EagleCash™ & EZpay™

Program Guidance - Standard Operating Procedures

Stored Value Card (SVC) Program
Federal Reserve Bank of Kansas City

Last Revised: 6 October 2022

Table of Contents

Table of Contents

Section 1 – Program Overview

EagleCash and EZpay Standard Operating Procedure (SOP) Purpose and Objective

This SOP provides an overview of the EZpay and EagleCash programs. It also outlines roles and responsibilities for military personnel and retail associates involved in the day-to-day administration. Where necessary, specific procedures are provided to help administrators and stakeholders with information to perform daily operations.

The EZpay and EagleCash Stored Value Card software application is fully accredited in accordance with the provisions of Fiscal Service Information Security Program Plan (ISPP) on Security Assessment & Authorization (SA&A), including being given an Authorization to Operate (ATO). Further, these Stored Value Card programs have been approved for use within the United States Army, Air Force, Marines, and Navy, through reciprocity agreements between Fiscal Service and each service component.

This SOP is updated on an as-needed basis. This SOP is comprised of sections, ensuring that published guidance is available upon changes to the procedures or policy shortly after changes are made. Detailed device operations instructions are found in separate user guides and quick reference guides located on the SVC Portal.

A. EagleCash / EZpay Program Overview

Processing, administrative, and operational support for Stored Value Card programs are provided by the Federal Reserve Bank of Kansas City (FRBKC). EagleCash and EZpay support the objectives of the U. S. Government to reduce dependency on currency/cash – at military training installations, Finance/Disbursing Offices, and at sea in contingency and for peacekeeping operations/missions worldwide; thereby improving operations and reducing costs.

As a payment system, EagleCash and EZpay support the needs of personnel during basic military training and while serving OCONUS by delivering a full-function cash replacement program that can be used for the purchase of goods and services at merchant and Post Office locations on base. EagleCash and EZpay are interoperable at all locations where the infrastructure for the EagleCash and EZpay programs have been implemented.

1. The EagleCash System

The EagleCash SVC program is a cash management tool used to support a cashless battlefield and to provide enhanced financial services to cardholders. The program was developed by the Bureau of Fiscal Service and designed to support U.S. military and civilian personnel deployed in combat zones, non-combat zones, and peace-keeping missions around the globe. Program components include the EagleCash card, kiosk and mobile kiosk, laptop, and POS device.

Deployed personnel are issued and use EagleCash cards rather than cash to make purchases at the Post Exchange/Base Exchange (PX/BX), U.S. Army & Air Force Exchange Service (AAFES) concessions, Navy Exchange (NEX) stores, Dining Facilities, certain Commissaries, and military Post Office (PO) facilities. Rather than going to the camp/installation Finance Office (FO)/Disbursing Office (DO) to cash a check or obtain a payroll advance, cardholders access funds in their U.S. accounts via self-service devices (kiosks) at convenient locations on the base.

2. EagleCash Cards

The EagleCash card is a plastic, re-loadable stored value card (SVC) embedded with a computer chip that stores "electronic money" in its memory. The card does not use a magnetic stripe, as do credit or debit cards. Because the specialized computer chip is capable of changing/storing data in its memory, the EagleCash card is often referred to as a "smart card." The card is used to reduce U.S. coin and currency transactions at the Finance/Disbursing Offices, Post Offices, PX/BX, various on-base service providers, such as barber and beauty shops, fast food concessions, and at other merchants who provide goods and services.

Using specially configured Point of Sale (POS) terminals capable of reading a smart card, the cardholder can transfer a specified amount of electronic money from the card to the merchant in payment for goods and services. During the transfer, the purchase amount is deducted from the chip balance on the card and transferred to the merchant terminal, which houses a similar electronic chip capable of receiving the transferred value. In addition to purchase features and balance features, the card provides other functionality, including the ability to load and unload or transfer value throughout the tour of duty at any location where the EagleCash program is implemented. The card is issued at the Finance/Disbursing Office and may be funded at self-service kiosks located at convenient locations on the base, or at the Finance/Disbursing Office via payroll advance (partial pay), cash, or by writing a check.

In addition to issuance, load, and balancing functions performed by the Finance/Disbursing Office, the EagleCash program includes kiosk support with software and functionality specifically designed for SVC management. EagleCash kiosks are freestanding devices like Automated Teller Machines (ATMs) that support cardholder-initiated value transfers from and to checking and savings accounts, card-to-card value transfers, balance inquiries, PIN changes, and activity reporting that includes the ten most recent transactions.

Program activity data and updates are transferred daily from all EagleCash hardware (laptop Personal Computers (PCs), POS terminals, and kiosks) to the program's processing agent, FRBKC.

3. The EZpay System

The EZpay SVC program is a cash management tool used to support a cashless training environment for cardholders. The program was developed by the Bureau of Fiscal Service and designed to support U.S. military and civilian personnel deployed at military training locations. Program components

include the EZpay card, laptop, POS devices, and EZpay card printers.

Military recruits/trainees are issued and use payroll advance-loaded EZpay cards rather than cash to make purchases at the Post Exchange/Base Exchange (PX/BX), U.S. Army & Air Force Exchange Service (AAFES) concessions, Navy Exchange (NEX) stores, Dining Facilities, certain Commissaries, and military Post Office (PO) facilities. Rather than going to the camp/installation Finance Office (FO)/Disbursing Office (DO) to cash a check or obtain a payroll advance, cardholders access funds at convenient locations on the base.

4. EZpay Cards

The EZpay card is a plastic, prepaid Stored Value Card (SVC) embedded with a computer chip that stores "electronic money" in its memory. Because the specialized computer chip is capable of changing/storing data in its memory, the EZpay card is often referred to as a "smart card." The card is used to reduce U.S. coin and currency transactions at the Finance/Disbursing Offices, Post Offices, PX/BX, various on-base service providers, such as barber and beauty shops, fast food concessions, and at other merchants who provide goods and services.

Using specially configured POS terminals capable of reading a smart card, the cardholder can transfer a specified amount of electronic money from the card to the merchant in payment for goods and services. During the transfer, the purchase amount is deducted from the chip balance on the card and transferred to the merchant terminal, which houses a similar electronic chip capable of receiving the transferred value. The card is funded at the Finance/Disbursing Office via payroll advance.

Program activity data and updates are transferred daily from all EZpay hardware (laptop Personal Computers (PCs) and POS terminals) to the program's processing agent, FRBKC.

B. Stored Value Card (SVC) EagleCash & EZpay Program Support Elements

- **Department of Treasury Bureau of Fiscal Service**

Nadir Isfahani Manager, Stored Value Cards Portfolio U.S. Treasury Department, Fiscal Service *Email:* nadir.isfahani@fiscal.treasury.gov	**Jonathan Homeyer** EagleCash Program Manager U.S. Treasury Department, Fiscal Service *Email:* jonathan.homeyer@fiscal.treasury.gov
Timothy Nixon EagleCash Sustainment Manager U.S. Treasury Department, Fiscal Service *Email:* timothy.nixon@fiscal.treasury.gov	**Tyrone Lynn** Information Security U.S. Treasury Department, Fiscal Service *Email:* tyrone.lynn@fiscal.treasury.gov

- **Federal Reserve Bank of Kansas City**

Ernest "Ernie" Craig Vice President | Stored Value Card *Email:* ernest.craig@kc.frb.org	**Todd Rich** Asst Vice President | Stored Value Card Operations Officer *Email:* todd.rich@kc.frb.org
Julie Nielsen SVC PMO Manager *Email:* julie.nielsen@kc.frb.org	**Christopher Hotchkiss** SVC Product Director *Email:* christopher.hotchkiss@kc.frb.org
Nate Arnold SVC Technology Operations Manager & ISSO *Email:* nate.arnold@kc.frb.org	**Cindee Barnard** SVC Technology Operations Asst Manager *Email:* cindee.barnard@kc.frb.org
John Lund SVC Customer Service Manager *Email:* john.lund@kc.frb.org	**Danielle Reynoldson** Sr. Supervisor | SVC Financial Operations *Email:* danielle.reynoldson@kc.frb.org
Michael McDonald SVC Customer Service Senior Supervisor *Email:* michael.mcdonald@kc.frb.org	**Customer Service Center** Office: 1-877-973-8982 DSN: 312-955-3555 *Email*: eagle@frb.org ; ezpay@frb.org Hours of Operations Mon–Fri 0000 - 1800 CT

- **PNC Bank, National Association**

John Bendana Vice President Senior Product Manager Treasury Management | Federal Services *Email:* john.bendana@pnc.com	**Michael Bolin** Senior Vice President TMO/Relationship Manager Treasury Management | Federal Services *Email:* michael.bolin@pnc.com

- **US Military Service Program Management**

Air Force	**Army**
Michael Windsor Air Force Banking Manager SVC-EagleCash/EZpay Program Manager *Email:* michael.windsor.2@us.af.mil	**Tony Taylor | Chad Samsel** EagleCash Program Manager U.S. Army Financial Management Command *Email:* Charles.a.taylor40.civ@army.mil chad.f.samsel.civ@army.mil
Navy	**Marines**
Beth Pollock - Navy Cash/DDS PM *Email:* Beth.a.pollock.civ@us.navy.mil **Michael Harants**, Navy Cash Deputy PM *Email:* michael.j.harants.civ@us.navy.mil	**Scott A. Billman** Supervisor, Financial Management Stored Value Card (SVC) Program Manager *Email:* scott.billman@usmc.mil

C. Implementation Environments

All four branches of the U.S. military have EZpay locations stateside and EagleCash systems in operation around the globe.

1. CONUS

There are 9 EZpay installations (1 Navy, 2 Marine Corps, 2 Air Force, and 4 ARMY), and 40 EagleCash installations stateside at card issuance sites. Most stateside installations are at basic military training locations.

2. OCONUS

The Stored Value Card program has EagleCash acceptance sites at locations in more than 20 countries.

3. At Sea (LCS Ships)

EagleCash implementation is a smaller equipment footprint due to limited space aboard the Littoral Combat Ship (LCS) class of U.S. Navy. The list of equipment includes two laptops, four POS devices, and two mobile kiosks. This implementation allows for the transaction of meal purchases without the exchange of cash aboard ships.

D. Program Events and Activities

1. eCommerce Training

This training provides new Finance Officers (FOs), Deputy Disbursing Officer (DDO), Information Management Officers (IMOs), and Cashiers with the information and resources necessary to successfully operation an EagleCash system when deployed. There are three methods of eCommerce training depending upon scheduling availability and military service. The Federal Reserve Bank offers an on-site week-long training agenda. The Army offers pre-deployment training for new Finance Officers, and there are also a variety of online videos available on the portal.

2. EagleCash Wellness Calls/Visits

Wellness calls and visits are a joint effort among military Service Program management, Fiscal Service, and Federal Reserve Bank staff to ensure the systems installed at military installations and vendor/merchant locations are running smoothly and to follow-up on operations to ensure all sites have the necessary equipment and support needed. The goal is to accomplish these calls on a monthly basis as time/schedules allow.

Topics discussed with Finance Officers during recurring EagleCash wellness calls include:

- Card counts, missing FS Form 2887s, missing issuance and Transaction Report (TR) files
- Equipment issues (kiosk, laptop, POS)
- Vouchers, Incident Reports, Automated Clearing House (ACH) Kiosk Returns
- Hotlist and other topics as required

3. Monthly EZpay Call

This meeting is hosted virtually by Fiscal Service as a wellness call to check in with military stakeholders to find out how operations are running, relay information, and coordinate schedules for program updates and on-site visits. Military Program Managers, the Federal Reserve, and EZpay base Finance Officers are invited.

