

## **FOR IMMEDIATE RELEASE**

Contact: Bill Harrod, COO  
First Harrison Bank  
812-738-2198

### **Con artists step up Southern Indiana phone scam with fraudulent emails.**

Corydon, IN – A bank scam that began with phony automated telephone calls to households in the 812 area code has increased and taken a new twist. The phone calls, which told Southern Indiana residents that their bank cards had been deactivated – then asked them to enter their card numbers – are now being followed up by fake emails claiming to be in response to that scam.

One of two known emails creates the appearance that it is from First Harrison Bank, and directs recipients to a Washington D.C. telephone number. That number is answered by an automated message for “Teachers Credit Union” and asks consumers, once again, to enter their card number. Another email includes a link to a website with a First Harrison logo and asks for a card number, expiration date and personal identification number (PIN).

“We, or any bank, would never ask for that information online, on the phone or in person,” said Bill Harrod, First Harrison COO. “Unfortunately, some consumers don’t realize that until it’s too late.”

Harrod continued, “this is a sophisticated fraud that’s being perpetrated by con artists, possibly outside the United States, on individuals as far away as the west coast. Bank data has not been compromised as a result of the scam, save for that of a handful of victims who have given the scammers their bank card numbers. Right now we’re advising customers of all banks in the area not to respond to phone calls or emails they may receive in regard to their bank cards.”

To combat the scam, First Harrison Bank has blocked all activity to the countries where fraudulently used card numbers have been traced. First Harrison has also refunded money that was stolen. They are providing full cooperation to the FBI and Office of Thrift Security (OTS) in the on-going investigation.

First Harrison Bank cautions all bank customers not to reveal confidential information to any caller or email. If they suspect their bank card information has been compromised in any way, customers should contact their bank immediately.

###