

# NEWS RELEASE

---

Office of Commissioner Brandon Presley  
MISSISSIPPI PUBLIC SERVICE COMMISSION  
NORTHERN DISTRICT

## **CONSUMER ALERT: Presley Warns Consumers of Debit Card Scam Calls**

Jackson, Mississippi (May 29, 2012) Public Service Commissioner Brandon Presley warned Mississippi consumers today of a weekend series of scam calls claiming to be BancorpSouth asking customers to either validate or re-instate their debit cards. Presley said his office contacted officials with BancorpSouth and verified that the calls were indeed a scam. Similar calls went out a few weeks ago referencing Renasant Bank customers.

"These calls came from a variety of numbers including 'private' numbers and asked consumers to give information including their debit card expiration dates and other confidential information in order to 're-instate' or 'validate' your debit card," Presley said. "Consumers who gave out any of their information should immediately contact their bank."

Presley said that his office plans to share all complaints and information with the Federal Trade Commission and Attorney General Jim Hood's office.

Attached to this press release are statements from BancorpSouth and Renasant Bank regarding this activity.



---

*for more information contact:*

Commissioner Brandon Presley ~ P.O. Box 1174 ~ Jackson, MS 39215-1174  
1-800-356-6428 ~ [brandon.presley@psc.state.ms.us](mailto:brandon.presley@psc.state.ms.us) ~ [www.psc.state.ms.us](http://www.psc.state.ms.us)

**May 29, 2012**

**Statement from BancorpSouth:**

*Over the Memorial Day weekend, BancorpSouth experienced an increase in the level of fraudulent type activity, often referred to as phishing, targeting numerous BancorpSouth customers and non-customers. The automated phone calls typically give the pretext of activating a debit card and ask the recipient to provide their debit card number and PIN for identification. These messages have been sent by way of cell phone calls, text messages, and email. The messages generally mention that the card number for the recipient has been deactivated. This is an effort to have the recipient contact a phone number or web site to provide card information. These calls are not legitimate. BancorpSouth will never ask for personal or account information by e-mail or solicit account information by phone. Should an account holder receive a suspicious phone call or e-mail, do NOT give out any personal or account information. In an effort to protect customer information, BancorpSouth takes certain actions, including the closing and reissuing of debit and credit cards, when the bank has reason to believe a customer's account has been compromised, or has the potential of being compromised. One should contact BancorpSouth's Call Center at 888-797-7711, or a BancorpSouth office, to verify, or to report, being contacted regarding personal account information.*

**Statement from Renasant Bank:**

*"North Mississippi has recently experienced a multitude of automated phishing attempts targeting various banks and their clients, especially in the Tupelo and Corinth areas. The automated calls, texts or emails give the pretext of activating a debit card and ask the recipient to provide their debit card number and PIN for identification. These calls, texts and emails are not legitimate," said John Oxford, director of external affairs for Renasant Bank. "We believe these phishing attempts are done at random and are not targeted towards any specific financial institution. If you believe you have been a victim of a phishing attempt, please contact your financial services institution immediately."*