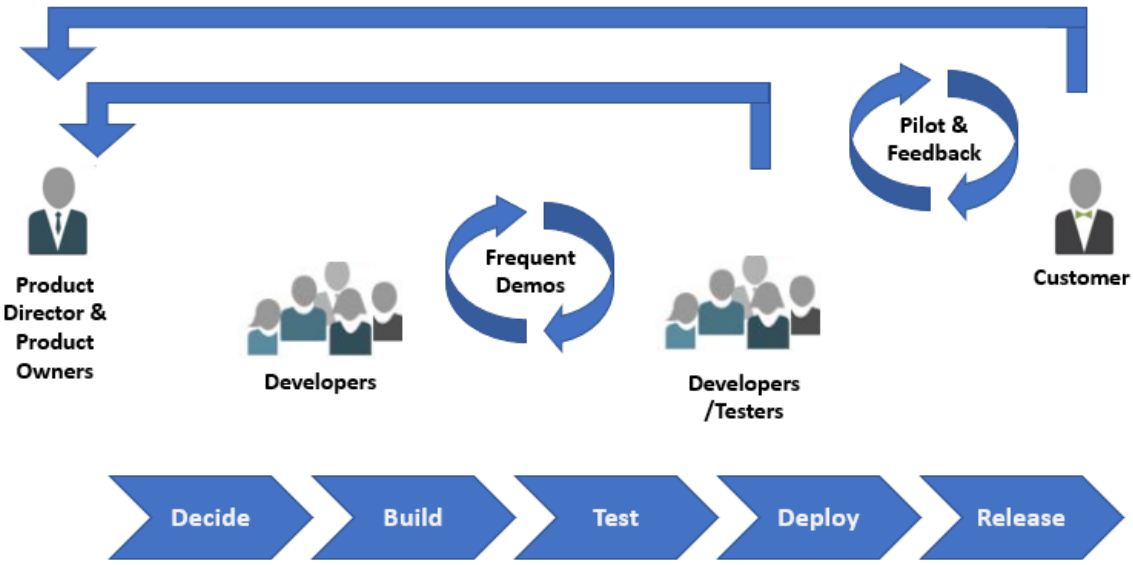
4. Change Control Board (CCB)

For general awareness, this is a quarterly meeting conducted in-person when possible and virtually otherwise. It is attended by military service Program Managers. The responsibilities of the CCB membership includes:

a. Approve the CCB's charter.
b. Solicit input from deployed users or CONUS support organizations.
c. Propose SVC software (SW)/hardware (HW) functionality based on business requirements and changing technology methods/implementations.
d. Review and evaluate all SW/HW change proposals.
e. Approve/reject proposed SW/HW changes.
f. Approve or recommends scope changes.
g. Prioritize approved changes.

Approved changes will proceed through the new work intake and prioritization activities internal to the Federal Reserve Bank's Scaled Agile Framework (SAFe) for software development. SAFe processes allow the developers to work through an actively groomed backlog of prioritized features.

E. Stored Value Card Program's Product Lifecycle



1. FRBKC Product Agile Development

The Federal Reserve Bank of Kansas City software development team is responsible for building, testing, and maintaining the Stored Value Card-unique software baseline developed for commercially available hardware products that work with the cards, and the merchants, and banking systems connected to them.

FRBKC has shifted to the Scaled Agile Framework to develop working software for our customers. Work created by feedback from customers about deployed devices/software is managed as a production support request for true break-fix issues. Enhancements and new features/capabilities requested are prioritized and added to an actively worked backlog.

Product Owners for the Stored Value Card line of products may reach out to you for input and clarification of any requests submitted. Requests for changes to existing device software/apps and processing are discussed during bi-weekly CCB Status Call meetings.

2. Card Processing Station (CPS) Software and Device Firmware Updates

There are three ways a CPS laptop can be updated. Technical support is available if needed by calling the Customer Service Center:

a. For unique environments, an equipment swap may be necessary.
b. A file may be placed on the SVC portal for download and install according to instructions made available.
c. For Navy account's LAN-connected devices, the local IT/Comms is responsible for any software updates/patches that may be automatically pushed to the devices.

3. New Equipment & Software Enhancement Pilots

Locations may be volunteered by their Military Service Program Manager to participate in new product pilots to ensure the products delivered yield the results/performance expected. During these pilots, SVC staff will host frequent stand-ups, hosted virtually to demo new features/fixes, and to gain valuable feedback from participants.

4. Production Releases and Deployments

FRBKC works closely with military service Program Managers, the Bureau of Fiscal Service, and the military customers to ensure that planning of software and equipment releases and deployment are coordinated and scheduled to ensure the smoothest possible implementation of new or changing SVC systems.

F. Program Stakeholder Roles and Responsibilities

U.S. TREASURY, FISCAL SERVICE
a. Represent U.S. Department of the Treasury. b. Fund back-office processes. c. Provide guidance for FRBKC administrative/customer service processes. d. Update operating policies and procedures. e. Present briefings to the major participants in the program. f. Oversee Memoranda of Understanding (MOU) with program participants. g. Authorize the development of enhancements. h. Prepare projected and actual budget reports. i. Maintain the funds pool. j. Provide monthly residual value reports. k. Provide funds settlement and clearing processes. l. Deployment assistance for USAFMCOM, SAF/FMP, Resources Fiscal Finance, Kansas City/Indianapolis (RFF-KCI), and NAVSUP. m. Demonstrate equipment and procedures to soldiers prior to deployment. n. Authorize hardware purchases. o. Maintain the EagleCash and EZpay web sites (https://fiscal.treasury.gov/eaglecash/ https://fiscal.treasury.gov/ezpay).

FEDERAL RESERVE BANK OF KANSAS CITY
a. Set high-level program policy and provides headquarters support. b. Coordinate project details and provide development updates with all agencies and commands. c. Coordinate funding of the program with the U.S. Department of the Treasury and military departments' budget offices. d. Assist the U.S. Department of the Treasury in the deployment of EagleCash and EZpay. e. Assist the Finance Units at contingency operation locations with EagleCash when required in Continental U.S. (CONUS) and OCONUS. Assist Finance Units stateside with EZpay. f. Coordinate pilots of system design and device changes; track success of all SW/HW releases and provide reports to stakeholders through User Acceptance Testing (UAT), Pilot, and Deployment stages. g. Provide recurring meeting and training facilitation. h. Manage files and forms, and maintain folders in the SVC Portal https://svcportal.fiscal.treasury.gov/

U.S. MILITARY SERVICE PROGRAM MANAGERS
a. Set high-level program policy and provides headquarters support. b. Coordinate project details with all agencies and commands c. Coordinate funding of the program with the U.S. Department of the Treasury and the AF Central Command. d. Assist the U.S. Department of the Treasury in the deployment of EagleCash. e. Assist the Finance Units at all locations with EagleCash and disbursing training. f. Coordinate funding of the Stored Value Card programs with the U.S. Department of the Treasury and the Army Budget Office. g. Oversee reciprocal acceptance of EagleCash and EZpay into the computing enclaves globally. h. Assist FRBKC with UAT and pilot efforts.

U.S. ARMY FINANCIAL MANAGEMENT COMMAND (USAFMCOM)
a. Act as ASA (FM&C) Field Representative. b. Fund hardware and deployment costs. c. Coordinate project details with all agencies and commands (e.g., U.S. Department of the Treasury, Defense Finance and Accounting Service [DFAS], AAFES, Finance Units, and Army Post Offices, etc.) as required on behalf of the ASA (FM&C). d. Assist the U.S. Department of the Treasury in the deployment of EagleCash and EZpay. e. Assist FRBKC with UAT and pilot efforts.

FIELD MILITARY SERVICE FINANCE/DISBURSING OFFICES
a. Support deployments. b. Create laptop administrator and CPS user accounts; manage accounts and access rights. c. Issue cards in accordance with the Card Issuance Policy. d. Accept cards in accordance with the EagleCash Card Acceptance Policy. e. Load and unload value. f. Maintain card stock. g. Transmit EagleCash files. h. Serve as POC for EagleCash kiosks on base. i. Submit Incident Reports. j. Ensure personnel changes are reported using FRBKC Form 417. k. Report all device issues/errors to FRBKC Customer Service Center. l. Assist FRBKC with UAT and pilot efforts.

Defense Finance and Accounting Service (DFAS)
a. Provide support related to disbursing policies and procedures. b. Assist FRBKC with UAT and pilot efforts.

Military Postal Service Agency (MPSA)
a. Set high-level postal program policy. b. Coordinate project details with Department of Defense (DoD) Post Offices. c. Assist U.S. Department of the Treasury and all Military Departments with deployment. d. Assist with pre-deployment shipping and transportation. e. Assist FRBKC with UAT and pilot efforts.

Merchants (AAFES, NEX, Military Post Offices)
a. Accept the EagleCash and EZpay cards at all (land-based) stores in accordance with the EagleCash and EZpay Acceptance Policy. b. Sponsor acceptance of EagleCash at all OCONUS concessions or merchants. c. Assist in EagleCash deployments. d. Create laptop administrator/CPS user accounts; manage accounts/access rights. e. Transmit EagleCash settlement files daily. f. Maintain current hotlist on POS terminals. g. Provide marketing strategy input and support. h. Provide policy to store managers on the use of EagleCash. i. Assist FRBKC with UAT and pilot efforts.

G. Operations

Day-to-day EagleCash and EZpay operations are conducted using EagleCash and EZpay systems and devices operated by trained Finance Office Staff and merchants who are supported by the Stored Value Card Customer Service Center. This SOP and device user guides (available in the SVC Portal) help Finance Officers and Merchants facilitate transactions and settle daily business. Authorized contacts have access to technical assistance with EagleCash and EZpay system maintenance, device support, and IT communications/processing issues when needed.

For additional information regarding EagleCash, EZpay or any of the topics covered in this SOP, contact your Agency Point of Contact (POC) or:

Stored Value Card - Customer Service Center (CSC)	
Hours of Operation:	Monday to Friday, 0100 – 1900 ET
Email:	eagle@frb.org; ezpay@frb.org
DSN OCONUS:	(312) 955-3555
U.S. Toll Free:	1-877-973-8982
Websites:	https://fiscal.treasury.gov/eaglecash https://fiscal.treasury.gov/ezpay https://svcportal.fiscal.treasury.gov/
Mailing Address:	Federal Reserve Bank of Kansas Cityc/o Stored Value Card 2201 Farnam Omaha, NE 68102

Section 2 – Finance/Disbursing Officer Procedures

A. EagleCash and EZpay Implementation/System Setup

1. Training & Documentation

FRBKC-provided training materials are available on the SVC Portal. This includes the SOP, user guides, quick reference guides, bulletins, and other policy documents and program bulletins.

