

The University of Georgia

Credit/Debit Card Processing Procedures

The University of Georgia currently accepts four major credit cards (MasterCard, Visa, Discover and American Express) for payment of services rendered and goods sold. Debit cards with the Visa or MasterCard logo are also accepted. All University departments are required to process card transactions through the merchant services provider selected by the University and/or the state of Georgia. Effective January 1, 2004, the State of Georgia selected FirstData and Suntrust Merchant Services as the state-wide provider.

General guidelines

- 1) Any University Unit wishing to accept credit/debit card for goods and/or services should complete a Credit/Debit Card Processing Application (www.bursar.uga.edu).
- 2) Upon approval, the Bursar's Office will request a merchant id for the University department from the merchant services provider. If the department will be conducting e-Commerce, an e-Commerce merchant id must be established which is separate from any point-of-sale merchant id.
- 3) The Bursar's Office will work with the department regarding the purchase of all card processing terminals. Effective July 1, 2004, all card equipment that prints a receipt is required to truncate the card number on the customer receipt.
- 4) If specialized software and/or systems are required, the Bursar's Office, the Chief Information Security Officer, Internal Auditing, and the applicable computer support unit will work with the department to ensure that processing standards and safeguarding measures are met.
- 5) University units should not store any sensitive cardholder data. To the extent possible on e-Commerce transactions, the sale transaction should not take place on University computers or network resources. It is acceptable for Point of Sale devices to store the sensitive cardholder data on their device until transactions are settled; once settlement occurs, no information should be stored electronically.
- 6) On a daily basis, the department must balance transactions and settle their sales electronically to the merchant services provider.
- 7) The department will complete and send the credit/debit card transmittal form to the Bursar's Office so that the sales revenue can be recorded in the University Accounting System. Transmittal forms summarizing the settled sales should be sent to the Bursar's Office by fax or email no later than noon of the day following settlement. The credit/debit card sales transmittal form is available at: http://www.busfin.uga.edu/forms/credit_card_transmittal.pdf.
- 8) All departments accepting credit/debit cards for payment must comply with the University of Georgia Credit/Debit Card Processing Policy and the University's Customer Information Security Program (UGA Gramm Leach Bliley Policy) to protect the private financial information of University customers. The policy is available at: <http://www.uga.edu/audit/glba/index.html>

Guidelines for Point-of-Sale Transactions

- 1) The Bursar's Office will coordinate all credit/debit card processing for the University. No individual department may enter into a contract with a credit/debit card processor without approval of the Bursar's Office and the Senior Vice President of Finance and Administration.
- 2) All card transactions will be processed on equipment compatible with the processing platform(s) of the University's card processor. As of January 1, 2004, the University's card processor is FirstData/Suntrust Merchant Services which is the card processor selected by the State of Georgia.
- 3) Effective July 1, 2004, all customer receipts must truncate the card number so that only the last four digits are printed.
- 4) Departments requiring customized equipment for point-of-sale transactions must contact the Bursar's Office before such equipment is purchased. The Office of Information Security will be consulted prior to equipment purchase.
- 5) In order to reduce fraud, credit card companies recommend the following procedures for processing cards when the card is present (i.e. a face to face transaction):
 - It is recommended that you ask for an ID at the point of sale to verify that the card member is using the card.
 - Always swipe the card through the terminal/point of sale device, if applicable.
 - Obtain authorization for every card sale.
 - Ask customer to sign the sales 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.
 - If you believe the card member or card sale is suspicious, make a Code 10 call to your voice authorization center for card being used.
- 6) If cardholder information is taken over the phone or via fax (i.e. card is not present), in order to reduce fraud, the following guidelines are recommended:
 - Obtain cardholder name, billing address, shipping address (if different from billing address and if applicable), account#, and expiration date.
 - Verify the customer's billing address either electronically (by entering the zip code in the POS device) or by calling the credit card automated phone system (Address Verification System - AVS).
 - Request the Security Code (the three-digit code on the back of the card in the signature panel) and validate the code at the time of authorization either electronically (through the POS device) or by calling the credit card automated phone system. This code should be destroyed once validated; it should not be stored physically or electronically.
 - Get a signature for each delivery that is not the card member.
 - Maintain credit card receipts and all delivery records for the retention period as specified in #13 below.

