

June 27, 2001

TO: Janet Hamilton, Vice Chancellor  
Administration

SUBJECT: CREDIT AND DEBIT CARD PROGRAM POLICY REVISIONS

At the beginning of the year, Information and Educational Technology (IET) appointed an Electronic Credit/Debit Card Transaction Workgroup to review security controls and merchant accounting requirements for accepting and processing credit card transactions over the Internet. The workgroup consisted of representatives from the IET, Office of Administration and Internal Audit Services. As a result of the workgroup findings, we recommend the Office of Administration incorporate the attached provisions into the Credit and Debit Card Program Policy (PPM 330-41).

The recommendations are intended to augment the existing web processing provisions of the draft Credit and Debit Card Program Policy (Section IV.4. Web Processing). As the Office of Administration moves forward with the implementation of the Internet credit card policies, IET would like to serve as a partner in this effort. We believe IET can play an important role in assisting the Office of Administration to develop, implement and support a secure, available, accurate and cost-efficient authorization, settlement and recording system for Internet credit card transactions. We look forward to this collaborative work.

If your staff would like to discuss the recommendations, please have them contact Dave Shelby, at 754-5266, or Bob Ono, at 754-6484.

Sincerely,

John Bruno  
Vice Provost  
Information and Educational Technology

CC: Lana Moffitt, Director  
Information Resources

Doug Hartline, Director  
Communication Resources

Dave Shelby, Chief Operations Officer  
Information and Educational Technology

Robert Ono, IT Security Coordinator  
Information and Educational Technology

Attachment

# Recommendations for Revision to Credit and Debit Card Program Policy (PPM 330-41)

## Information and Educational Technology

June 27, 2001

We recommend the draft Credit and Debit Card Program Policy (330-41) be revised by addition of the following provisions:

- 1) The Vice Chancellor of Administration must approve all Internet retail offerings that require the acceptance of credit and/or debit cards. The use of debit cards for Internet payments is not encouraged due to the general lack of consumer demand for such Internet services.
- 2) Internet web sites that accept credit cards must notify cardholders that credit cards will not be accepted for the purpose of cash advances.
- 3) Internet web sites that accept credit cards must clearly state the return policy and procedures and methods to resolve any disputes regarding purchased merchandise and/or services. Payment of refunds or adjustments to a cardholder must be made by crediting the customer's card account number.
- 4) Campus units accepting Internet credit card payments for on-line purchases must use a campus designated Internet payment gateway solution for transaction authorization. The Office of Administration will coordinate the selection of the campus Internet payment gateway. All Internet retail components, such as customer information collection, shopping cart functionality, order confirmation, fulfillment and settlement must be capable of being integrated with the campus Internet payment gateway. The Associate Vice Chancellor, Finance; Director, Internal Audit Services and Information Resources Security Guidelines Coordinator must approve any deviation from use of the campus Internet payment gateway.

*Information and Educational Technology (IET) will assist the Office of Administration to prepare and evaluate an RFP to select the single Internet payment gateway vendor for retail Internet purchase authorizations and account settlement.*

- 5) Campus units should use an Office of Administration designated Internet shopping cart application in order to promote a singular look and feel for all UC Davis Internet retail transactions.

*If desired, IET will assist the Office of Administration to prepare and evaluate an RFP for online shopping cart functionality.*

- 6) The Internet transaction credit card authorization, settlement, reporting and archival functions will be automated to the greatest extent possible. DaFIS technical staff will be responsible for developing and maintaining a secure and reliable interface between the campus Internet payment gateway authorization system and Accounting and Cashier for authorization, settlement, reporting and archival purposes.

*DaFIS technical staff should be able to draw from their previous experience developing an interface between the TAPS online permit system, a credit card processor and DaFIS.*

- 7) An appendix should be added to the Credit and Debit Card Program policy specifying e-commerce information security standards for Internet-based credit card authorization, settlement, reporting and archival requirements (See Appendix A, Security Standards).