2. Deployment, installation, and configuration of EagleCash and EZpay assets

a. A system implementation includes the following:

- All equipment, hardware, and support required to issue cards, process transactions, and transfer files for settlement.
- All required card stock branded, primed, and ready for issuance.
- Merchant POS terminals with smart card read capability and with custom developed software application tailored to the program's features and functionality.
- On-site training of all program participants involved in card issuance and acceptance. This on-site training includes the Finance/Disbursing Officers, Post Office, and AAFES employees. Training of AAFES concessions and other program users, such as Dining Facilities (DFAC) and MWR sites, is also provided.
- Ongoing operational and customer support from the Customer Service Center (CSC) under the direction of the program operations support manager, FRBKC.
- Documentation for all program elements, including terminal operation, kiosk operation *(for EagleCash only)*, card issuance, merchant acceptance, and day-to-day program management and troubleshooting.
- Marketing materials that educate participants, create awareness, and promote the program availability, benefits, and enrollment procedures.

b. The Card Processing Station (CPS Laptop): CPS is a software application installed on the laptop and is located in an EagleCash or EZpay folder on the Desktop. This application has an SVC Admin Tool that is for use by Administrators only with the duty title of DDO/DA/PA or COPE. This SVC Admin Tool allows administrators to create, update, and delete user accounts. Individual accounts are created with pre-defined roles for the different functions required to perform operations. Examples: Cashier, Exchange, Post Office, MWR, NAF, etc.

CPS provides the following capabilities for the DDO/DA:

- Card Enrollment and Issuance (FS Form 2887)
- Cashless Kiosk Program (ACH)
- Revalue
- Update EagleCash Card Info
- Generate reports
- Collection transactions from POS, kiosks, and MOKI devices
- Import hotlist/warmlist and DevNames (warmlist reason) files
- Deliver transactions to FRB

Be sure to consult the CPS User Guide for operating details for each of these listed capabilities. As of this publication, CPS laptops are not reimaged in the field, and EagleCash software cannot be installed in the field. Laptops are delivered pre-configured with all needed software installed.

c. Configuration Management: A configuration file contains the programming for a particular device and provides a unique ID for each device. FRB can email these files or upload them to the SVC Portal. Below are some key reasons for using configuration files:

- Reloading a lost configuration
- Updating information (merchant's name, facility)
- Relocating a device in the field (Merchant IDs are tied to Device IDs). If a device is moved without contacting FRB prior to relocating, the wrong merchant will receive the funds from sales made on that device.

NOTE: You must contact the FRB Customer Service Center and the Military Service Program Manager in order to approve the FS Form 410 prior to relocating a device!

3. EagleCash Point of Contact (POC) Software Change Requests

If you have ideas or recommendations for enhancements or improvements to device operations, procedural changes, or other feedback regarding how the EagleCash software works, please send them to your military Service Program Manager who can bring these to the appropriate forum for review, analysis, and possible inclusion into the backlog for prioritization and development.

4. SVC Rules of Behavior

- Users must ensure that the Information Technology (IT) resources with which they have been entrusted are used properly, as directed by Fiscal Service and Local IT policies and standards, taking care that the laws, regulations, and policies governing the use of such resources are followed and the value of all information assets are preserved. Each user is responsible for all activities associated with their assigned User ID.

- Users must take positive steps to protect SVC equipment, software, and data from loss, theft, damage, and unauthorized use or disclosure.

- Users must report improper or suspicious use of SVC equipment.

- Users must follow proper logon/logoff procedures.

- Users must not browse or search SVC data except in the performance of authorized duties. Ability to access data does not equate to authority to manipulate data.

- Users must not install or use unauthorized software on SVC equipment. Do not use freeware, shareware, or public domain software on SVC computers without permission from Treasury.

- Users must ensure that anyone seen using a SVC workstation in the area is authorized to do so. When leaving and active workstation unattended, users will log off or secure the workstation from unauthorized use.

- Users must protect user IDs and passwords from improper disclosure. Passwords provide access to Bureau of Fiscal Service (U.S. Treasury) data and resources. Users are responsible for any access made under his/her user ID and password.

- Users do not reveal passwords under any circumstances. Password disclosure is considered a security violation and is to be reported as such. If password is necessary for problem resolution, immediately select a new password once the problem has been resolved. Do not share password with anyone else or use another person's password.

B. IT Systems Accountability (Asset Management)

1. Replacement Hardware and Supplies (FRBKC Form 411)

There is a separate FRBKC Form 411 for EagleCash and EZpay. These forms are used for requesting supplies and replacement equipment. Completed forms must be emailed to eagle@frb.org or ezpay@frb.org and include the following text in the subject line of the email: "Hardware and Supply Requests – (Base name – Type of Vendor)"

2. New Hardware Requests (FRBKC Form 412)

For EagleCash, this form is used for requesting an increase (footprint expansion or new merchant) to your existing authorized equipment footprint. These requests are reviewed by the Service PM and the Treasury Department, Bureau of Fiscal Service before FRBKC is authorized to build, configure, and ship the requested items. New equipment requests must be emailed to eagle@frb.org and include the following text in the subject line of the email: "New Hardware Requests – (Base name – Type of Vendor)." There is no FRBKC Form 412 for the EZpay program.

Requests for devices must include:

- Requestor's Name
- Vendor/Merchant Name
- Mailing Address
- Base Name
- Business Justification

3. Return Tracking Notifications

Customers needing a replacement device will receive a notification via email that the request has been confirmed and receive a separate notification upon build completion that the device has been shipped, along with a shipping vendor's tracking number.

Once a device that is in use has been identified for return/replacement, a Customer Service Representative will provide a return shipping label for the defective/excess device to place on the box with the returned item. Ensure these defective/excess devices are returned promptly to FRBKC.

Devices being mailed back for replacement must be listed on the FRBKC Form 411 and include:

- Base Name
- Merchant Name
- Facility/Postal Number
- Device ID & Serial Number
- Description of the Problem
- Whether the Device has Transactions not Batched Out
- RTN Number provided by a Customer Service Representative

4. Inventory Tracking

Each organization will ensure proper custody and accountability of Department of Treasury, Stored Value Card program equipment. The below listed forms are used to transfer hardware and supplies between organizations:

- DA Form 2062 (Army & Marines only) – Hand Receipts
- Acknowledgement of Receipt of Equipment - Shipping Notice Email Reply
- Transfer of Hardware/Supplies (FRBKC Form 410)

5. Kiosk and POS destruction in place procedures

These procedures are only applicable during life cycle replacement activities. To save on costs, field destruction of some equipment is allowed; however, it is critical that all personnel follow the specific guidance published in bulletins available on the SVC Portal. There are programmed cards inside the device that contain data which must be retrieved and returned to FRBKC. Process details are not included in this SOP due to the temporary nature of the need for the action due to equipment end of life

or other circumstances.

6. CPS and Device Administration/Configuration

In most circumstances, devices are provided to customers pre-configured based upon information collected at the time of the equipment request or replacement. In the event of a malfunction or power surge that triggers a configuration reset to factory defaults, please contact the Customer Service Center for support.

FRBKC has posted user guides on the SVC Portal for all of the devices used within an EagleCash and EZpay system. If there is an issue with the configuration of EagleCash devices, please contact the Customer Service Center for assistance.

In the event a device is moved from one merchant to another, a new configuration file must be obtained to update the device with the new merchant account data. A configuration file can be requested through the Customer Service Center.

7. System/Device Maintenance Activities

FRBKC has card reader cleaning kits that can be requested to ensure the readers are able to support operations without malfunction. Depending upon the implementation environment, some readers may need to be cleaned more frequently than others. Refer to bulletins and other user guide references to ensure devices are kept cleaned and maintained. The following key components should receive attention regularly:

- Card Readers (Point of Sale, Laptop, Kiosk)
- Laptop (Screen, Keyboard, Cable Management)
- Kiosk (Screen, Printer, Cable Management)
- POS (Screen, Keypad, Print Roller)

8. System/Device Operating Procedures

All devices are tested and validated as operational before being shipped. The appropriate version of software, device IDs, and merchant names are pre-programmed. Finance Officers, DDOs/DAs, and cashiers should contact the Customer Service Center if a device is not functioning properly after all local troubleshooting (power, battery, restarts) fails to achieve normal device operations. Key actions for finance officers to remember:

- Batch Point of Sale devices regularly to ensure proper settlement of accounts
- Rotate backup devices into daily operations to ensure proper functioning and load of current hotlist/warmlist
- Contact the CSC before moving a device from one merchant to another

C. Settlement and Accounting - End of Day Processing

Settlement and accounting is the process by which EagleCash and EZpay documentation is provided by the field to enable the FRBKC to process, reconcile, and post financial transactions to the applicable Merchant or Card Holder accounts.

The SVC Portal is the central location for uploading files and forms by field units, and retrieval by FRB for processing. The key files used to facilitate settlement and accounting process are:

- Transaction Files (TR) – from batched devices, uploaded weekdays before 11:30 a.m. CT
  - TR Files are generated by the CPS laptop
  - TR files should not be renamed
  - TR file formats support sorting and processing

- Vouchers Files – used to move funds to and from Finance Offices
  - 215s move funds FROM Finance Office DSSN (decreases FO DSSN's accountability)
  - 5515s move funds TO Finance Office DSSN (increases the FO DSSN's accountability)
  - Used to reconcile cash payments
  - Reconcile casual pay and checks made and received by the Finance Office

- Incident Reports – Lost, stolen, damaged, or expired cards (supports the hotlist)

- FS Form 2887s – New Card Holder Enrollments

**** FO Responsibility** - On a daily basis**, the FO should review the **Unresolved/Unattached Voucher** report and work with contacts at FRBKC to resolve in a timely manner. The **Unresolved** ticket/vouchers indicates vouchers that are missing transactions, are overstated, and/or are missing refunds (incident reports). The **Unattached** section of the report indicates FRBKC has received transactions; however, did not receive the corresponding ticket/voucher.

1. Batching Out

Batching out is the process of collecting the transactions from a POS day's business. The batch receipt must read "Successfully batched." If you don't see this, the funds were not transferred to the laptop and the batching process must be repeated. Hotlist files are updated at the time of batching to the version currently on the laptop.

Be sure to rotate and batch out devices each week (if you have a spare devices) to update the hotlist on the POS and ensure that the device is functioning properly.

2. Transaction File Processing

CPS laptops with internet connectivity can use the *Globe* option to directly upload files and forms to the FRBKC back office for processing. For timely EagleCash processing of stand-alone devices, batch out devices DAILY and submit vouchers and associated TR files, then upload them to the SVC Portal. *(EZpay POS devices batch directly to the back office via a phone line.)*

> ***NOTE:*** Forms that are received after 11:30 a.m. CT will be processed on the next business day and remain in the SVC Portal until processing has been completed. FRBKC is closed for business on Federal holidays and weekends.

3. Daily Reports

The Incident Report Log is a consolidated list of all incident reports uploaded into the portal by individual Finance Officers. There are separate reports for EagleCash and EZpay in the portal. The log has three tabs: 1) In Process; 2) Pending; and 3) Resolved. This is organized to help Finance Officers keep up-to-date on the status of these reported incidents. The current day's report will always be the file available in the portal. The previous day's reports are deleted.

- In Process tab – Shows cards reported and in-work for 10 business days. The goal for processing cards on this tab is any money remaining on a card is returned to the cardholder. In the case of a card that has a negative balance, these cards are researched for debt collection.
- Pending – Shows pending some action due to no banking information on record, incorrect, or missing cardholder information, or the card is warmlisted (due to a negative balance or by association when a cardholder has more than one card). Cards showing on this tab remain until the research or work required is completed.
- Resolved tab – Shows cards listed on the report where the residual funds have successfully been returned to the cardholders. There may also be notes associated with cards that are "End of Life, e.g., the card can no longer be used. This tab also only retains the past 13 months' of data.

