

AMENDMENT  
TO THE AGENCY PARTICIPATION AGREEMENT  
FOR THE PLASTIC CARD NETWORK  
INTERNET PROCESSING

The Plastic Card Network (PCN) Agency Participation Agreement (APA) between **the Financial Management Service (FMS)**, \_\_\_\_\_ and  
\_\_\_\_\_ (Financial Institution Name)

\_\_\_\_\_  
(Agency Name)

is hereby amended to provide for the purchase or lease of goods and services and payment of fees, fines, or debts by customers through Internet processing.

**9.0 CARD TRANSACTIONS OVER THE INTERNET**

**9.1 Receiving Card Numbers over the Internet**

The Agency may accept credit and off-line debit cards from cardholders over the Internet using the World Wide Web ("Cards Received over the Internet"). The agency shall not accept card data using other Internet services, such as electronic mail.

Cards Received over the Internet shall be treated as "mail or telephone orders" until and to the extent that the card networks defined in section 2.1 of the APA generally deem otherwise.

Each Card Received over the Internet shall require the Agency to obtain an authorization from the Financial Institution or its agent prior to completing the transaction. Such authorizations may take place over the Internet. A transaction for a Card Received over the Internet shall be considered complete upon the Agency's transmittal to the Cardholder of the Agency's acceptance of the Cardholder's offer, which in no case shall take place before the Agency obtains the authorization. When the agency elects to use the FMS transaction processing server to assist in processing card transactions over the internet, the FMS transaction processing server will fulfill the authorization requirement on the agency's behalf.

For purposes of Cards Received over the Internet, Sections 2.6 (a), (c), and (d) do not apply.

**9.2 Implementation Requirements for Cards Received over the Internet**

The Agency shall use the Secure Sockets Layer (SSL) Version 3 protocol to secure Cards Received over the Internet. The Agency shall not process a transaction if an SSL Version 3 security session can not be established with the cardholder's Web browser.

The Agency shall use the Address Verification Service (AVS) as part of the authorization process to validate cardholders.

The Agency shall use a tamper resistant hardware encryption device to generate and store all Web server private and secret SSL cryptographic keys used to secure Cards Received over the Internet.

The Agency shall obtain the Web server SSL digital certificate used to secure Cards Received over the Internet from its acquiring bank.

The Agency shall not store any card numbers on a Web server or otherwise maintain a database of credit card numbers on a machine accessible from the Internet.

In addition to the Web server, the Agency must maintain a protected server (or a protected back end system) which is not accessible from the Internet for the purpose of temporarily storing credit card numbers pending authorization, communicating with the acquiring bank, and performing other sensitive financial functions off the Internet. The protected server must be secured from the Internet by appropriate firewall and networking configurations or by air gap.

### **9.3 Obtaining Authorizations over the Internet**

The Agency may obtain authorizations over the Internet using the World Wide Web for card numbers submitted to the Agency by mail, phone, fax, or over-the-counter ("Authorizations Over the Internet"). Authorizations Over the Internet for cards received in person or over-the-counter are "card present" transactions.

### **9.4 Implementation Requirements for Obtaining Authorizations over the Internet**

The Agency shall use the Secure Sockets Layer (SSL) Version 3 protocol to secure Authorizations Over the Internet. The Agency shall not transmit a card number for authorization if an SSL Version 3 security session can not be established with the server(s) processing the transaction.

FMS may require the Agency to use client SSL certificates at all agency PCs or workstations where card numbers are keyed or otherwise entered to obtain Authorizations Over the Internet. FMS may require the agency to use smart cards to store the client SSL private keys.

The Agency shall obtain any client SSL certificates used to secure Authorizations Over the Internet from FMS.

FMS may require the Agency to use a tamper resistant hardware encryption device to generate and store all private and secret SSL cryptographic keys on any servers used to process Authorizations Over the Internet.

The Agency shall not store any card numbers on a Web server or otherwise maintain a database of card numbers on a machine accessible from the Internet or accessible to unauthorized Agency LAN users. The Agency shall ensure that all LAN PCs or LAN workstations where card numbers are keyed or otherwise entered are secured from the Internet by appropriate firewall and networking configurations.

### **9.5 FMS Transaction Processing Server**

The FMS Transaction Processing Server acts as an Internet gateway to the Financial Institution's authorization center, secures and receives the transmission of card data over the Internet, and obtains transaction authorizations on behalf of the Agency. If the Agency elects to use the FMS Transaction Processing Server to assist in processing card transactions over the Internet, FMS will implement the security requirements on behalf of the agency in accordance with the requirements of the APA, including the implementation requirements set forth in Sections 9.2 and 9.4 above. However, the agency and not FMS will be responsible for maintaining a backup of data relating to transactions facilitated through the FMS server.

If the agency uses the FMS Transaction Processing Server over the internet only for the purpose of authorizing credit card orders received off-line, then Sections 9.1 and 9.2 do not apply.

The FMS Transaction Processing Server does not host the Agency's merchant Web site. The Agency is responsible for hosting and maintaining a merchant Web server with on-line catalogs, forms, Internet "shopping carts," order accounting, and other necessary Internet commerce services. The Agency is responsible for the security and content of its merchant Web server, and agrees to provide FMS with all necessary information to link its merchant Web server to the FMS Transaction Processing Server.

Neither FMS nor the Financial Institution shall be responsible or liable for any transaction if the Agency fails to transmit to the Transaction processing server the information necessary to compute the transaction.

**Signatures**

By affixing their signatures, the parties certify that they are authorized to amend the APA and bind their respective organizations to the provisions of this Amendment.

\_\_\_\_\_ (Agency Official's Signature)  
Date (Official's Name)  
(Official's Title)  
(Agency Name)  
(Official's Phone Number)

\_\_\_\_\_ (Bank Official's Signature)  
Date (Official's Name)  
(Official's Title)  
(Bank Name)  
(Official's Phone Number)

\_\_\_\_\_ (FMS Official's Signature)  
Date Kristine Conrath (Official's Name)  
Director, Emerging Technology Division (Official's Title)  
Financial Management Service (FMS Name)  
202-874-7019 (Official's Phone Number)