# Sample of Procedures for Processing Payment Cards

University of Illinois at Chicago
Department of Disability and Human Development
Assistive Technology Unit

## Credit Card Processing Procedures

1. The Assistive Technology Unit (ATU) will accept Visa, MasterCard, American Express, and Discover Card payments for services rendered.

2. The ATU will comply with the Payment Card Industry Data Security Standard (PCIDSS).

3. The ATU will designate a Fiscal Officer (William Barrett), an Operations Manager (Karen Haasen) and a Dispute Resolution Contact (Raymon Cunha).

4. The following are procedures for processing credit cards transactions when the card is present (i.e., face to face transaction):

- Swipe the card through the terminal/point of sale device.
- Obtain authorization for every card sale.
- Ask the customer to sign the sales receipt. Only the last 4 digits of the credit card number are printed on the receipt.
- Match the embossed number on the card to the four digits of the account number displayed on the terminal
- Compare name and signature on the card to those on the transaction receipt. Request an ID at the point of sale to verify the cardholder is using the card when appropriate for further validation (but is not required).
-

5. The following are procedures for processing credit card transactions when cardholder information is taken over the phone, mail order or at a restricted accessible, non-digital fax machine (i.e., card is not present). The ATU will not send or accept payment card information via email.

- Obtain cardholder name, billing address, account number, and expiration date.
- Do not retain documents containing full card number or expiration date and destroy with crosscut shredder once the transaction has been authorized.
- Request the Security Code (the three digit code on the back of the card in the signature panel or as embossed on front of card if an American Express card) and validate the code at the time of authorization electronically (through the POS

device). This code will be destroyed with a crosscut shredder once validated; it will not be stored physically or electronically.
- Verify the customer's billing address electronically (by entering the zip code in the POS device)
- Key the payment information in manually into the processing system

6. For any paper that contains sensitive card information, the ATU will follow these procedures:

- Store all materials containing cardholder account information in a restricted/secure area. These materials will be kept in a locked file cabinet in Room 415 of the DHSP Building, which is the ATU's main office. This office is closed and locked when no personnel are present. Only the Operations Manager and the Dispute Resolution Contact will have a key to the locked file cabinet containing any forms with cardholder information.
- Individuals with access to cardholder information will be limited to only those persons whose job requires such access as stated above.
- Sensitive Authentication data such as CVC2/CVV2/CID or expiration date will never be stored subsequent to authorization. The PIN will never be stored. All documents containing sensitive cardholder data will be shredded using a crosscut shredder.
- If paper records containing payment card account numbers are stored, all but the last four digits will be redacted within 60 days, or as soon as refunds or disputes are no longer likely, but no more than 180 days. A china marker will be used for redaction.
- Printed customer receipts that are distributed outside the unit will show only the last four digits of the payment card account number.
- The ATU will not store card information in a customer database or electronic spreadsheet.

7. Credit card receipts will be maintained for the retention period as specified University of Illinois policy. Currently, University of Illinois procedures recommend keeping all transaction records until the new guidelines have been released.

- Access to the physical location of stored credit card receipts will be in a restricted area where authorized persons can be easily identified and access to the area can be limited and restricted.
- Cardholder information will not be taken or distributed for unauthorized purposes.

8. Depositing and Reporting Charge Sales

- The ATU will perform a credit card transaction settlement procedure at the end of the business day. A batch settlement report is produced at this time.

- The batch settlement report will be attached to the individual sales receipts and filed as outlined above.
- The ATU will also maintain a control log of the daily sales transactions.
- The ATU will perform a monthly reconciliation to ensure that the credit card sales log balances to the amounts posted to BANNER GL. The reconciliation worksheets will not contain card information to expose the full card number (only the last four digits), expiration date, or card security code (CVC2/CVV2/CID) but will be retained in a locked cabinet.

9. Refunds

When an item or service is purchased using a payment card and a refund is necessary, the refund will be credited to the same account from which the purchase was made. Under no circumstances will a refund be issued with cash or a check. A refund will never exceed the original payment amount.

If any portion of a payment is non-refundable, the ATU will declare this information to the customer before the transaction is processed and the customer must provide a means of acknowledgement (e.g., signature) that they understand and accept the terms of the payment.