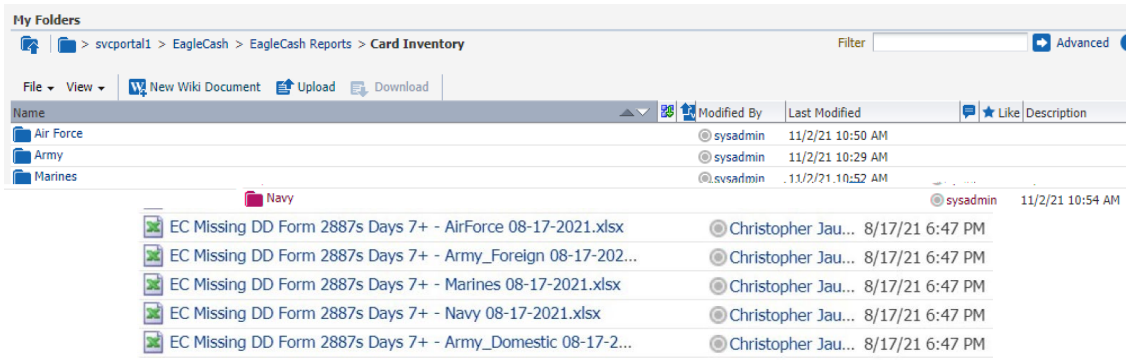
For EZpay Negative Card Reports – Two reports are posted daily to the SVC Portal

- Army, Air Force, Navy (social security numbers are stripped out of the reports)
- Marines (social security numbers are stripped out of the reports)

4. EC Missing or Incomplete FS Form 2887s

A report is published to the portal each Friday for each branch of the military, by base, showing cards issued that having a missing or incomplete 2887s. Using this report, Finance Offices can find a listing of any missing 2887s on tab 3 "Detail Missing Forms 7+ Days" by selecting their base from the base name dropdown.

**** FO Responsibility** - Each Friday**, FOs should locate the missing FS Form 2887 forms, scan and post them to the portal:



D. Fraud & Suspicious Activities

In a final rule issued in 1999, the Secretary of the U.S. Treasury added Money Services Business (MSBs) to the non-bank financial institutions required to comply with the Bank Secrecy Act (BSA). As the U.S. Treasury is an issuer of Stored Value Cards (SVC) through its operation of two SVC programs, EagleCash and EZPay, the SVC program is designated a Money Services Business under 31 CFR 1010.100(ff). A Money Services Business under 31 CFR 1022.210 is required to maintain an Anti-Money Laundering (AML) Program and prevent the Money Services Business from being used to facilitate money laundering and terrorist financing. The Anti-Money Laundering program shall be tailored to the product/service risk, customer risk, and geographical risk of the Money Services Business.

This guidance is provided to mitigate the risks to the EagleCash program. The Risk, Fraud, and Compliance (RFC) Group at FRBKC asks for the Finance Office and other responsible parties that administer the EagleCash program's assistance, as well as responsible AAFES personnel and others responsible for managing the EagleCash program, to comply with all Federal Rules and Regulations, EagleCash program policies and procedures, and DoD regulations, to prevent the program from being utilized for illicit activities. All Finance Offices and other responsible parties that administer the EagleCash program should adopt the EagleCash program SOP and AML Compliance program recommended procedures.

Information contained here will provide the local Finance Office with the information required to ensure AML Compliance Program that meets the regulatory requirements. The quality and effectiveness of the program depends on all administrators of the program's commitment to it. The only opportunity to verify cardholder information and identify suspicious activity is at the point of issuance and/or point of sale. This can only be done with a knowledgeable, well-trained Finance Office staff. Your participation and compliance with the EagleCash AML program is critical.

FRBKC is required to:

a. Incorporate policies, procedures, and internal controls reasonably designed to assure compliance.

b. Designate a person to assure day-to-day compliance with the program.

c. Provide education and/or training of appropriate personnel concerning their responsibilities under the program, including training in the detection of suspicious transactions to the extent that the Money Services Business is required to report such transactions.

d. Provide for independent review to monitor and maintain an adequate program.

1. What is Money Laundering

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership, or control of illegally obtained money. Money laundering is illegal and can involve any type of money, including money orders, money transfers, and other financial transactions.

Three Stages of Money Laundering

1. Placement: The introduction of illegally obtained money into the financial system.
2. Layering: The conversion of the illegally obtained money into another form, making it difficult to trace the money back to the original source.
3. Integration: The placement of laundered proceeds back into the economy.

MONEY LAUNDERING EXAMPLES

Example 1: A group of soldiers at Bagram, a military base located in Afghanistan, participate in an illegal gambling ring and have won some money. At the end of their deployment they do not want to travel with the cash proceeds, so they go to the local Finance Office conduct a Credit (i.e. Load) transaction to their EagleCash card. Once the funds are on the EagleCash card, the soldier walks over to an EagleCash Kiosk and ACH Unloads the funds back to his/her U.S. bank account. This soldier repeats this for several weeks. In order to avoid the reporting and recordkeeping requirements, the soldier only conducts Credit transactions of $350.00 per day, the daily load limit of the EagleCash card. In total, the soldier sent over $7,000.00 in illicit proceeds back to his/her U.S. bank account.

Example 2: Two government contractors (Contractors A & B) conspire and participate in a fuel skimming scheme by selling fuel to a 3rd country national for $40,000.00. On Monday, Contractor A brings $9,000.00 into the Finance Office and perform a Credit (i.e. Load) transaction to their EagleCash. On Tuesday, Contractor B brings $9,000.00 into the Finance Office and performs a Credit (i.e. Load transaction to their EagleCash card). Contractor A and B continue to alternate which day they go to the Finance Office to perform the Credit Loads until all $40,000.00 has been loaded onto the two cards. They then ACH Unload the funds at the EagleCash Kiosk back to their U.S. bank account; therefore laundering the money and integrating it back into the U.S. economy.

2. Compliance Standards

The United States Department of the Treasury, who administer the EagleCash program, expects all Finance Office Personnel who administer the EagleCash program to monitor the following compliance standards designed to detect and prevent money laundering and terrorist financing activities. This SOP portion outlines your responsibilities in regards to AML/BSA. Failure to adhere to these guidelines presents a risk to the EagleCash program and more importantly combatant command initiatives and goals, and may also violate Federal laws.

- Always conduct business in accordance with the highest ethical standards.
- Ensure that you obtain and enter accurate information into the EagleCash application.
- Ensure that you confirm that the customers are who they say they are.
- Do NOT assist in structuring.
- Do NOT assist in Money Laundering.
- Report any suspicious activity to FRBKC, specifically the Customer Service Center (CSC), your Command structure, and report to the local authorities immediately if the activity could involve criminal behavior.

PROHIBITED CONDUCT: There are certain behaviors which the Finance Office should not engage in, such as:

- ***Structuring*** - the Finance Office should not assist with or engage in structuring EagleCash transactions.
- ***Custom Roles*** - The Finance Office should not create and/or assign a custom role to Finance Office personnel without a valid reason and approval from Finance Office command and Branch Program Manager with notification to U.S. Treasury and FRBKC.
- ***Failing to Change Daily Download Limit Increases*** - Once the Finance Office increases the DDL for an EagleCash cardholder, the Finance Office must immediately change the DDL back to $350.
- ***Failure to Maintain Separation of duties*** - During the card issuance procedure, Finance Office personnel cannot issue themselves their own card.

3. Customer Service Identification Procedures (CIP)/ Know Your Customer (KYC)

The cornerstone of a strong BSA/AML program is the adoption and implementation of comprehensive CIP/KYC policies, procedures and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing.

As the EagleCash program provides a Stored Value Card, the program is required to verify the identity of a person who obtains an EagleCash card and obtain identifying information concerning such a person, including name, date of birth, address, and identification number. This is completed during the card issuance process as the applicant fills out the FS Form 2887.

Identifying the individual to whom the card is issued to is extremely important in reducing the risk of fraud at account opening. The Common Access Card (CAC) should be used to verify identify at account opening. If the individual does not have a CAC please refer to the other identity verification methods below. If the identity of the individual cannot be verified, the Finance Office personnel should notify the DDO/DA and the SVC program manager.

4. Suspicious Activity

EagleCash suspicious activity is defined as reported or detected unauthorized activity involving an EagleCash card and/or other EagleCash equipment.

Detected unauthorized activity includes patterns indicating misuse of the EagleCash card to transport funds derived from commercial or illegal activities, as well as misuse of program equipment in an attempt to hide fraudulent or illegal activities.

A suspicious transaction is one of more transactions:

- That involve funds derived from illicit activity and is intended or conducted in order to hide or disguise the illicit funds; or
- Designed to evade the BSA requirements, whether through structuring or other means; or
- Appeared to serve no business or apparent lawful purpose.

Many factors are involved in determining whether transactions are suspicious, including the amount, location of the transaction, where the transactions are being sent to, where the transactions are received from, source of funds (as well as AML concerns that may exist between the Finance Office location and the send/receive location), and/or comments made by the cardholder and the cardholder's behavior.

Examples of what the Finance Office should be looking for:

- A Credit Load transaction over the AML reporting threshold of $400.00 in deployed environments, where the source of funds is unknown
- Multiple transactions that are structured to avoid the reporting requirement
- A cardholder asks Finance / Disbursing Officer how to avoid a reporting requirement
- A cardholder threatens or bribes a Finance Officer to avoid providing information or having a report filed
- A cardholder uses an apparently fake identification or more than one cardholder tries to use the same identification
- A cardholder refuses to proceed with a transaction when asked for identification
- A cardholder refuses to provide all of the information required or seems excessively nervous or anxious
- Transactions are associated with illicit or suspicious funding sources
- A cardholder (or group of cardholders working together) sends or receives money transfers in amounts just below the recordkeeping thresholds or to avoid reporting. This would include anytime a transaction requires the cardholder to present identification
- A cardholder conducts transactions that are unusually large based on their past history, employment, rank, or level of income
- A cardholder comes into the Finance Office frequently with similar amounts of local currency and exchanges it for U.S. currency or deposits into their EagleCash account.
- A cardholder uses multiple EagleCash cards to structure their transactions into smaller denominations to avoid the reportable threshold
- A cardholder comes into the Finance Office and conducts a transaction that is out of pattern for their usual transaction activity

5. Structuring

Structuring is the act of breaking up a potential large transaction into several smaller transactions. It is illegal for an EagleCash cardholder to structure transactions to avoid the reporting requirements. Structuring is not only limited to multiple transactions on the same day, it also includes those conducted over more than one day if done to evade the reporting requirements.

Any load over the $400 threshold requires a source of funds memorandum. Anti-Money Laundering (AML) mitigation process implementation. Any Stored Value Card (EagleCash) cash to card credit transaction exceeding $400 within Finance Disbursing Operations requires supporting documentation. Finance Officers should upload documentation, in Memorandum format or other format as may be suitable, substantiating the source of such funds and purpose of the transaction to the SVC Portal.

> *NOTE: It is illegal for Finance Office personnel or a cardholder to assist anyone in structuring transactions. For example, Finance Office personnel may not tell or even imply to a cardholder that they can avoid reporting requirements by conducting smaller transactions. Finance Office personnel also may not notify the cardholder that their transaction is suspicious and that the Finance Office personnel is contacting FRBKC. Any suspicious activity detected by the Finance Office must bem kept confidential and referred to FRBKC.*

6. Additional Suspicious Activity Monitoring Efforts

a. High Risk List: On a quarterly basis, the RFC Group monitors cardholders who are deemed "High Risk." These cardholders include, but are not limited to, cardholders with more than four EagleCash cards, cardholders issued a card under an invalid SSN, and ad-hoc cases the RFC Group classifies as high risk.

b. Invalid SSN Monitoring: On a quarterly basis, the RFC Group asks Treasury Application Services to run a report on EagleCash card users with invalid SSNs. This is to ensure that all cards without a valid SSN are not ACH enrolled and to make sure Organization Cards are issued under the responsible party's name and information.

c. Large Returns: Bi-weekly, the RFC Group monitors large ACH Returns to ensure that the individual is aware of the return and its implications and ensure they are not engaging in illicit behavior.

