UNITED STATES
POSTAL SERVICE

December 3, 2004

Mr. Chris Hoofnagle
Associate Director
Electronic Privacy Information Center
1718 Connecticut Ave NW, Suite 200
Washington, DC 20009

Dear Mr. Hoofnagle:

We have completed processing your August 2 Freedom of Information Act (FOIA) request for records regarding requirements and data management policies concerning personal data collected by Automated Postal Center (APC) kiosks. Specifically, you requested records relating to cameras and credit card/bank information.

Enclosed are copies of all responsive records found to be releasable in full or in part (15 pages). Redactions have been made on some of the pages and 159 pages have been withheld in their entirety. The exemptions applied are FOIA Exemption 2, which relates to records related solely to internal personnel rules and practices that would enable circumvention of laws or regulations; FOIA Exemption 6, which applies to personal information, including medical and personnel files, the disclosure of which would be a clearly unwarranted invasion of personal privacy; and Exemption 3 which applies to information that is exempt from disclosure under another federal statute. The statute relied upon is 39 U.S.C. 410(c)(2), which pertains to information of a commercial nature, including trade secrets, whether or not obtained from a person outside the Postal Service, which under good business practice would not be publicly disclosed.

The types of information withheld pursuant to FOIA Exemptions 2 and 3 include application screen flows. These are the majority of pages withheld (141 pages). The release of this type of information would compromise the integrity and security of the APC kiosks. Other material withheld pursuant to these Exemptions include the data architecture of the system; specific security requirements, controls and processes; determinations of information sensitivity and criticality; and mapping of system activity log activities to the database.

Withheld pursuant to FOIA Exemption 6 are the identities of employees located on the Business Impact Assessment. That exemption does not require an agency to disclose information when such disclosure would result in an unwarranted invasion of an individual's privacy.

You may appeal this partial denial by writing to the General Counsel, U.S. Postal Service, Washington, DC 20260-1100, within 30 days of the date of this letter. The letter of appeal should include statements concerning this denial, the reasons why it is believed to be erroneous, and the relief sought, along with copies of your original request, this letter of denial, and any other related correspondence.

Sincerely,

Jane G. Eyre

Jane G. Eyre
Manager, Records Office

Enclosures

UNITED STATES POSTAL SERVICE™

Business Impact Assessment (BIA) Questionnaire

APPLICATION NAME: Automated Postal Center (APC) Self Service Platform
Corrected version 06/16/04

EIR NUMBER: 1363.00

SENSITIVITY: [redacted] b2 + b3

CRITICALITY: [redacted] b2 + b3

DATE: 12/01/03

TABLE OF CONTENTS

Version 3.14

July 15, 2003

b6
FOR
ALL ON
THIS PAGE

1 PROJECT IDENTIFICATION

IDENTIFICATION INFORMATION			
APPLICATION NAME:	Automated Postal Center (APC) Self Service Platform		
ISA NUMBER:	DR2002134082123	EIR NUMBER:	1363.00
CONTACT INFORMATION FOR SOLE OR DEVELOPING ORGANIZATION			
Functional Vice President:	[redacted]	**Other:**	[redacted]
Telephone Number:	[redacted]	Telephone Number:	[redacted]
Email Address:	[redacted]	Email Address:	[redacted]
Executive Sponsor:	[redacted]	**Executive Sponsor Designee:**	
Telephone Number:	[redacted]	Telephone Number:	
Email Address:	[redacted]	Email Address:	
Portfolio Manager:	[redacted]	**Portfolio Manager Designee:**	[redacted]
Telephone Number:	[redacted]	Telephone Number:	[redacted]
Email Address:	[redacted]	Email Address:	[redacted]
Program Manager:	[redacted]	**Project Manager:**	[redacted]
Telephone Number:	[redacted]	Telephone Number:	[redacted]
Email Address:	[redacted]	Email Address:	[redacted]
ISSO:	[redacted]	**ISSR:**	[redacted]
Telephone Number:	[redacted]	Telephone Number:	[redacted]
Email Address:	[redacted]	Email Address:	[redacted]
CONTACT INFORMATION FOR RECEIVING ORGANIZATION (if applicable)			
Vice President:		**Other:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
Executive Sponsor:		**Executive Sponsor Designee:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
DEVELOPMENT AND PRODUCTION INFORMATION			
Development Organization:	IBM		
Development Site:	Houston, TX		
Production Site(s):	Eagan, COSC		

