



FRAUD SCHEME

Please be cautious—contact your merchant Risk Department if you are suspicious of any transaction

Synopsis

We are receiving reports of a fraud pattern targeting hotel, bed and breakfast and other similar recreation service type businesses.

How fraud is perpetrated

Typically, the fraud is executed by a suspect stealing a cardholder account number or by using an account generation program. The suspect may have obtained additional account holder information (e.g., CVV2, Expiry Date, etc.) as well as other data elements. The suspect then attempts to use the stolen card account for a transaction with business owners at an amount greater than the required transaction. The suspect ends the scheme by requesting the business owner mail the transaction difference back to them through a wire transfer or money order service.

This fraud scenario typically transpires as follows, with all correspondence taking place via e-mail:

- Fraudster e-mails merchant inquiring about room availability
- Fraudster explains that they have other family members who need accommodations and provides date range for reservation (typically 5-7 nights)
- Merchant advises customer on room availability and price
- Fraudster agrees to rates and provides payment card information
- At this point, the fraudster requests the merchant add an additional amount to the transaction to cover additional expenses for the fraudster's family members. The fraudster will then claim that their travel consultant does not have a facility to charge their payment card.
- Fraudster instructs merchant to wire transfer the additional fee amount to a third party where it can be picked up

Recommended Strategies and Best Practices

We strongly recommend heightened vigilance in your authorization strategies for future "Card Not Present" transactions. Fraud Investigations and Incident Management recommend the following best practices for this fraud scenario:

- Merchants should authorize transactions for the actual purchase amount, not for additional or "future" sums for which a customer may seek reimbursement.
- Merchants should be advised to contact their acquirer or processor if they are suspicious of a transaction.

5405 Utica Ridge Road, Suite 110 Davenport, IA 52807 direct#: 563.359.9564 fax#: 563.359.0480

www.trisourcesolutions.com

TriSource Solutions™ LLC is a registered ISO/MSP of Merrick Bank Corporation, Woodbury, N.Y.