ARCHDIOCESE OF ST. LOUIS
Cardinal Rigali Center
20 Archbishop May Drive
St. Louis, Missouri 63119

Office of Internal Audit
p) 314.792.7241
f) 314.792.7145
InternalAudit@archstl.org
www.archstl.org/internal-audit

RISK ALERT

Date: **November 4, 2021**

To: **All Parishes, Offices and Agencies**

Cc: **Cory Nardoni**

From: **Internal Audit**

Subject: **Security of Payment Devices**

Recently, an Archdiocesan office's point of sale credit card terminal was used in several attempts to post fraudulent credits or refunds to a personal credit card or gift card. Please remind all of your parish, department and agency employees of the importance of maintaining proper controls to prevent fraudulent transacations on credit cards terminals.

Physical Security Controls

Credit card equipment should be kept in a secure location with limited access when the equipment is not in use to prevent unauthorized individuals from gaining access. Unauthorized individuals may include volunteers, maintenance staff, janitorial staff, other employees, visitors, etc. If possible, password/pin protect the credit card terminal and ensure that the default password/pin has been changed.

Inspect Your Credit Card Terminal Regularly

Establish a routine for inspecting your devices for signs of tampering. These include looking for:

- Signs that indicate potential attempts to tamper with the device, such as scratches or damage on the plastic covering. These could appear near seams and connection ports. Consider placing a sticker over the seam of the device to prevent potential tampering.
- Objects, such as skimmers, attached to the front of or behind card swiper slots.
- Items plugged into ports such as USB thumb drives, which are becoming increasingly small and are easy to miss when inspecting your devices. To give your equipment a full inspection, completely unplug it and examine the underside, the back and the front for anything plugged into ports or attached to the credit card terminal.

Reconcile, Reconcile, Reconcile

Credit card transactions should be batch/transmitted on a daily basis. A batch detail report should be generated for the credit card transactions. This report should be reviewed for unusual transactions and compared to the transactions recipts and manual sales records or transaction logs. Unusual transactions could include the following:

- Unauthorized transactions, including refunds or credits
- Duplicate transactions
- Mis-keyed transactions

Suspected Fraud Cases

In the event you suspect that unauthorized transactions may have occurred or your credit card terminal has been tampered with, please contact the merchant bank and the Director of Internal Audit immediately.

Please contact the Office of Internal Audit if you have any questions or concerns. In the meantime, stay safe, and God Bless.