2 PRIVACY COMPLIANCE

The purpose of this section of the questionnaire is to ensure compliance with privacy requirements, including applicable laws and USPS policy. Questions or comments regarding this section should be referred to the USPS Chief Privacy Officer (CPO). In general, privacy compliance covers two categories: 1) collection or maintenance of information relating to employees or customers, and 2) externally-facing websites. Customers covered by this section are external, non-vendor customers.

2-1 The Privacy Act of 1974

The Privacy Act of 1974 places restrictions on the collection, use, and dissemination of information relating to customers or employees that is maintained by an agency, including the USPS. The USPS must create and maintain a system of records for programs or systems where information is retrieved by customer or employee name or other identifier.

1.	**Does the program or system collect or store personal data related to a customer or employee where data is retrieved by name, unique number, symbol, or other identifier assigned to the customer or employee? [Refer to Section 4-1.1 for examples of personal data.]**	
□	No (If "No," skip to 2.2.)	
☒	Yes (If "Yes," a Privacy Act system of records is required. Answer 1a – 1h.)	
	a)	**Is this a new system of records?** (See ASM[1] and Privacy Office for assistance if a new system is needed or to modify an existing system.)
	□	No
	☒	Yes (If "Yes," contact Privacy Office)
	b)	**Name the System of Records you will be using:** (If you need further information, see Privacy Office.)
		Operations Data Collection system - Workload/Productivity Management Records, USPS 170.010
	c)	**When is the new or modified program or system expected to be operational? (mm/dd/yyyy)**
		01/31/04
	d)	**How long does the system indicate documents will be retained? (Explain process by which documents will be purged at the end of that time period.)**
	e)	**If a customer or employee is asked to supply information, a Privacy Act notice is required** (distinct from privacy policy on usps.com). **The notice must provide the following:** (All boxes must be checked or contact Privacy Office for assistance.)
	□	The principal purpose(s) for which the information will be used.
	□	The authority which authorizes the collection of the information.
	□	Whether providing the information is voluntary, and the effects, if any, of not providing it.
	□	The routine uses (disclosures) which may be made of the information.
	f)	**The Privacy Act Notice must be available at the time information is collected.** (One or more boxes must be checked or contact Privacy Office.)
	□	For Web sites, notice is provided in text where the information is collected, or can be accessed via link.
	□	For forms or other documents where data is collected, notice is on the document or form, and can be retained by the customer or employee.

[1] Please see Administrative Support Manual, Appendix: Privacy Act Systems of Records found at http://blue.usps.gov/cpim/manuals/

	g)	**Check all boxes that indicate how customers or employees may access data the USPS maintains on them, and how they may request a correction or amendment.** (One or more boxes must be checked.)
	□	With a link that leads to accessing information on the Web site.
	□	By providing specific written instructions on how to gain access to and correct their information.
	□	By providing a phone number of a USPS representative who will provide instructions.
	☒	Other: To request access to data, employee would contact System Manager of SOR 170.010.
	h)	**Steps must be taken to ensure the following:** (Please check all the boxes below where steps have been or will be taken to ensure the following.)
	□	Information is processed and maintained only for the purposes for which it was collected.
	□	Information is reliable for its intended use.
	□	Information is accurate.
	□	Information is complete.
	□	Information is current.
		Please explain steps taken to ensure the above requirements are fulfilled.

2-2 Gramm-Leach-Bliley Act

The USPS voluntarily complies with the Gramm-Leach-Bliley Act (GLB), Title V, which governs the treatment of personal information when certain financial services are provided. The GLB contains certain additional notice and choice requirements. Examples of financial services include banking activities or functions; wire or monetary transfers; printing, selling, or cashing checks; or providing USPS credit services. It does not include accepting payment by check or credit card issued by another entity.

