert: Spoofed Phone Calls Targeting PPP Loan Recipients

One of the latest fraud trends involves spoofed phone calls aimed at businesses who received Paycheck Protection Program (PPP) loans. Using publicly available information, the callers pretend to be from Brenham National Bank, hoping to trick you into sharing sensitive information.

This blog post will break down what's happening and how to protect yourself

What's Happening?

Fraudsters are using caller ID spoofing—a tactic that makes their phone number appear as if it's coming directly from Brenham National Bank. These callers may claim they need to “verify transaction details,” “update your account,” or “confirm information.” In some cases, a scam call related to PPP loans may be followed by fake bank messages or emails designed to appear legitimate. Their goal is to convince you to “verify” or “secure” your account—when in reality, they are gaining access to it.

Once scammers obtain account access, they may attempt to transfer funds into their own accounts, which are often difficult to trace.

Their objective is simple: to access your financial information.

These scams can sound convincing because fraudsters may reference accurate PPP loan terminology or other banking details. Some use high-pressure tactics, urging you to act immediately to avoid supposed account issues or security threats.

Red Flags to Watch For

- Requests for Sensitive Information: Brenham National Bank will never call and ask you for your full online credentials
- Urgent or Threatening Language
- Scammers often try to create panic. They will create a sense of urgency in an attempt to gain your financial information or provide log-in credentials
- Scammers may also pose as the fraud department or law enforcement and request that you provide credentials to stop fraudulent transactions or in order to prevent a payment from being frozen

- Caller ID That Looks Real: Don't rely on caller ID alone to verify legitimacy. Spoofing makes it easy for scammers to mimic a legitimate phone number- including one that may come from Brenham National Bank

How to Protect Yourself

- ✓ Hang Up and Call Brenham National Bank: If something feels off, end the call and contact your local branch
- ✓ Never Share Login Credentials
- ✓ Never Click Suspicious Links
- ✓ Monitor Your Accounts: Regularly review your transactions and report anything suspicious immediately.
- ✓ Educate Your Team: If you're a business owner, make sure employees who handle financial information know how to spot these scams.
- ✓ If you have questions or concerns about your loans or accounts—or want to verify a call you received—reach out to Brenham National Bank directly at your local branch. Staying informed is the best way to stay protected.

Report Fraud at: reportfraud@bnb.bank