Fraud Alerts for University Travel & Meeting Cards

On rare occasion, a fraudulent transaction may occur on a University travel or meeting card. Unauthorized activity by the merchant, or unexpected/unintended use by the merchant, is considered misuse.

You can take action and guard against fraud by learning the methods perpetrators often use to commit fraud. Some types of fraud include the following:

- Merchant network or processor weakness. Vulnerable merchant networks are accessed using malicious software, or some other tool, to identify files and credit card information. Unsecured wireless networks at retail stores are particularly vulnerable.
- Skimming. A card reading device placed on a merchant terminal captures magnetic strip data. Skimming most commonly occurs at hotels, restaurants, ATMs, and unattended gas pumps. Cameras can also be used to collect key-entered information, such as a user's PIN.
- Theft at the merchant. Stolen merchant computer equipment, or pilfered receipts/transaction records, can occur.
- Phishing/Social Engineering. Perpetrators gain access to critical systems by tricking the merchant or cardholder into providing confidential security credentials via fraudulent email, phone, or text messages that appear legitimate.
- Credit master. Perpetrators use an algorithm to generate and test valid account numbers and expiration dates. This process usually begins with the thief obtaining one or more valid account number and expiration date pairs.

Enroll in Fraud Alerts

JPMorgan offers an option to enroll in fraud alerts. Click on the above link to receive notifications on your mobile and via email for any suspicious account activity.

For more information on travel and meeting cards, contact the TravelND helpdesk at travel.nd.edu or (574) 631-4289.