2.	**Does your program provide a financial service?**
☒	No
□	Yes (If "Yes," contact Privacy Office.)

2-3 Children's Online Privacy Protection Act

The USPS voluntarily complies with the Children's Online Privacy Protection Act (COPPA), which requires notices and parental consent for certain practices if a website collects information from children under the age of 13.

3.	**If your program is online, do you know, or have reason to expect, that you are collecting personal information from children under the age of 13?**	
☒	No	
□	Yes (If "Yes," answer 3a.)	
	a)	
	□	**Check that you have read and comply with the USPS privacy policy on usps.com related to collection of information from children, or contact Privacy Office.**

2-4 Other Compliance

General	
4.	Are contractors or business partners employed regarding your system?
□	No (If "No," skip to 5.)
☒	Yes (If "Yes," answer 4a- 4b.)
	a) Do contractors/partners have access to customer or employee information?
	□ No
	☒ Yes
	b) Do contractors/partners help design, build, or operate an externally-facing web site?
	☒ No
	□ Yes
	If "Yes" is checked in 4a or 4b above, list all prime contractors and partners, and contact Privacy Office to coordinate Law Department inclusion of appropriate privacy and confidentiality clauses in contract. IBM
5.	If you would like to use customer information for another purpose than why it was collected (e.g., market another USPS product), customers must have been given a choice regarding that use. Please check the box that applies.
☒	Will not use customer information for another purpose.
□	Yes, with the choice to Opt-in for other uses (customers must perform some action to show permission).
□	Other: ______________________________ (Approval of the CPO is required.)
6.	Is the system using technologies, different from usps.com (see Question 11), that have the capability to identify, locate, and monitor individuals?
□	No
☒	If "Yes," specify: (Contact Privacy Office.) Camera required by FAA. Privacy Office is requiring a notice for customers, advising that photograph may be taken during the transaction.

Online Applications (If not an online application go directly to Section 3)

7.	Does your application operate on usps.com?
☒	No (If "No," please state where your application resides.)
□	Yes
8.	Does your application require customers to register?
☒	No (If "No," skip to 11.)
□	Yes
9.	Does your application use the usps.com registration process?
☒	No (If "No," what registration process will your system use?)
□	Yes (If "Yes," skip to 11.)
10.	Will the registration process you use capture customer preference (as described in Question 5) on how the information is used?
☒	No, the system will not be using the data collected for another purpose.
□	No, other means will be used. (Approval of the CPO is required.)
□	Yes
11.	Are any additional web analysis tools[2] to be used beyond those used by usps.com? See usps.com privacy policy for authorized web analysis tools. For example, persistent cookies, web beacons, and other tools (except for session cookies) must be specifically authorized by the policy and CPO.
☒	No
□	Yes (If "Yes," approval of the CPO is required.)
12.	Will the website include links to external sites of any sort?
☒	No
□	Yes (If "Yes," check and comply with the box below or contact Privacy Office.) □ Links comply with the affiliate program's standards[3] and usps.com privacy policy relating to banners and links.
13.	Will the website include ad banners of any sort?
☒	No
□	Yes (If "Yes," check and comply with the box below or contact Privacy Office.) □ Banners comply with the usps.com standards[4] and privacy policy relating to banners and links.

[2] A web analysis tool is a file or code that is placed on a user's browser or hard disk, or a tool that is placed on a web page from another server, to provide information about what sites or site pages are visited. Examples include cookies and web beacons.

[3] See Management Instruction AS-610-2001-1.

[4] See Management Instruction AS-540-98-2, Dissemination of Postal Information, Products, and Services via the World Wide Web.

3 GENERAL DATA ATTRIBUTES

This section will be used later in the Information Security Assurance (ISA) process to assess the adequacy of security controls that are implemented to protect the application.

3-1 Data Types

What type of data is being collected, or who does the data apply to? Please check all that apply.

☒	Customer (external, non-vendor customer as defined by Section 2, *Privacy Compliance*)
☒	USPS Employee
□	USPS Employment Applicant
☒	Contractor, Vendor, or Business Partner
□	Other:

3-2 Data Sources

Please check all the data sources that apply.