7. When Do I Contact the Customer Service Centerv (CSC)?

a. Suspicious Activity: If you become aware of potential suspicious activity or need additional information, contact CSC.

b. Investigator Requests: If you are asked for EagleCash records from an investigator, contact CSC as all record requests need to go through the SVC Program Manager. Refer the requestor to the Privacy Letter template in the Appendix, Section 5, for requesting access to records.

c. CSC is available at:

EagleCash Program Customer Service Center
Federal Reserve Bank of Kansas City
Office: 1-877-973-9882
Email: eagle@frb.org or ezpay@frb.org

8. When Do I Contact Local Authorities?

a. Theft or Larceny: If you become aware of potential theft or larceny, contact local authorities immediately. This includes theft of EagleCash cards or EagleCash equipment.

b. Criminal Activity: If criminal activity or what you suspect to be criminal activity is reported to the Finance Office, contact local authorities immediately.

9. What Does the Risk, Fraud Compliance Group Do?

a. Monitor and Detect Suspicious Activity: The RFC Group runs weekly, monthly, and quarterly reports to monitor and identify suspicious activity. This includes monitoring the source of funds of a transaction, if a transaction is out of pattern for a cardholder or typical EagleCash program user, and if an EagleCash card is being used not for the purpose intended.

b. File Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs): The RFC Group monitors all transactions to determine if a SAR is needed. Under Financial Crimes Enforment Network (FinCEN) guidelines and Federal rules and regulations, a SAR must be filed when an EagleCash transaction is both (1) Suspicious, and (2) $2,000.00 or more within 30 days from the date of the initial detection of suspicious activity.

To be in compliance with the FinCEN guidelines and Federal rules and regulations, EagleCash must file a CTR for each transaction in currency (Credit Load or Debit) of more than $10,000.00 in one business day. Multiple transactions in one day must be aggregated to determine whether a CTR is filed or not. Within 15 days of the day following the day of the reportable transaction, the Risk Fraud and Compliance Group will file a CTR.

c. Process Record Requests for EagleCash Investigators (on behalf of U.S. Treasury): On a routine basis, U.S. Treasury receives requests from investigatorsr. These requests are forwarded to the RFC Group for completion. Most of these requests pertain to providing EagleCash transaction detail reports and other identifying information on a specific cardholder or group of cardholders.

NOTE: *If someone comes into the Finance Office and asks for records, please refer them to Customer Service Center, as all records requests must go through CSC and the EagleCash program manager.*

d. Identify Ongoing Trends through Data Analytics: Identifying trends and placing mitigating controls in place is important in protecting EagleCash cardholders. Throughout the year, the

RFC Group performs data analysis on SAR volume, trends in suspicious activity, and trends in record requests. The RFC Group also analyzes data to identify risks to the program and implements changes based on the analysis.

e. Program Awareness and Education: The RFC Group works on EagleCash program awareness and education throughout the year. This includes sending bulletins to the Finance Office via the Portal, providing information on AML initiatives, and reaching out to individual Finance Offices.

10. Data Protection

In addition to meeting your recordkeeping requirements, you should also protect your cardholder data. Protecting cardholder data includes:

- Use Privacy Act coversheets when hard copy documentation is not in a file cabinet
- Properly destroying forms or notes with cardholder Personally Identifiable Information (PII) and/or transaction information
- Locking cardholder records in a secure location. This can include forms, copies of identification, government reports, and EagleCash transaction reports
- Locking and securing lost or cancelled EagleCash cards

11. Best Practices for Finance Offices

a. Ensure timely updates to authorized account contacts by providing FRBKC Form 417s on a regular basis.

b. Monitor creation of users and assignment roles.

c. Review EagleCash CPS Admin Tool Reports & Activity Logs to ensure no custom roles are being assigned to finance office personnel that should not have a custom role.

d. Limit physical access to cards and equipment.

e. Ensure all lost cards are turned into the DDO/DA and an incident report is filed with FRBKC.

f. Ensure if a cardholder discovers suspicious activity on their card, they should contact CSC to provide a transaction detail report, report the cardholder is requesting a card cancellation, and file a report to the local Military Police.

g. If the Finance Office receives an investigative request, contact CSC, as all investigative requests should go through the Bureau of Fiscal Service.

h. Ensure back up equipment is stored in a secure location and batched out every 30 days.

i. Review and maintain equipment and card inventories.

j. Review and respond to missing kiosk and laptop file requests.

k. Review EagleCash ACH Returns Log daily.

l. Review the missing 2887s report on the Portal and ensure all missing 2887s are located and uploaded to the portal.

12. Policies and Procedures Governing AML Compliance

- DOD FMR Volume 5, Chapters 4, 10, 11
- Treasury Financial Manual, Chapter 9000

** Note: If there is any discrepancy between what is included in this EagleCash Standard Operating Procedures and a DoD Policy and/or Procedure, the DoD Policy and/or Procedure is the higher authority and should be followed.

E. Finance Officer Appointment - Turnover

1. Training

During normal operations, new EagleCash and EZpay Finance Officers are offered eCommerce training virtually or on-site at the Federal Reserve Bank of Kansas City – Omaha Branch. Additionally, training materials are available on the SVC Portal. Training is provided to teams during initial installation of EagleCash and EZpay system by a joint team of Department of Treasury, Bureau of Fiscal Service, Federal Reserve Bank, and military service Program Management staff.

Local Finance Officer turnover should be completed following local military procedures (hand receipts, operations logs, etc.) during rotations when a new unit takes responsibility for a particular site.

2. System Asset Accountability Transfer

Each military branch publishes procedures for asset/equipment custodian/property book transfers are to be followed. However, it is critical that all provisioned equipment provided during the EagleCash/EZpay installation process are accounted for and regularly reported to FRB for tracking purposes.

Section 3 – Card Management

A. EagleCash Account Enrollment

1. Evaluating Eligibility

a. Prospective cardholder presents photo-ID and completed FS Form 2887 to Finance/Disbursing Office Cashier.

b. Cashier compares government issued photo-ID to name printed on FS Form 2887.

c. Cashier confirms eligibility of prospective cardholder to participate in the EagleCash program as follows:

d. If the prospective cardholder is a member of the U.S. Military or a U.S. Government Civilian:

i. The Finance Officer inserts the new cardholder's CAC or new EagleCash card into EagleCash Card Processing Station and enters the prospective cardholder information contained on the FS Form 2887.

ii. The prospective cardholder signs the back of card and hands the card back to the cashier.

e. If prospective cardholder is NOT a member of the U.S. Military or a U.S. Government Civilian:

i. Cashier checks the list of Contractors with approved Check Cashing Agreements on file with the Finance/Disbursing Office.

ii. If an agreement is on file and current, cashier follows steps above and issues card (enter the name of the Contractor Firm in Block 11a on FS Form 2887).

iii. If no agreement is on file or is expired, cashier informs prospective cardholder they are not eligible to participate in the kiosk portion of the EagleCash.

f. In the rare case that a hard copy FS Form 2887s must be created, Finance Officers should ensure they are scanned and submitted to FRBKC for safeguarding. Where scanning is not available hard copy originals will be sent daily via government official mail. FRBKC secures and maintains the forms on file indefinitely. The Finance/Disbursing Office retains copies of completed FS Form 2887s in the safe for at least 60 days to ensure that the forms have been successfully received by FRBKC, and then disposes of them according to policy for destruction of documents containing Personally Identifiable Information.

g. Finance/Disbursing Office transmits EagleCash card issuance files captured in the EagleCash Card Processing Station electronically to FRBKC at the close of each business day.

B. Card Issuance Policy

1. Overview

Prior to any card issuance, all Finance/Disbursing Office personnel must be trained on all aspects of the equipment, forms, and processes related to account creation and card issuance. The Finance/Disbursing Office issues all cards used in the EagleCash and EZpay programs.

When an EagleCash card is first issued to any authorized military personnel, government official, or civilian contractor, the card has no value. EZpay cards are issued with pre-set values. After issuance, EagleCash cards can be loaded at a self-service kiosk or the Finance/Disbursing Office with funds drawn from a valid form of currency. EagleCash kiosks are free-standing cashless ATM-like devices carry the trademarked EagleCash signage for easy identification and are installed in key traffic areas such as Finance/Disbursing Offices, Army & Air Force Exchange Service (AAFES), Navy Exchange (NEX) stores, Post Office facilities, and the MWR centers at each theater where the EC program has been implemented. Cardholder kiosk activity requires entry of a Personal Identification Number (PIN) to gain access to the kiosk transaction menu.

EagleCash cards should be issued to all deploying soldiers and Department of Defense (DoD)/Department of the Army civilians at a designated Soldier Readiness Processing (SRP)/Army Military Pay Office (AMPO) located at a CONUS issuance site. If not, the EagleCash card must be obtained in the contingency area of operation.

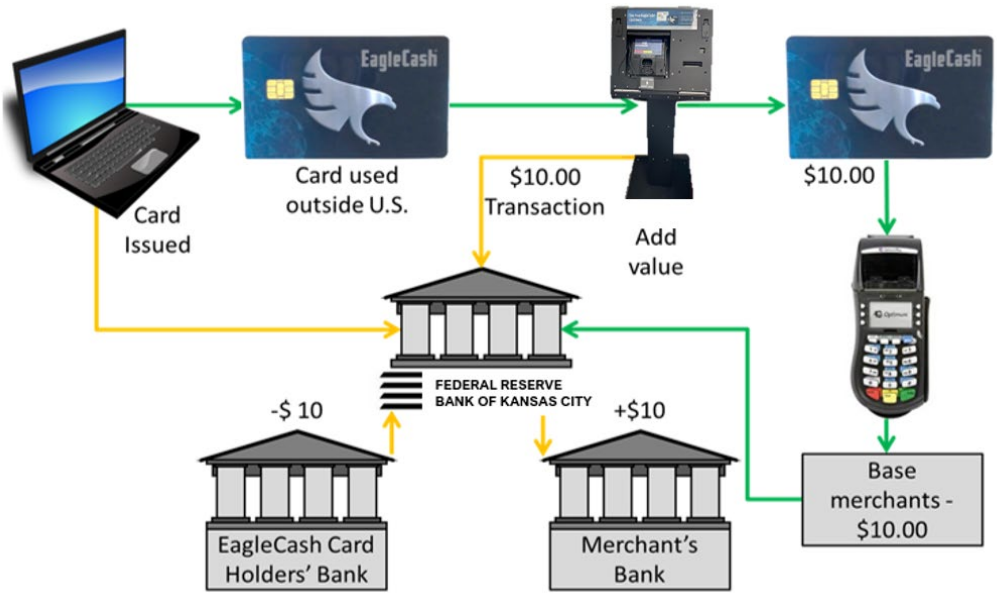
All cards are issued for 13 months, funds on the card will expire at the end of the issuance period. The issuance period can be extended at a CPS prior to the funds expiring. If the funds are allowed to pass the expiration date the card cannot be reactivated until 60 days have passed at which point the card can be re-issued.

At card issuance, bank information is verified and collected, and a PIN is assigned at the chip level. This PIN must be entered by the cardholder at the time of purchase at a POS terminal.

