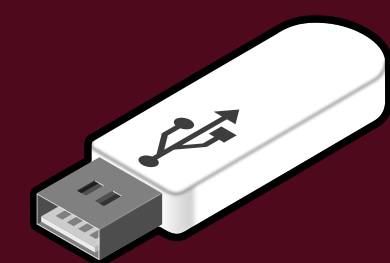# DON'T BE THE NEXT VICTIM

Not securing credit card terminals can cause financial headaches. Here are the steps you can take *now* to prevent and detect fraud.

## SECURE THOSE DEVICES!

Credit card equipment should be stored in a location free from unauthorized access when the machine is not in use.

## LOOK FOR TAMPERING

Periodically inspect the device for the following:

- Scratches/damage to the device
- Items attached to the device, such as USBs, skimmers, etc.

← Skimmer

## RECONCILE, RECONCILE, RECONCILE

Review batch detail reports for:

- Unauthorized transactions (including refunds/credits)
- Duplicate transactions
- Errors (incorrect amounts)

## SUSPECT FRAUD?

**1** Immediately contact the merchant bank

**2** Contact the Archdiocesan Director of Internal Audit
*Phone: 314-792-7241*
*E-mail: InternalAudit@archstl.org*

**BROUGHT TO YOU BY THE OFFICE OF INTERNAL AUDIT**
archstl.org/internalaudit