*The appendix must be consistent with e-commerce information security provisions required by major card-issuers. Due to changing business requirements for Internet credit card transactions, the appendix will require periodic review and updating. IET will provide the leadership and resources to the Office of Administration to maintain the information security appendix.*

- 8) Use of the campus designated Internet payment gateway system for retail web-enabled purchase transactions will follow one of three models (See Appendix B, Model Matrix).

a) Model 1: Central Service for UC Davis E-commerce

- i) Development of the e-commerce application and retail functionality will be the responsibility of the sponsoring campus unit. The campus unit may choose to use the campus e-commerce shopping cart application in order to provide Web users with a similar look and feel across UC Davis e-commerce applications and to reduce development costs.
- ii) The e-commerce application, web server(s), supporting backend systems and Internet payment gateway must be housed in a secure data center. Backend systems are defined as including transaction databases and integration applications between DaFIS and account settlement functions.
- iii) E-commerce applications, web server(s), supporting backend systems and Internet payment gateway will be maintained by central service technical staff to campus e-commerce information security standards. Central service technical staff will be responsible for support of the campus e-commerce web server complex, including performance issues relating to security and load balancing.
- iv) The secure data center must maintain Internet payment gateway transaction records in accordance to UC policy and e-commerce information security standards. Upon the request of the Accounting department and/or campus credit card processor, transaction information must be available in the event of a cardholder dispute over

the nature, quality or performance of the goods or services or in the connection with any return or rejection of such goods and services.

- v) Network traffic to e-commerce web servers and backend systems will be controlled by central service technical staff, consistent with the campus e-commerce information security standards.
- vi) E-commerce data center compliance to the campus e-commerce information security standards will be subject to periodic audit by Internal Audit Services. Substantial deviation from compliance to policy provisions, as determined by Internal Audit Services, will require immediate corrective action.

b) Model 2: Campus unit Operated E-commerce Web Server and Central Service for Internet Payment Gateway and Supporting Systems.

- i) Development and maintenance of the e-commerce application and retail functionality will be the responsibility of the sponsoring campus unit. Campus units may choose to use the campus e-commerce shopping cart application in order to provide Web users with a similar look and feel across UC Davis e-commerce applications and to reduce development costs.
- ii) Any campus unit e-commerce web server supporting online credit card transactions will use a web server dedicated to e-commerce applications.
- iii) The campus unit hosting the Internet retail function will control network traffic to isolated department e-commerce web servers, as required by the campus e-commerce information security standards.
- iv) Network traffic to central payment transaction systems will be controlled by central service technical staff, consistent with the campus e-commerce information security standards.
- v) The Internet payment gateway and supporting backend systems will be maintained by the central service data center to campus e-commerce information security standards. Backend systems are defined as including transaction databases and integration applications between DaFIS and account settlement functions.
- vi) The central data center must maintain Internet payment gateway transaction records in accordance to UC policy and e-commerce information security standards. Upon the request of the Accounting department and/or campus credit card processor, transaction information must be available in the event of a cardholder dispute over the nature, quality or performance of the goods or services or in the connection with any return or rejection of such goods and services.
- vii) E-commerce data center compliance to the campus e-commerce information security standards will be subject to periodic audit by Internal Audit Services. Substantial deviation from compliance to policy provisions, as determined by Internal Audit Services, will require immediate corrective action.

c) Model 3: Campus Unit Accepts Full Responsibility for Operating Internet Payment Gateway and Supporting Services

