## March 06, 2014

## SCAMS TARGETING MERCHANTS

The FBI is aware of various scams pertaining to re-loadable pre-paid debit cards, but specifically wants to alert the public on a bomb scare scam targeting businesses.

One scenario is scammers begin calling businesses and fraudulently representing themselves as a utility company employee and advising the utility bill payment is past due. The caller claims the service will be terminated unless payment is made immediately. Acceptable forms of immediate payment are Green Dot "MoneyPak" cards purchased from a local convenience store or a valid credit card or bank account information. Once the account numbers from the MoneyPak, credit cards, or banks are provided, the scammer removes the funds associated with the MoneyPak or steals funds from the accounts.

A second scenario involves a scammer who calls in a bomb threat to a retailer and demands to speak with the manager. Instructions are provided to the store manager to purchase and activate Green Dot MoneyPak cards with \$500 loaded on each card. The card numbers are to be read to the scammer over the phone. If managers do not comply, the caller threatens to blow up the establishment and continues to threaten store employees' homes and families.

In all reported instances, no manager has complied with the caller, and no explosive devices have been found.

According to MoneyPak.com, Green Dot MoneyPak cards are convenient and easy to use and can be purchased at participating retailers. There is a \$4.95 charge associated with the MoneyPak card, but after purchase, it can be used to "reload prepaid cards, add money to a PayPal account without using a bank account, or make same-day payments to major companies." MoneyPak cards are similar to wire transfers and are untraceable.

Several law enforcement agencies and media outlets across the United States have issued alerts on their websites pertaining to various scams associated with prepaid Green Dot MoneyPak cards.

To receive the latest information about cyber scams, go to FBI.gov and sign up for e-mail alerts by clicking on the red envelope labeled "get FBI updates." If you have received a scam e-mail, notify the IC3 by filing a complaint via <a href="www.ic3.gov">www.ic3.gov</a>. For more information on e-scams, please visit the FBI's "New E-Scams" and Warnings webpage at <a href="http://www.fbi.gov/scams-safety/e-scams">http://www.fbi.gov/scams-safety/e-scams</a>.