

## **For Immediate Release**

### **CONTACTS:**

**Leo Ditchcreek – President / CEO**  
**Rick Burden – Senior Vice President / CLO**  
**Notre Dame Federal Credit Union**  
**574/239-6611**  
**800/522-6611**

On January 20, 2009, Heartland Payment Systems, the nation's sixth-largest provider of credit and debit card payment processing services, announced that its processing systems had been breached sometime last year, allowing thieves to capture confidential customer card data from the magnetic strip on the back of the card. The compromised data includes name, card number, expiration date, and CVV values.

Heartland Payment Systems, Inc., headquartered in Princeton, New Jersey, offers credit and debit card processing to more than 250,000 merchants nationwide, and handles over 4 billion transactions per year. **Notre Dame Federal Credit Union is not a merchant, nor does Heartland process payments for Notre Dame Federal Credit Union.** Notre Dame Federal Credit Union members were affected due to a breach of Heartland's system on which information regarding a payment method (credit or debit card) was stored. These payments were made to merchants who process payments through Heartland.

Although the exact number of affected cards is not yet known, it is expected to be many millions, making this data breach the largest to ever occur.

Due to the severity of the situation, Notre Dame Federal Credit Union has blocked any cards that have been reported compromised. As of January 23, the number of cards that have been blocked is just over 2,000. The decision to block the affected cards was made for the cardholder's protection, as well as for that of the credit union. Thus far, Notre Dame Federal Credit Union has not discovered any fraud on its members' accounts. However, the threat of fraud is very real, and therefore, all exposed cards were blocked, and new cards have been issued for affected members.

To help protect themselves, members should carefully examine their accounts online, or review their monthly statement. If any suspicious activity is noticed, members should contact Notre Dame Federal Credit Union immediately.

In the event that fraud does occur due to Heartland Payment System's data breach, Notre Dame Federal Credit Union members are protected. Visa<sup>®</sup> debit cardholders are protected with Visa's Zero Liability\* policy, which means cardholders pay nothing for unauthorized purchases. Visa's Zero Liability policy covers U.S.-issued cards only and does not apply to commercial credit cards, ATM transactions or PIN transactions not processed by Visa.

Furthermore, upon notification of fraudulent activity, Notre Dame Federal Credit Union will credit its members' accounts for the full amount of the fraudulent activity – on the same day of notification.

For more information regarding the Heartland Payment Systems data breach, please visit [www.2008breach.com](http://www.2008breach.com).

To contact Notre Dame Federal Credit Union: 800/522-6611 or [ndfcu@ndfcu.org](mailto:ndfcu@ndfcu.org).