DATA SOURCES	
☒	Customer (external, non-vendor customer)
☒	USPS Employee
□	USPS Employment Applicant
☒	Contractor, Vendor, or Business Partner
□	Other USPS Data Source or Business Entity
□	Other Government Data Source
□	Consumer Reporting Agency
□	Law Enforcement Agency
□	Other:

3-3 Data Access

Please check all the individuals and organizations that will have access.

DATA ACCESS	
□	Customer (external, non-vendor customer)
☒	USPS Employees
☒	USPS Managers
☒	Contractor, Vendor, or Business Partner
□	Other:

211.3 Access to Records

211.31 Records and Documents

The OIG and Postal Inspection Service are authorized access to all records and documents of possible relevance to an official audit, evaluation, fact-finding, inspection, investigation, review or other inquiry whether they are in the custody of the Postal Service or otherwise available to the Postal Service by law, contract, or regulation. This includes information about mail sent or received by a particular customer. Exceptions to authorized access are listed in 211.33.

211.32 Disclosure

Information obtained under 211.31 may be disclosed to other postal employees who have a need for such information in the performance of their duties or to any federal, state, or local government agency or unit thereof that needs such information for civil, administrative, or criminal law enforcement. Any such disclosure must be consistent with Postal Service privacy regulations (see Handbook AS-353, *Guide to Privacy and the Freedom of Information Act*).

211.33 Exceptions

There are no exceptions when an inquiry, such as an investigation, inspection, evaluation, fact-finding, review, or audit is conducted under the authority of the Inspector General Act. Exceptions to the policy of disclosure are the following:

a. For information from the covers of mail, see 213. For dead mail, see the *Domestic Mail Manual.*

b. For access to employee restricted medical records and Employee Assistance Program records, see Handbook EL-806, *Health and Medical Service,* Chapter 2, and *Employee and Labor Relations Manual* (ELM) 870.

c. For access to an employee's Form 2417, *Confidential Statement of Employment and Financial Interests,* see the ELM or 39 CFR 447.42(e)(2).

212 Circulars and Rewards

212.1 Wanted Circulars

The Postal Inspection Service and the OIG issues wanted circulars to help locate and arrest fugitive postal offenders. Post these circulars in the most conspicuous place in the post office lobby and in other prominent places. Post near Poster 296, *Notice of Reward.* Telephone immediately the postal inspector in charge or inspector general with any information on the possible location of the person wanted. Remove and destroy circulars immediately when notified of their cancellation or when the circular is not listed in the periodic *Postal Bulletin* notices of current wanted circulars.

DATA ARCHITECTURE

Figure 5 APC Data Architecture depicts the data retained by the components of the APC Solution. The SSP Operational Database and Kiosk Management System provide the long-term data storage for the solution.

Withheld: b2
b3

Figure 5 APC Data Architecture

PERSISTENCE STRATEGY

APC

The APC retains transaction data, application logs, user photographs, and alerts for a relatively short time. [redacted] Photos are retained for a configurable period of time. The remainder of the operational data is archived after closeout and retained for possible retransmission or recovery for a configurable period of time. b2