The expiration date on the back of the EagleCash card is the date that the card is physically expired and can no longer be re-issued. If the EagleCash card is expired a new card can be immediately issued to replace it.

For Cards that expire with funds on them, within 21 days after expiry FRBKC generates an ACH credit to the cardholder's bank account of record for the residual balance of the card.

Below is a graphic depicting the card issuance, loading value onto the card, and the value exchange from the card, through the merchants and linked bank accounts:



2. Card Issuance to an Individual

Upon request to open an account, the finance office requires the applying cardholder to fill out the CPS electronic version of the FS Form 2887. This form provides identifying details to better understand the customer the card is being issued to. The card holder is required to provide theirv (some of this information will pre-fill into the CPS online FS Form 2887 automatically from cardholder's CAC):

1. Full name, military branch, or organization/company name
2. Date of Birth
3. Social Security Number/ Tax-Payer Identification Number (SSN/TIN), DoD ID Number
4. Other ID number if non-U.S. citizen
4. Permanent residential address, personal email

Additionally if the individual is choosing to ACH Enroll their card, they must provide:

1. Bank or Credit Union Name
2. ABA Routing Number
3. Account Number
4. Account Name (Bank account must be in name of cardholder)
5. Whether the account is Checking or Savings account

3. Card Issuance to an Individual Without a SSN/TIN

EagleCash cards issued to an individual that does not have a SSN/TIN are not allowed to be ACH Enrolled. The finance office should follow the "Card Issuance to an Individual," section (a) above.

As the individual does not have a SSN/TIN, in the SSN field please use "000" followed by the first six numbers of the identification used. Please refer to the "Additional Identification Acceptable for Individuals without valid Social Security Number for ACH UnEnrolled Cards" located above. Also, if the number of the identification used does not have 6 digits, precede the number with an additional "0."

4. Card Issuance to a Dependent and/or Spouse

Currently there is no policy on the issuance of cards to a dependent and/or spouse.

It is recommended that if a card is issued to a dependent and/or spouse that the card is issued in the primary cardholder's name, SSN, address, and date of birth with the dependent and/or spouse receiving a second card tied to the primary cardholder's account. It is the primary cardholder's choice to ACH Enroll the dependent and/or spouse card. If the card is ACH Enrolled the banking information must be the same as the primary cardholder.

> ***NOTE:*** *In certain situations, a dependent cardholder may be under the age of 18 years old. It is the primary cardholder's decision to ACH Enroll their dependent's EagleCash card. The primary cardholder will be responsible for any illicit activity conducted on the dependent EagleCash card.*

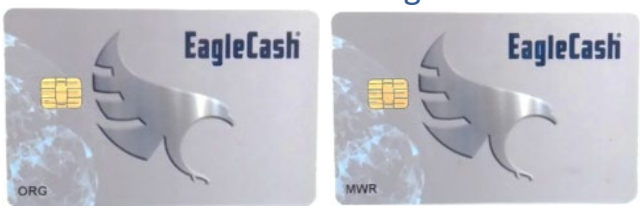
5. Issuing More Than One Card to an Individual

Multiple cards for a single card holder are authorized for legitimate reasons, (i.e. dependents using the sponsor's social security number (SSN)). Organization cards should be issued in the name of the Responsible Party; the Responsible Party may have multiple EagleCash cards issued.

While multiple cards are allowed, they are deemed risky by the RFC Group, as the potential for structuring and for a larger loss to Treasury is increased when a cardholder has multiple EagleCash cards.

> ***NOTE****: Each individual is permitted a DDL of $350, meaning the sum of all personal EagleCash cards, tied to the same bank account, issued to an individual needs to be $350. (Eg.,. Card #1 DDL is $150; Card #2 DDL is $200.)*

6. Card Issuance for an Organization



Upon account opening for an Organization card, the finance office will require the Organization card to be issued in the name of the responsible party (i.e. Treasurer) and under the responsible party's SSN/TIN. This will better help the RFC Group identify a person who is responsible for the card and its activity. The responsible party will be required to provide the same information as required for an individual card issuance with the addition of the "Organization Name" listed in Box 11a.

If the Organization is a Military Sponsored Organization and wants to ACH Enroll their card, the Finance Office will require additional information to be provided, such as:

a. A completed FS Form 2887
b. Articles of Incorporation of the Organization/ Orders from their Command
c. Proof of identification: TIN/SSN or copy of the authorized party's personal identification card
d. Proof of business banking account in the Organization's name, with the responsible party listed as authorized user (unless instructed otherwise)
e. A document stating the purpose of the Organization and anticipated transactions

NOTE: *Organization cards that are issued to military organizations should not be ACH Enrolled.*

7. Card Issuance to a Merchant (EagleCash Deposit Card):

This issuance process is completed by FRBKC and requires vetting through FRBKC Legal.

a. Description: A special type of EagleCash card, known as a Deposit Card, is issued by Finance/Disbursing Offices to Post Office Custodian of Postal Effects (COPE), AAFES PX/BX and NEX store managers, and non-AAFES vendors that have a valid U.S. bank account. The Deposit Card replaces the use of Cash Collection Vouchers (CCVs), and Treasury checks to convert cash from deposits to EagleCash. In this instance, Finance/Disbursing Office personnel will load value onto the card using cash funds brought in by Post Office, AAFES, NEX, or other merchants from their daily receipts. After issuance and funds loading, the Deposit Card owners—generally the Post Office COPE or AAFES store manager—goes to an EagleCash Kiosk and performs an unload of the full card balance, which results in a credit to the associated Postal/corporate bank account.

b. Deposit Cards must be issued to a merchant using the following conventions:

- Organization = Merchant Name. Example: AAFES
- Location = Location and Zone as applicable. Example: Liberty or Arifjan Z1
- SSN = Primary four numbers of the facility code followed by 5 zeroes

Example: Facility Code 1551 shows as SSN 155100000.

c. At AAFES or NEX locations where cash deposits are likely to exceed $100,000, the Finance/Disbursing Office will issue multiple cards. When multiple cards are issued, the naming convention is:

- Organization = Merchant Name. *Example: AAFES*
- Location = Location and Zone, if applicable, followed by 1, 2, etc. to differentiate each card

Example: Two cards issued to AAFES at Camp Liberty would be issued as AAFES Liberty 1 and AAFES Liberty 2.

NOTE: *The AAFES / NEX store manager or COPE must complete FS Form 2887. The Finance/Disbursing Office is responsible for ensuring accurate completion of this form. See Appendix A, Form 1a. FS Form 2887 Application for Department of Defense (DoD) Stored Value Card (SVC) Programs or 1b. Sample of a Completed FS Form 2887.*

8. ECAS Card Issuance:

a. EagleCash Agent SVC Cards (ECAS) are used by various Military programs for a variety of reasons. One current use for ECAS cards is for Intelligence Contingency Funds (ICF) agents who are issued ECAS cards at the local Finance/Disbursing Office. The agent can load or unload electronic U.S. currency onto the card at self-service kiosks linked to a designated U.S. checking account. ECAS is re-loadable and can be used immediately anywhere on base where EagleCash is accepted. Using ECAS, agents can also conduct exchange transactions for cash at Finance/Disbursing Offices. Not all Military programs that issue ECAS cards allow the cards to be used at self-service kiosks.

b. The ECAS program includes all software, hardware, training, processes, and support to implement and maintain the application. The Finance/Disbursing Office will issue ECAS and serve as an intermediate point of contact for customer service issues (cardholder questions, lost, damaged, stolen cards). To be issued an ECAS card, agents must complete the Authorization to

Fund EagleCash Agent Stored Value Card (ECAS) (FS Form 2888, Formerly SVC FORM 500). Only Class B agents can obtain this type of card.

c. Cards are issued at the Finance Office in a similar fashion to an EagleCash card except that these cardholders fill out a FS Form 2888, FS Form 500 (Authorization to Fund EagleCash Agent Stored Value card) and obtain a signature from the Class B agent signature authority. The FS Form 2888 is scanned into the portal and FRBKC uploads to the 2887/2888 catalog.

C. Card Acceptance Policy

1. Cardholder presents EagleCash (EC) card and photo-ID to cashier at time of payment.

2. Cashier compares name printed on EC card to name on photo-ID.

   a. If names match — cashier compares the photo-ID to the physical appearance of the purchaser. If there is a match, cashier completes the sale.

   b. For legacy card stock: If names do not match — cashier rejects the EagleCash card and requests an alternate form of payment. Cashier directs customer to the Finance/Disbursing Office.

   c. For legacy card stock: If there is no printed name or completed signature on the EagleCash Card — cashier rejects EagleCash card and requests alternate form of payment. Cashier directs customer to Finance/Disbursing to validate customer information on the chip and update back panel of the card.

   d. If there is a printed name but no signature on the EagleCash Card — cashier confirms purchaser is appropriate cardholder by checking government issued photo-ID and requests they sign the back of the card before accepting it as the form of payment.

3. Cashiers direct any EagleCash cardholder customer service issues to the Finance/Disbursing Office.

4. Compliance with the EagleCash Card Acceptance Policy and the EagleCash Hotlist Procedures indemnifies AAFES and MPSA from any liability associated with any EagleCash transactions that are subsequently deemed to be unauthorized by the cardholder.

5. Non-compliance with the EagleCash Card Acceptance Policy and EagleCash Hotlist Procedures should be handled according to internal AAFES and MPSA policies that govern employee work rules and job performance. AAFES and MPSA are not indemnified from liability associated with EagleCash transactions that involve intentional violation of this policy or fraudulent activity and are subsequently deemed to be unauthorized by the cardholder. All such incidents will be evaluated on a case by case basis.

6. Types of Identification

The Finance Office must make every reasonable effort in determining the identity of each EagleCash cardholder. If the applying cardholder is refusing to provide identifying information, the Finance Office should contact their DDO/DA and elevate to the RFC Group through the CSC. As a reminder, a CAC is the preferred method of identification. If a CAC is not available, refer to the list below of acceptable forms of identification.

a. Identification Acceptable for Individuals/Organization Cards (should be issued in individual's name) for ACH Enrolled and ACH UnEnrolled cards:

- A valid Common Access Card (CAC) **Preferred*
- A valid Military ID
- A valid state driver's license
- A valid state issued non-driver identification card
- A State-issued ID
- A valid US passport

b. Additional Identification Acceptable for Individuals without valid Social Security Number for ACH Unenrolled Cards:

- A valid foreign passport
- A U.S.- issued alien registration card
- A Resident Alien card
- Base Identification Card
- Employee Identification Card

c. Unacceptable Identification:

- Temporary or expired driver's license
- Club and association cards
- Library card