- i) Development, maintenance and support of an e-commerce application, credit card authorization and retail functionality will be the responsibility of the sponsoring campus unit. In order to carryout this responsibility, the campus unit may choose to perform all the necessary work itself or contract with an external organization to host the e-commerce function.
- ii) If hosting the e-commerce application itself, the campus unit will:
  - (1) Use the campus e-commerce shopping cart application, if feasible, to promote a similar look and feel across UC Davis e-commerce applications and to reduce development and support costs.
  - (2) Use the campus designated Internet payment gateway product. The campus unit may choose to use available Internet payment gateway contract rates negotiated by the Office of Administration or negotiate a separate contract. Any use of an Internet payment gateway product that varies from the campus selection, must be approved by the Associate Vice Chancellor, Finance; Director, Internal Audit Services and IT Security Coordinator. In addition, any use of a non-campus supported Internet payment gateway will require the campus unit to be responsible for all related costs to automate the integration of the gateway with the DaFIS settlement function.
  - (3) Maintain supporting transaction records in accordance to UC policy and e-commerce information security standards. Upon the request of the Accounting department and/or campus credit card processor, the organizational unit must be able to ensure the availability of this information in the event of a cardholder dispute over the nature, quality or performance of the goods or services or in the connection with any return or rejection of such goods and services.
  - (4) Ensure e-commerce applications, web server(s), supporting backend systems and Internet payment gateway will be housed on a secure network location isolated from other network devices and hosts.
  - (5) Ensure web servers and databases supporting online credit card transactions are dedicated to only e-commerce functions.
  - (6) Ensure network traffic between department e-commerce web and database servers and from e-commerce servers to external hosts are consistent with campus e-commerce information security standards.
- iii) It is the responsibility of the individual campus unit to ensure e-commerce applications, web server(s), supporting backend systems and Internet payment gateway are developed and maintained to campus e-commerce information security standards. If a campus unit contracts with an external organization to host all or part of the e-commerce application, it is the responsibility of the campus unit to require the contractor to meet or exceed credit-card issuer privacy and security requirements.

iv) Campus unit compliance to the e-commerce information security standards will be subject to periodic audit by Internal Audit Services. Substantial deviation from compliance to the standards, as determined by Internal Audit Services, will require temporary disruption of the e-commerce application for corrective action or migration of the application to the central e-commerce service (see Model 1 or Model 2). If a campus unit contracts with an external organization to host all or part of the e-commerce application, the contractor must agree to annually audit its compliance to card-issuer security requirements using an independent third-party agency. A high-level summary of the annual report is to be provided by the contractor to the campus unit.

# Appendix A: Security Standards

## Proposed E-Commerce Information Security Standards

- 1) IET will lead the development of e-commerce information security standards that comply with card-issuer (VISA/MC/AE/Discover) and credit card payment processors (FDMS) information security requirements. The standards will be an appendix to the proposed Credit and Debit Card Program Policy. Campus units, central data center operations or contractors supporting e-commerce transactions will ensure systems are compliant with the standards described below:
  - a) Physical security for web servers, Internet payment gateway and supporting backend systems
    - i) Monitor physical entry and exit through entry/exit logs
    - ii) Restrict physical entry web servers, Internet payment gateway and supporting backend systems to authorized personnel
    - iii) Ensure paper output and electronic media output is protected from unauthorized inspection/duplication/removal
  - b) Physical security for network devices
    - i) Place routers, firewalls, web servers and supporting servers in locked rooms/cabinets
  - c) Logical security controls for web servers, Internet payment gateway and backend supporting systems
    - i) Perform regular OS and application maintenance
    - ii) Encrypt sensitive data in storage (3DES or equivalent)
    - iii) Protect encryption key
    - iv) Use and maintain anti-virus controls
    - v) Perform account management
      - (1) Assign and track user unique (non-shared) ids
      - (2) Password aging in use (and/or strong authentication)
      - (3) Account lockouts after repeated invalid login attempts
      - (4) Password protected screensavers in use
      - (5) Restrictions on access to administrative accounts
      - (6) Removal of default user accounts and passwords
      - (7) Removal of user access when no longer needed
      - (8) Define authorization based on “need to know” principal
    - vi) Change default vendor software settings
    - vii) Remove unnecessary services/processes
    - viii) Maintain and review audit trails for user actions and system events
    - ix) Periodically test for security vulnerabilities
    - x) Develop and maintain host intrusion detection and alerting

