**MEMORANDUM**

**To:** Volunteer Leaders

**From:** TU Staff

**Date:** July 17, 2014

**Re:** Personal Confidential Information – Handling Credit Cards

The high profile credit card breaches of Target and Neiman Marcus this past year are a great reminder to review your credit card handling procedures to minimize the chances of that happening to your chapter or council.

Personal Confidential Information consists of a person's name, their credit card number, expiration date and the security code on the card. The handling of this information should be done with the utmost care and under no circumstances should this information be kept, even in storage, after the credit card transaction has been authorized by your credit card processing vendor.

Tips for Handling Credit Card Information

- Do not accept credit card information via email or send it via email. Should you receive this information, delete the email immediately and ask the donor/volunteer not to do that again.
- Ensure than any computers used to process credit card information have up-to-date firewall and virus software installed (This includes cell phones and iPads.)
- Buy and use only point-of-sale machines and software from reputable banks and merchant services companies. These banks and companies should be able to tell you that their device has been validated by the PCI Security Standards Council to be in compliance with the Data Security Standards.
- Monitor volunteers collecting credit card data. Remind them of the need to be sensitive to the information collected and careful how they handle it.
- Keep the software up-to-date on your point-of-sale machine.
- Use strong passwords and change them at least quarterly but ideally monthly. (A strong password is at least 8 characters in length and has a combination of upper and lower case letters, numbers and special characters.)
- Do not use paper to collect credit card data. If you are still using the old carbon paper machines, please reach out to your merchant services provider and get a point-of-sale machine.

If you are trying to figure out how to accept credit cards at your events, work with your local bank. Most have merchant services departments that can properly guide you and help you take payments by credit cards in a secure fashion.

What to do if you believe Personal Confidential Information was compromised

Unfortunately reporting requirements range in complexity and vary by state. In general, you will be required to notify all possible donors whose data passed through the compromised machine within a certain time period of the breach. You will also be required to notify the credit card companies, many of whom will fine you or remove your right to process their card in the future. Should you believe this has happened, please notify TU National staff as soon as possible, and the staff will assist you in finding an attorney who can guide you through this process.

Upcoming changes to credit cards

By the end of 2015, all credit card issuers in the United States (Visa, MasterCard, Discover, etc.) are required to issue credit cards with microchip and PIN technology. They have been doing this overseas for several years. If you have an older point-of-sale machine or are using a computer and browsing to a screen for your volunteers to key information into, you should be contacted to replace these machines or to get an additional device for your computer for individuals to type in their PIN. If you do not have a point-of-sale machine and are looking for one now, get one that is already enabled to accept PIN information.