- 7) UGA units should not accept credit/debit card information via email.
- 8) All point-of-sale terminal transactions must be batched and transmitted to the card processor on a daily basis.
- 9) Sales totals (net of refunds) must be reported to the Bursar's Office on a credit card transmittal form (http://www.busfin.uga.edu/forms/credit_card_transmittal.pdf) no later than noon the day following the day of settlement. These forms should be faxed to 706-542-3959 or e-mailed to bursar@uga.edu.
- 10) It is important that departments reconcile their point-of-sale transactions and report the sales amounts to the Bursar's Office. The department's transmittal should be the origination point; the Bursar's Office should not report the sales amount per the credit card processor reports to the department in order for the department to prepare the transmittal.
- 11) The Bursar's Office will compare the sales amount per the transmittal to the records at the card processor and will immediately inform the department of discrepancies. All discrepancies should be resolved within 24 hours so that sales can be posted to the departmental account in the UGA Accounting System on a timely basis.
- 12) When the Bursar's Office receives charge back inquiries from the credit card companies, the applicable department will be contacted to provide the necessary information about the sales transaction in question.
- 13) Departments should maintain adequate records of the sales transactions. Daily sales totals, logs, etc. substantiating revenue should be stored for 5 years in accordance with state record retention policies (Records Retention Series A, <http://www.usg.edu/usgweb/busserv/series/>). Individual receipt slips and other documents with cardholder data should be stored in a locked filing cabinet or safe and only need to be retained for 12 months. In order to dispute a charge, customers must report the item to the credit card company within 12 months of the date of sale. At the time of disposal, all documents containing sensitive cardholder data should be shredded using a cross-cut shredder.

e-Commerce Transactions

- 1) The Bursar's Office will coordinate all e-Commerce processing for the University. No individual department may enter into a contract with a card processor without approval of the SVPFA, CIO or delegate(s).
- 2) Departments should contact the Bursar's Office prior to purchase of specialized software or equipment so that customized processing applications are reviewed in conjunction with policy and procedure. The Bursar's Office, the Chief Information Security Officer, Internal Auditing, and the applicable computer support unit will work with the department to ensure that processing standards and safeguarding measures are met.

- 3) All card transactions will be processed through a payment gateway approved by the SVPFA and the CIO.
- 4) To the extent possible, card processing transactions should be performed on the website of the payment gateway (i.e. the customer should enter sensitive cardholder data on a payment engine website) and not on University computer or network resources.
- 5) No department should store any sensitive cardholder data on any UGA server or PC. All sensitive cardholder data should be maintained by an approved service provider. All outside service providers must comply with the security programs of Visa CISP, MasterCard SDP, American Express DSS, and Discover's Merchant Operating Regulations.
- 6) All ecommerce transactions must be batched and transmitted to the card processor on a daily basis.
- 7) Sales totals (net of refunds) must be reported to the Bursar's Office on a credit card transmittal form (http://www.busfin.uga.edu/forms/credit_card_transmittal.pdf) no later than noon the day following the day of settlement. These forms should be faxed to 706-542-3959 or e-mailed to bursar@uga.edu.
- 8) It is important that departments reconcile their ecommerce transactions and report the sales amounts to the Bursar's Office. The department's transmittal should be the origination point; the Bursar's Office should not report the sales amount per the credit card processor reports to the department in order for the department to prepare the transmittal. Departments will be given web access to the payment manager database which houses the card transactions. This will enable the department to perform reconciliation and research.
- 9) The Bursar's Office will compare the sales amount per the transmittal to the records at the card processor and will immediately inform the department of discrepancies. All discrepancies should be resolved within 24 hours so that sales can be posted to the departmental account in the UGA Accounting System on a timely basis.
- 10) When the Bursar's Office receives charge back inquiries from the credit card companies, the applicable department will be contacted to provide the necessary information about the sales transaction in question.
- 11) Departments should maintain adequate records of the sales transactions. Daily sales totals, logs, etc. substantiating revenue should be stored for 5 years in accordance with state record retention policies (Records Retention Series A, <http://www.usg.edu/usgweb/busserv/series/>). Individual receipt slips and other documents having cardholder data should be stored in a locked file cabinet or safe and only need to be retained for 12 months. In order to dispute a charge, customers must report the item to the credit card company within 12 months of the date of sale. At the time of disposal, all documents containing sensitive cardholder data should be shredded using a cross-cut shredder.

Technical Specifications:

Each University unit processing credit/debit cards will be responsible for adhering to the credit card merchants' data security program. The Office of Information Security will maintain links to the various merchant's data security programs at:

<http://www.infosec.uga.edu/standards.html>.

Any questions with regard to the technical specifications should be directed to the Chief Information Security Officer.

Each merchant id assigned will have at least one person subscribed to the ecomm and ecomm-tech listservs for updates on credit/debit card policy and procedure.

Exceptions to Policy:

In order to be granted an exception to the policy please submit "Request for Exception" located at: www.bursar.uga.edu.

Request should include:

- Reason for requesting exception.
- Steps that are being taken to become compliant with the policy.
- Date your division is expected to become compliant.

The Bursar's Office will work with the SVPFA and the CIO to determine if an exception to the policy can be granted.