



ALERT 0920

To: Primary Contact
From: Risk Management
Re: Preliminary Report of New Payments Industry Data Compromise
Date: February 11, 2009

Action May Be Required

The Risk Office Team has received information from Visa and MasterCard regarding the confirmed compromise of a U.S.-based acquirer processor. Please note that the compromised card alerts for this event are *not* related to the Heartland Data Systems' breach.

Given that confirmation of the Heartland breach and this new compromise occurred in such close proximity, it's possible that the same card numbers could appear on compromised card lists associated for both events. You may wish to take this into consideration as you execute your organization's monitoring and/or reissue plans for recently compromised cards.

Visa's preliminary investigation has revealed the following:

- A U.S.-based acquirer processor has confirmed unauthorized access to its settlement system.
- Evidence of a SQL injection on processor server.
- Data elements at risk are account numbers and expiration dates only.
- Card not present fraud has been reported.
- All card brands are involved.

Thus far, it has been determined that this is a significant event and we are receiving an increased number of compromised card alerts. Preliminary findings, however, indicate that the scope will be smaller than the recent Heartland breach.

Based on prior cases of this nature, we expect to receive additional compromised card alerts from the networks. If your institution is affected, you may expect to receive additional details directly from the networks or from your debit card sponsor.

We are continuing to monitor this event closely, and we will update you if and when we receive any new information.

In the meantime, if you have any questions, please contact eft_investigations@fiserv.com.