[redacted] b3

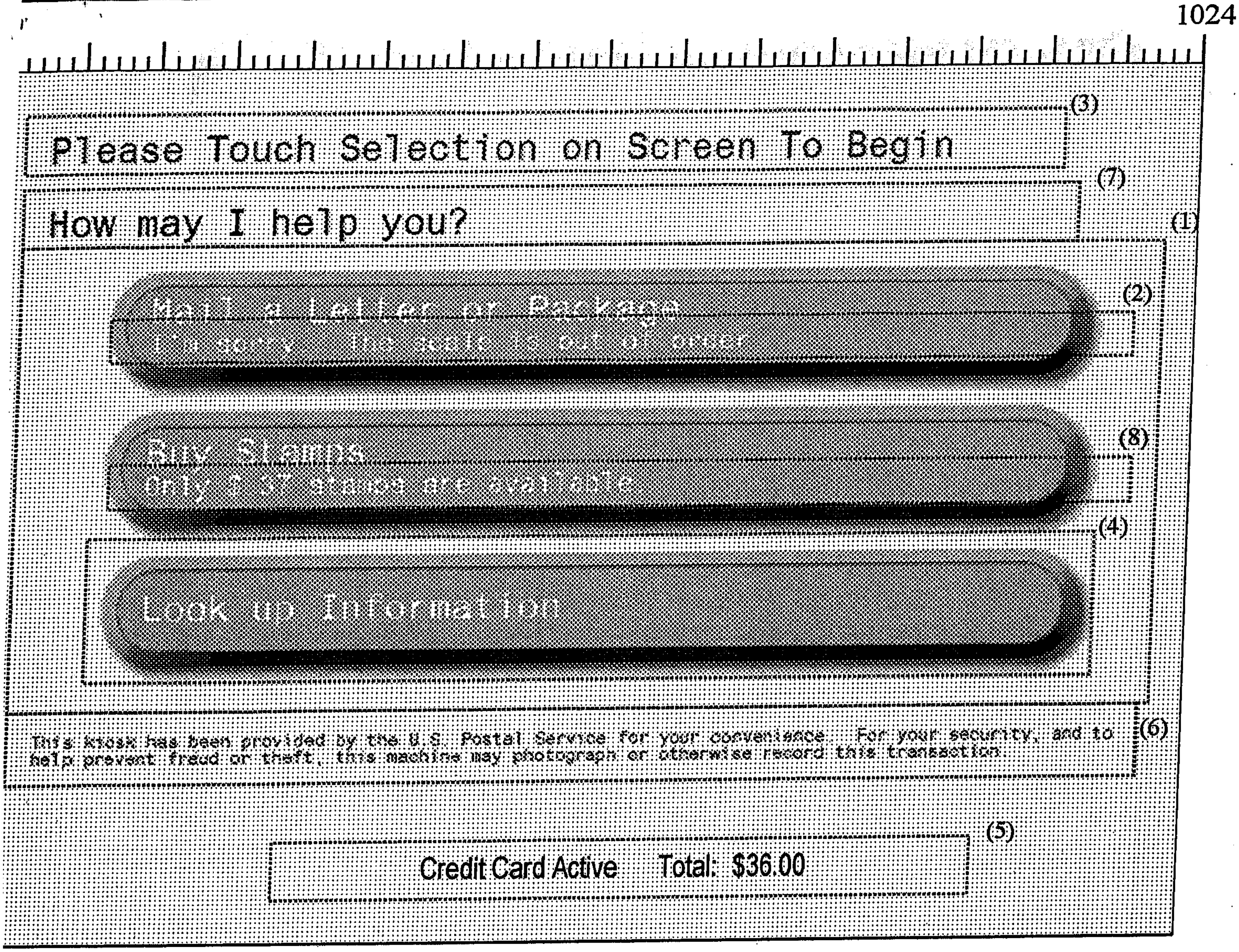
These three types of data are stored on the internal hard drive of the kiosk and also on the external hard drive to protect the data from loss. [redacted] b2 + b3

Retained Data (Numbers correspond to items in Figure 5)	Description	Storage Type	Period of Retention	Sensitivity/Criticality
	NOT WITHIN SCOPE OF REQUEST			
2. Application Logs and Alerts	APC Application transaction data, inventory and closeout data, alerts	Windows XP File System	24 hours	[redacted]
	Photographs of Customers and Servicers	Windows XP File System	30 days	
NOT WITHIN SCOPE OF REQUEST				

b2 + b3

Table 2 APC Retained Data

NOT WITHIN SCOPE OF REQUEST



Please Touch Selection on Screen To Begin

How may I help you?

Mail a Letter or Package
I'm sorry. The scale is out of order

Buy Stamps
Only $.37 stamps are available

Look up Information

This kiosk has been provided by the U.S. Postal Service for your convenience. For your security, and to help prevent fraud or theft, this machine may photograph or otherwise record this transaction.