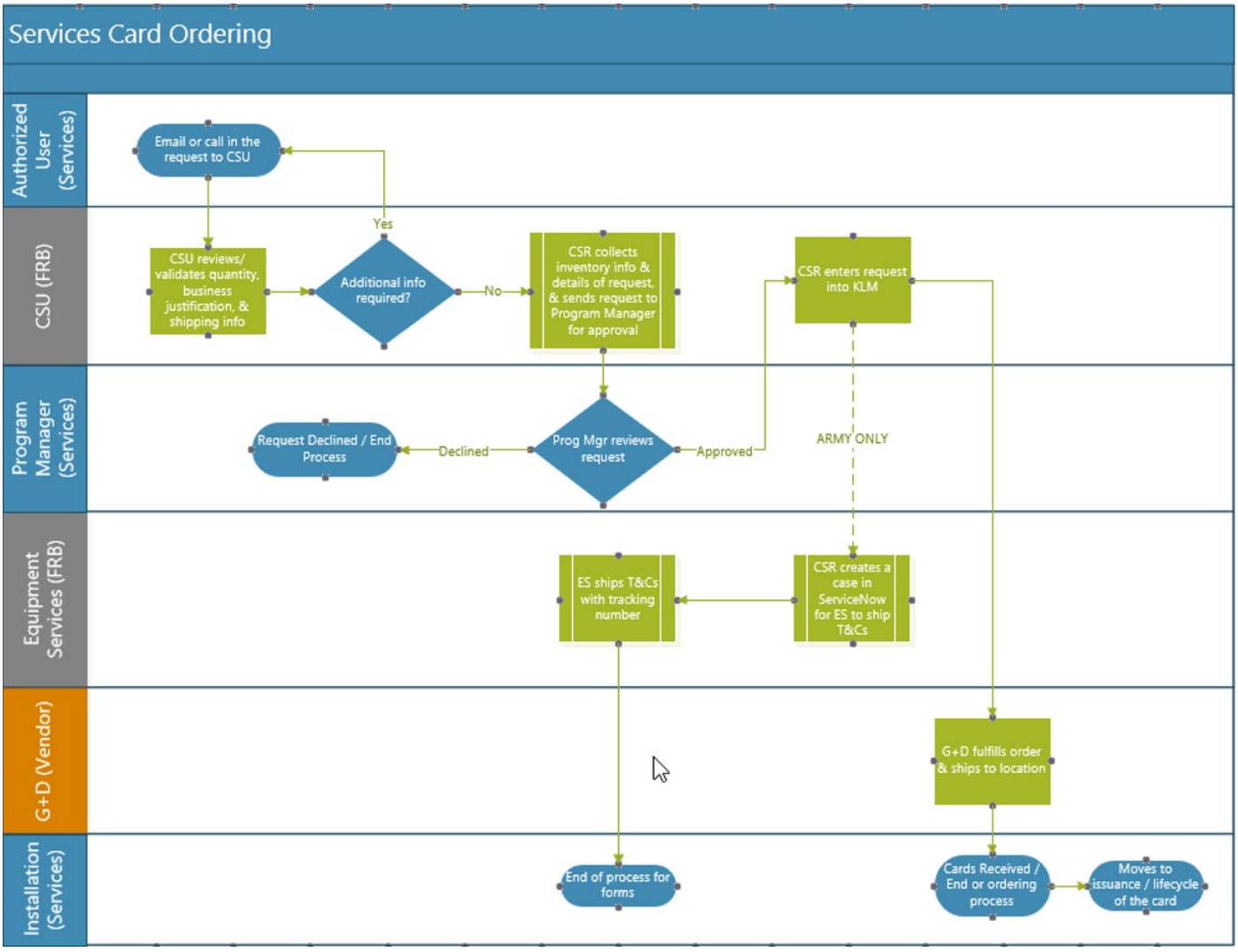
NOTE: If you encounter a form of identification not mentioned above, contact your Command to ensure it is a valid form of identification.

D. Card Ordering:

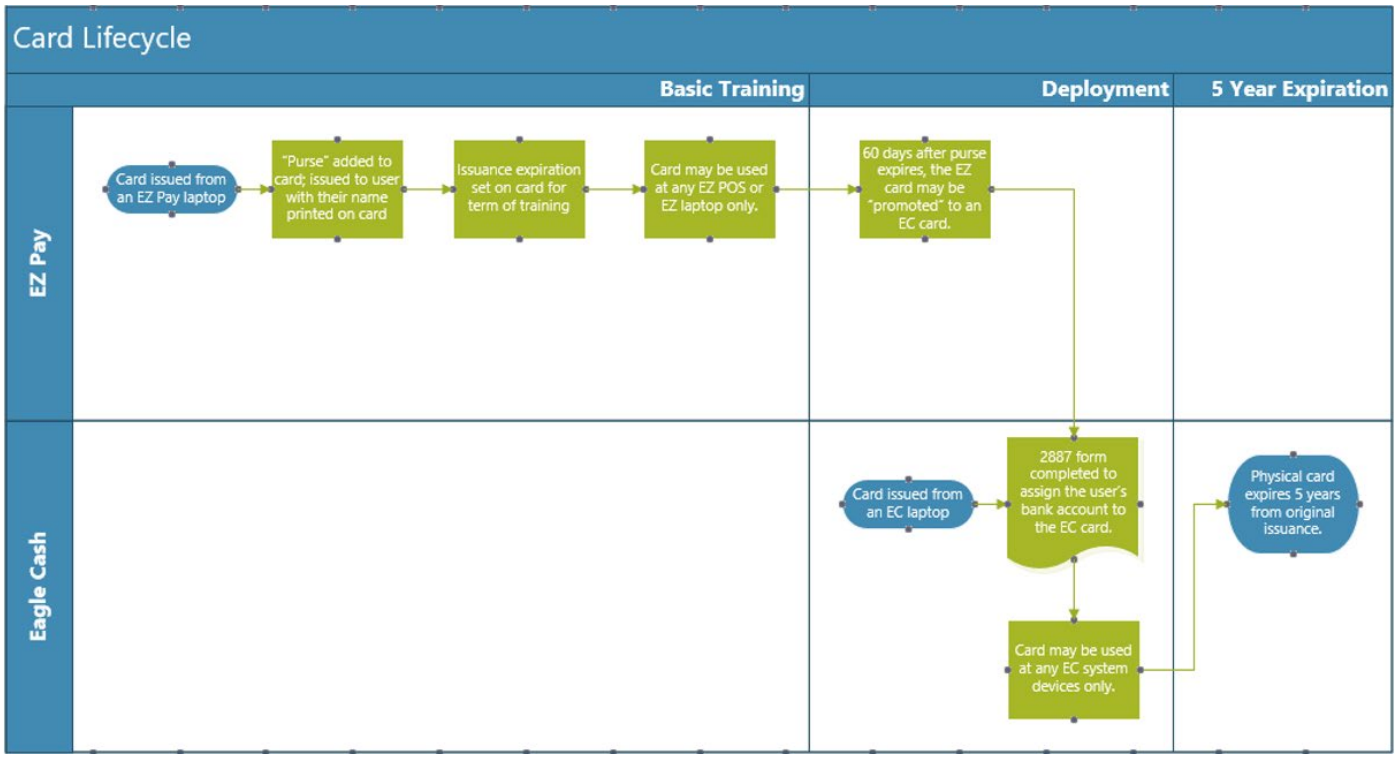
Card ordering begins with an email or phone call. FRBKC Customer Service has a card order template for collecting necessary data to facilitate the card order request:

- Account/Location
- Shipping Address
- Current Card Inventory on Hand
- Quantity of Cards Requested
- Card Priority (Urgent/Standard)

The graphic below depicts the stages/flow of the card ordering process with swim lanes for the parties involved in requesting/fulfilling card order requests:



The graphic below depicts the lifecycle of EagleCash and EZpay cards from issuance at a military training location, the transition to deployment and finally, expiration:



Current legacy card stock inventories should continue to be used/issued before using new card stock unless otherwise instructed. All card accepting devices are backwards compatible with legacy and new card stock.

**** FO Responsibility** - The 1st of each month**, the FO should complete an accurate card stock inventory and post the results to the SVC Portal using the template titled "Monthly Card Inventory Report Template.xls" Fill it out, rename the file using the following naming convention "Base Name_Inventory_Month_Year," and upload it into your applicable service folder (i.e., Army, Air Force, Marines, Navy) at the following SVC portal directory folder:

> svcportal1 > EagleCash > EagleCash Reports > **Card Inventory**

E. Card Inventory & Control

The Finance/Disbursing Office plays a key role in the implementation and day-to-day management of the EagleCash program. The Finance/Disbursing Office is responsible for EagleCash card issuance, transaction processing, incident reporting of lost, damaged, and stolen cards, and oversight of all EagleCash kiosks on base. As the owner of card issuance, the Finance/Disbursing Office must train and educate personnel on the mechanics of card issuance, implement procedures to ensure safekeeping and audit of all card stock held on premise, and actively help promote the growth of the program on base.

Additionally, all Finance/Disbursing Office personnel are to be trained on, understand, and follow the requirements of the EagleCash Card Issuance and EagleCash Card Acceptance procedures and the EagleCash Cash Back policy outlined in this section. All card stock within the EagleCash program is tracked and audited. Army, Air Force, Marines, and Navy Finance/Disbursing Offices maintain cards in inventory for issuance. Cards are stored in the manner of blank check stock in compliance with Volume 5, DoD FMR (Department of Defense Financial Management Regulation), and paragraph 0310 and are inventoried on a monthly basis. The Finance/Disbursing Office issues the cards and can load/unload funds to the chip on the cards if requested by cardholders and as permitted by policy.

EagleCash cards are supplied to Finance/Disbursing Offices by FRBKC when authorized by Army, Air Force, Marines, or Navy. Cards are numbered with a card serial number and packaged in sealed sleeves. Initial inventory must be verified, and the inventory sheets attached to each sleeve must be signed. As EagleCash cards are allocated to Finance/Disbursing Office personnel for issuance to cardholders, a Statement of Agent Officers Account DD Form 1081 must be completed and referenced back to Subsidiary Accountability Record DD Form 2667.

For legacy card stock, the cards must be kept and issued in numerical order. A monthly inventory of EagleCash card stock must be performed and relevant information entered onto DD Form 2667 or other approved form. This inventory information must be sent via email to the Customer Service Center (CSC) at eagle@frb.org. All cards must be counted and totals confirmed by email. Damaged, expired, or any cards held as a result of Incident Reports (IR) must be kept in a secure place. The CSC will provide direction on how damaged or expired cards are to be managed.

The following are quick reference points for handling inventory of EagleCash cards. The Finance/Disbursing Office is responsible to do the following:

- Check and verify the number of cards delivered
- Sign receipt for cards received
- Maintain card stock in sleeves by serial number
- Issue cards by serial number
- Perform monthly inventory or turnover to responsible person with full inventory and receipt
- Send the monthly inventory or turnover report status to the CSC via email at eagle@frb.org

F. Card Usage – Load & Unload Funds

EZpay cards are pre-loaded using payroll advance for the cardholder with a fixed dollar value.

EagleCash cards load or unload funds at a kiosk (bank to card, card to card, card to bank). Reference the device user guide for details on specific funds load and unload activities.

G. Negative Balances

- Cards with a negative balance will appear on the warmlist and researched for debt collection.
- If a cardholder has more than one card, all cards for that member are warmlisted by association.

H. Incident Reporting (Lost, Stolen, or Damaged Cards)

When an EagleCash card is lost, damaged, or stolen, the cardholder should report the incident immediately via phone call to the EagleCash Customer Service Center (CSC) or at the local Finance/Disbursing Office. If the cardholder requires a new EagleCash card, they can be issued a new card at the Finance/Disbursing Office. The Finance/Disbursing Office will complete an Incident Report (IR), FRBKC Form SVC-414, and post the IR on the SVC Portal.

The timely reporting of the lost/damaged/stolen card by the cardholder is essential. Cardholders should be made aware of this policy upon the issuance of a new card. The receipt of the phone call triggers several activities by the EagleCash CSC. First, the card information is added to the Hotlist file, which is updated on EagleCash laptops that transmit files to FRBKC via a LAN / Internet connection, or distributed via email or SVC Portal. At the end of the day, these files are manually uploaded to EagleCash devices. In addition to the call, an IR should also be completed at the Finance Office. FRBKC researches the IR, validates recent card transaction history, and the card balance. If the lost, damaged, or stolen card has a linked bank account, CSC then returns the residual balance to the cardholder's bank account via ACH. If the lost, damaged, or stolen card is not linked to a bank account, CSC authorizes the Finance/Disbursing Office to return the residual value to the cardholder with cash or a newly issued EagleCash card.