- xi) Develop, test and maintain system backups (credit card backups must remain in encrypted format)
- xii) Isolate web servers and support systems from public and Internet traffic
- xiii) Restrict network traffic to e-credit web servers
- xiv) Restrict network traffic to e-credit support systems
- xv) Use directory/file/object/device access control
- xvi) Activate OS and web logs
- xvii) Protect and archive OS and web logs
- xviii) Review OS and web logs
- xix) Encrypt cardholder network traffic for web and email
- xx) Use network intrusion detection systems
- xxi) Develop and maintain incident response management
- xxii) Destroy data when it is no longer needed
- xxiii) Refrain from directly connect modems to e-credit card system or supporting systems unless strong authentication used

d) Information Security

- i) Develop and publish information security policy and standards
- ii) Post a UC Davis privacy and security statement on the Internet web pages accepting credit card information.
- iii) Assign information security responsibilities
- iv) Develop, implement and maintain security awareness for employees
- v) Perform background checks for employees handling e-credit systems
- vi) Maintain awareness to new threats and vulnerabilities impacting data integrity, confidentiality and availability
- vii) Perform security assessment on account/transaction systems prior to placement into production
- viii) Develop, implement and maintain change management process Ensure production data is not used for testing purposes
- ix) Centrally report any suspected or confirmed security/privacy breach of an e-commerce Internet payment gateway or related e-commerce databases to the campus organizations responsible for incident response.

## Appendix B: Model Matrix

Business Function	Task(s)	Primary Organizational Responsibility	Model 1 Operational Example <sup>1</sup>	Model 2 Operational Example <sup>2</sup>	Model 3 Operational Example
Business Planning and Development	Develop E-Commerce Web Application	UC Davis Campus Unit	UC Davis Campus Unit	UC Davis Campus Unit	UC Davis Campus Unit
Promote & Support of Organizational Unit Mission & Objectives	Acquire, Maintain and Support E-Commerce Web Server Host	UC Davis Campus Unit	Information and Educational Technology	UC Davis Campus Unit	UC Davis Campus Unit or External Web Host
Provide Business Function for Credit Card Payment Authorization and Account Settlement	Acquire, Implement, Maintain and Support Internet Payment Gateway Host and Transaction History Database	Office of Administration	Information and Educational Technology	Information and Educational Technology	UC Davis Campus Unit or External Web Host
Ensure Effectiveness and Efficiency of Operations, Reliability of Financial Reporting and Compliance with Applicable Laws and Regulations	Perform Periodic Review of Financial Controls, Reporting and Compliance to Laws, Regulations and Industry Best Practices	Internal Audit Services	Internal Audit Services	Internal Audit Services	Internal Audit Services or External Audit Organization for External Web Host

<sup>1</sup> Under Model 1, the support of the e-commerce web server, Internet payment gateway, credit card backend systems, and related infrastructure requirements could be delegated to IET under a service program.

<sup>2</sup> Under Model 2, the support of the Internet payment gateway, credit card backend systems, and related infrastructure requirements could be delegated to IET under a service program.

## **Appendix C: Definition of Terms**

E-commerce application – A software application that permits the conducting of retail business functions on-line via the Internet. This includes, for example, buying and selling products with credit cards, payment authorization, account settlement and fulfilling the order for goods/services.

E-commerce shopping cart - A shopping cart is a piece of software that acts as an online store's catalog and ordering process. Typically, a shopping cart is the interface between a company's Web site and its deeper infrastructure, allowing consumers to select merchandise; review what they have selected; make necessary modifications or additions; and purchase the merchandise.

Shopping carts can be sold as independent pieces of software so companies can integrate them into their own unique online solution, or they can be offered as a feature from a service that will create and host a company's e-commerce site.

Internet payment gateway – A software system that accepts credit card payment information from an e-commerce application, seeks payment authorization from a credit card issuer via a third-party processor, and provides account settlement information to the merchant.

Wednesday, June 27, 2001