Credit Card Active Total: $36.00

3.2.8	**Photograph the User**
FR3.2.8.1	In order to augment security, a digital photo of the customer will be necessary for some transactions. A camera built in to the basic kiosk shall be capable of generating a portrait style identification photograph of users while they are in front of the user interface screen.
FR3.2.8.2	[redacted]
FR3.2.8.2-1	[redacted]
FR3.2.8.2-2	[redacted]
FR3.2.8.2-3	[redacted]
FR3.2.8.2-4	[redacted]
FR3.2.8.2-5	REQUIREMENT DELETED
FR3.2.8.2-6	[redacted]
FR3.2.8.2-7	[redacted]
FR3.2.8.2-8	A picture shall be taken of individuals who interface with the SSP to access the machine for either service or maintenance purposes.
FR3.2.8.2-9	[redacted]
FR3.2.8.2-10	[redacted]
FR3.2.8.3	The photograph storage parameter shall be defaulted to 30 days.
FR3.2.8.3-1	The photograph storage parameter shall be data configurable via data update.
FR3.2.8.4	[redacted]
FR3.2.8.5	[redacted]

b2 +
b3

FR3.2.8.6	No revenue transactions shall be permitted to complete in the event the analysis of the photograph determines the photograph to be compromised [redacted]
FR3.2.8.7	The SSP shall display a Privacy Notification to the customer prior to the customer beginning a transaction.
FR3.2.8.8	The content of Privacy Notification shall be data configurable via a data update.
FR4.5.3	The contractor shall provide the capability for the retrieval of the stored photographs for a specific date range.
FR4.5.4	[redacted]

b2 + b3

and for debit/credit:

FR3.2.5.2.7	The debit card receipt shall include the last four digits of the account number.
FR3.2.5.1.9	The credit card receipt shall include the last four digits of the account number.
FR3.2.5.3.6	The EBT card receipt shall include the last four digits of the account number.
FR5.7.25-1	[redacted]
FR5.7.25-2	[redacted]

b2 + b3

b2 + b3
FOR ALL ON THIS PAGE

Transactions:

1.1.1.1.1 Sheetlet Sale

1. Customer selects Buy Stamps
2. Customer selects 37¢ First Class
3. Customer selects 1 Booklet $6.66
4. Customer selects Credit
5. Customer dips Visa card
   a. [redacted]

1.1.1.1.1 Postage Sale in Buy Stamps

1. Customer selects Buy Stamps
2. Customer selects 23¢ Postcard
3. Customer selects 2 for $.46
4. Customer selects Debit/EBT
5. Customer dips Debit card
6. Customer enters PIN
   a. [redacted]

1.1.1.1.1 Postage Sale in Mailing

1. Customer selects Mailing
2. Customer select Letter
3. Customer weighs 2 oz letter
4. Customer enters destination zip code
5. Customer selects $.83 First Class service
6. Customer selects buy the stamp
7. Customer selects Debit/EBT
8. Customer dips EBT card
9. Customer enters PIN
   a. [redacted]

b2 & b3
FOR ALL ON
THIS PAGE

1.1.1.1.1 E-Label Sale in Mailing

1. Customer selects Mailing
2. Customer select Large Envelope
3. Customer weighs 4 oz letter
4. Customer enters destination zip code
5. Customer selects $1.06 First Class service
6. Customer selects buy the stamp
7. Customer selects Credit
8. Customer dips MasterCard
    a. [redacted]

1.1.1.1.1 Shopping Basket Transaction

1. Customer selects Mailing
2. Customer select Large Envelope
3. Customer weighs 4 oz letter
4. Customer enters destination zip code
5. Customer selects $1.06 First Class service
6. Customer selects buy the stamp
7. Customer selects Credit
8. Customer dips American Express card
    a. [redacted]

1. Customer selects Yes when asked if he/she wants to make another purchase
2. 1 $1.06 E-Label is dispensed
3. Customer takes the label
4. Customer is asked to take the label and selects the Continue button to continue purchasing
5. Customer selects Buy Stamps
6. Customer selects 37¢ First Class
7. Customer selects 1 Booklet $6.66
8. Screen is shown saying "Just a moment please" while the additional tender amount is authorized
    a. [redacted]

Retail DAta Mart files keep only the last four digits of the credit/debit/EBT card number . Attached is the SAL Mapping file which has the layouts and shows this.

-----Original Message-----