1st NEW MEXICO BANK

SHAZAM

Cybersecurity Alert – September 2026

🚨 SECURITY ALERT: Watch Out for Fake "SHAZAM" Fraud Calls

At **First New Mexico Bank** your security is our top priority. We want to alert you to a sophisticated new scam targeting debit cardholders. Fraudsters are impersonating our card processor, **SHAZAM**, to steal card details.

Please take a moment to read how this scam works so you can protect your hard-earned money.

How the Scam Works

1. **The Fake Caller ID or Text Alert:** You receive a phone call or an unexpected text message asking you to validate a recent debit card transaction. Your caller ID may actually say **"SHAZAM"** or show a number associated with them. *(Scammers use technology to "spoof" these numbers to gain your trust)*.
2. **The Follow-Up Phone Call:** If you reply to the text, a fraudster will immediately call you. To gain your trust, they will pretend to be from **First New Mexico Bank** or **SHAZAM**.
3. **The Trap:** To "verify your identity" or "cancel the transaction", or "reverse the funds" the caller may ask you to read aloud **your full debit card number, expiration date, and CVV** (the 3-digit code on the back) **OR** they may ask you to **send money to yourself or a "test account" using apps like Cash App or Venmo**.
4. **The "Legitimacy" Trick:** The scammer might tell you to hang up and call them back at a specific number they provide to prove they are real. **Do not do this.** This is a tactic that routes you right back to the criminal.

Once they have your details, the scammers immediately begin using your card for unauthorized purchases.

🛑 The Golden Rule of Fraud Alerts

SHAZAM and First New Mexico Bank will NEVER ask you for your card details or to send money.

Because they are our official processor, they already have your card information on file. They will only ever ask you to confirm a **"Yes" or "No"** regarding whether a specific transaction was authorized.

What SHAZAM and Your Bank Will NEVER Do:

- ❌ **NEVER** ask you to share your PIN, full card number, CVV code, or online banking passwords.
- ❌ **NEVER** ask you to read back a one-time passcode texted to your phone.
- ❌ **NEVER** ask you to send money via Cash App, Venmo, Zelle, or any other payment service to "verify" or "protect" your account.

1st NEW MEXICO BANK SHAZAM

💡 4 Steps to Protect Yourself

- **Do NOT Reply to Suspicious Texts:** If a text message about a transaction looks unexpected or suspicious, do not reply to it. Contact the bank for details on the transaction.
- **Hang Up and Call Us Directly:** If someone calls you claiming to be a fraud investigator and begins asking for personal details, verification codes, or card numbers, hang up immediately.
- **Never Use Apps to "Verify" Accounts:** No legitimate financial institution will ever ask you to move money through a third-party app to resolve a fraud issue. Never give out your full 16-digit card number, PIN, expiration date, or CVV code over the phone to anyone who called ***you***.
- **Trust Your Instincts:** Real fraud departments will never pressure you, demand immediate card details, or get angry if you choose to hang up and call your bank directly. If you are ever unsure whether a message or call is real, do not use the phone number the caller/sender provided. Always call **575-556-3000** or the official number listed on the back of your debit card.

⁉️ What happens during a REAL SHAZAM fraud alert?

If a transaction looks suspicious, the real SHAZAM automated system will text or call you.

- They will state your name and ask you to confirm a specific transaction (e.g., *"Did you spend $45.22 at Walmart?"*).
- You will only be asked to reply **Yes** or **No**.
- If you say **No**, they will block the card to protect you, and you will need to contact the bank to reissue a new card. **They will never ask you to read your card number to them or require any additional information or enter a code on your phone.**

If you believe you have fallen victim to this scam or shared your card information, please contact **First New Mexico Bank** immediately at **575-556-3000** so we can freeze your card and protect your account.

The bank recommends use of **card control** to protect your account. Card control is a simple process to turn off your card until you need to use it. Call the bank for details.