A new card can be issued once the initial call to FRBKC has been made. The balance for the card reported during the call cannot be refunded or disbursed until CSC emails the phone request to the EagleCash Processing Group. The card will be Hotlisted on the same business day. FRBKC waits 4 business days prior to returning the balance of the card to the cardholder.

The customer can add value to the new card by writing a check, receiving a (qualified) casual pay (partial payment), or at an EC kiosk, and can return to the Finance/Disbursing Office later for the refund.

> *NOTE: FRBKC maintains and logs all IRs submitted. A copy of this report is located on the SVC Portal. The Finance/Disbursing Office is responsible for maintaining a copy of all IRs submitted for its own records.*

**** FO Responsibility** - On a daily basis**, the Finance Office should review the Active tab of the **Incident Reports Logs.xlxs** file located in the SVC Portal to monitor current Incident Report Form statuses. The FO should also monitor the Pending tab, which indicates all of the Incident Report forms that FRBKC is unable to process.

I. Hotlisted/Warmlisted Cards

Eagle Cash kiosks and Point of Sale Devices also receive the HotList and WarmList during the daily preprogrammed DSN/commercial telephone line file transfer process. In some instances, the HotList/WarmList is transferred to the kiosk via a dialup DSN line. However, should the DSN line be inoperative or unavailable, it is the responsibility of Finance/Disbursing Office or KMBO (Kiosks Managed by Others) personnel to update the kiosk daily with the latest HotList/WarmList using an authorized method based on local guidance (i.e. EC kiosk collection laptop). Additionally, when a kiosk is unable to use DSN, Finance/Disbursing Office personnel are responsible for collecting all transactions stored at the kiosk and ensuring that those transactions are uploaded into their respective folder on the SVC Portal.

1. Hotlist:

If a HotListed card is inserted into a kiosk or POS terminal that contains the most recent HotList, that card will become permanently disabled.

Monday through Friday, FRBKC prepares and distributes four electronic files daily to the Finance/Disbursing Office, Post Office, AAFES, NEX and to EC kiosks (via Defense Switched Network (DSN)). All files are distributed via either LAN/Internet, email, and/or the SVC Portal. Each file plays a distinct and critical role in the management of the EagleCash program.

These files are the HotList, WarmList (non-readable file), Warmlist Reason File, and the WarmList Excel file with the name Open ACH Return Log.xls. These files are explained in detail below:

Hotlist File: This is a file of all EagleCash cards reported lost, damaged, or stolen once an IR is submitted, WarmListed (cards that are not eligible to be used in an EagleCash kiosk until they are resolved) or HotListed (permanently inoperable) across all theaters where EC is implemented. Finance/Disbursing Offices, Post Offices, and AAFES receive the daily HotList and download it to their respective EagleCash laptops, kiosks, and POS terminals. Cards on the HotList are disabled at POS terminals and kiosks. Cards reported lost, damaged, or stolen are added to the next regularly scheduled HotList following receipt of an IR. Once a card is on the HotList, it is not removed. A cardholder who has reported a card lost and subsequently finds it must be issued a new EagleCash card. The lost card is rendered inoperable once it is placed on the HotList.

It is the responsibility of each program participant – Finance/Disbursing Office, Post Office, AAFES, and NEX – to ensure that the most recent HotList is loaded to all EagleCash laptops, POS terminals and kiosks in production (meaning installed and accepting transactions). Refer to the HotList/WarmList Procedures in the CPS User Guide. During the daily upload of transactions from POS terminals to the laptop, the HotList is automatically downloaded to the terminal.

Collecting (Batching) Transactions from the POS Terminal: If a HotListed card is presented for payment, the transaction is not approved and the response HOT CARD is displayed at the terminal. Should that occur, an alternate form of payment should be requested and the cardholder should be instructed to see the local Finance/Disbursing Office.

2. Warmlist:

All EagleCash kiosks receive a daily WarmList. This file contains EagleCash card numbers that for one reason or another are not eligible to be used in a kiosk until they are resolved. The most common reasons a card is WarmListed are that American Bankers Association (ABA) routing or bank account information was processed incorrectly during issuance, cards had transactions returned for insufficient funds, or closed bank accounts. While cards on the HotList are not accepted for purchases and are rendered permanently inoperable, cards on the WarmList are still accepted for purchase at POS terminals up to the balance remaining on the card, but are temporarily blocked by EagleCash kiosks for load and unload functions. Thus, additional value cannot be transferred to or from the card until the reason the card was WarmListed is resolved.

When a cardholder attempts to use a WarmListed card at the kiosk, the cardholder receives a SEE FINANCE OFFICE response. The EagleCash cardholder should go to the local Finance/Disbursing Office for resolution assistance. Unlike a card that is on the HotList, a card on the WarmList does not need to be re-issued. Once the reason causing the card to be on the WarmList is resolved, the card is removed from the WarmList making the card operable at the kiosk once again. Cardholders on the WarmList should not be issued new cards.

**** FO Responsibility** -** If a cardholder is having difficulty using their EagleCash card, the Finance Office should search the log to determine if the cardholder is warmlisted. If the cardholder is warmlisted, the cardholder should contact the FRBKC Customer Service Cetner. Please remember, warmlisted cardholders should not receive a new EagleCash card until their debt is resolved.

J. Refunds

There are no refunds with the EZpay program. All EagleCash refunds are subject to the $350 daily download limit. Cardholders should work with the vendors who sold items for any necessary refunds.

K. Closing Cardholder Accounts

Accounts will close upon card expiration unless extended. Approximately three weeks after expiration of a card, any funds remaining on the card will be returned to the linked bank account. If there is no linked bank account, the cardholder can cash out the value remaining on the card by visiting the Finance Office. Once funds are provided to the departing individual, the Finance Office will complete a incident report along with a DD Form 215 for reimbursement of the expended funds.

Cardholders departing the deployed theater should unload any remaining value on their cards at a kiosk before returning stateside. If departing cardholders do not have the opportunity to unload funds at a kiosk prior to departure from the theater and there are funds remaining on the card, contact the Customer Service Center and they will assist.

Section 4 – Appendix

A. Customer Support Resources

1. Customer Service Center

Remember, to ensure devices are in proper working order, batch them out regularly whether they are used in daily operations or not (backups).

Device user guides and operational bulletins are posted on the SVC Portal for your reference.

If you have any questions or issues with devices, contact the Customer Service Center. Call the EagleCash Customer Service Center (CSC) at DSN (312) 955-3555 or US Toll Free 1-877-973-8982 Monday through Friday (except Federal Holidays) from 0000 to 1800 CT or email eagle@frb.org or ezpay@frb.org.

2. Case Management

Case Creation and Assignment:

- All phone calls and emails to FRBKC Omaha Branch Customer Service are logged as cases.
- The customer service representative handling the case will request information from the caller to verify the individual is an authorized account contact or cardholder.
- Depending upon the issue, most cases are resolved during first contact. In some cases, additional review/troubleshooting may be required and the case reassigned to another department for resolution.

Case Processing:

- Cases for all SVC Card programs are resolved after confirmation of resolution with the customer.
- Cases are closed 30 days after being resolved. Information can be added after resolution, or the case can be reopened if the same issue for the same account/device persists.
- If there is interaction with the customer via phone or email on an open/active case, these activities are captured in the case work log. If there is an open/existing case for an issue being worked, when customers call in, the case number is used to locate and update the case record.

3. SVC Portal

File Upload and Download:

- Access Secure Restricted Reports
- Access Forms Templates
- Upload files and forms (FS Form 2887s; AML Supporting Documents; Incident Reports; Vouchers (EagleCash only); Card Inventory; TR Files and Register Receipts)

4. User Guides & Quick Reference Guides

- **EagleCash Refunds User Guide** EC users guide.qxd (treasury.gov)
  https://www.fiscal.treasury.gov/files/eaglecash/ec-refund-guide.pdf
- **EagleCash Kiosk User Guide** Kioskguide.qxd (treasury.gov)
  https://www.fiscal.treasury.gov/files/eaglecash/kioskguide2.pdf
- **EZpay Users Guide and EZpay Smart Card Agreement**
  EZ foldernew.QXD (treasury.gov)
  https://www.fiscal.treasury.gov/files/ezpay/EZpay-user-guide-2014.pdf
- **EZpay Bluebird Point of Sale (POS) User Guide 1.3** Bluebird POS User Guide (treasury.gov)
  https://www.fiscal.treasury.gov/files/ezpay/bluebird-pos3.0.0-user-guide-for-ezpayv1.3.pdf
- **EZpay Bluebird POS Quick Start Guide** svc-bluebird-ct280-pointofsale-quick-start-guide-for-ezpay.pdf (treasury.gov)
  https://fiscal.treasury.gov/files/ezpay/svc-bluebird-ct280-pointofsale-quick-start-guide-for-ezpay.pdf
- **Performing a Sale on the EZpay Bluebird POS** performing-a-sale-on-the-ezpay-bluebird.pdf (treasury.gov)
  https://www.fiscal.treasury.gov/files/ezpay/performing-a-sale-on-the-ezpay-bluebird.pdf

B. References – List of Related Organizational Regulations/ Websites:

1. Department of Defense

- Forms, Directives, Instructions (defense.gov) - https://www.defense.gov/Resources/Forms-Directives-Instructions/

2. Fiscal Service

- Stored Value Card (treasury.gov) – https://www.fiscal.treasury.gov/stored-value-card/
- EagleCash (treasury.gov) - https://www.fiscal.treasury.gov/eaglecash
- EZpay (treasury.gov) – https://www.fiscal.treasury.gov/ezpay

3. Federal Reserve Bank of Kansas City

- SVC Portal – https://svcportal.fiscal.treasury.gov/

C. Forms

1. SVC Equipment-related Forms

These forms are located in the SVC Portal

- FRBKC Form 409 – HYP_File_Requestz_OCT-2019
- FRBKC Form 410 – Transfer of Hardware/Supplies
- FRBKC Form 411 – EZ and EC_Replacement_Hardware_Supply_Request
- FRBKC Form 412 – EC_New_Hardware_Request_OCT-2019
- FRBKC Form 418 – Mobile_Kiosk_Password_Reset_HYP_File_Request_OCT-2019

2. SVC Card Program Enrollment/Appointment/Disclosure Forms

- **FS Form 2887 Individual Enrollment** Navy Cash™Application for Enrollment and Authorization Agreement (treasury.gov)
  https://www.fiscal.treasury.gov/files/navycash/forms/FSForm2887.pdf
- **FS Form 2888 Accountable Official Enrollment** FSForm2888.pdf (treasury.gov)
  https://www.fiscal.treasury.gov/files/navycash /forms/FSForm2888.pdf
- **FS Form 5752 Authorization to Disclose Information Related to Stored Value Account** FSForm5752.pdf (treasury.gov)
  https://www.fiscal.treasury.gov/files/navycash/forms/FSForm5752.pdf
- **DD Form 577 Appointment/Termination Record-Authorized Signature**
  DD Form 577, Appointment/Termination Record - Authorized Signature, November 2014 (treasury.gov) https://www.fiscal.treasury.gov/files/navycash/forms/DDForm577.pdf

D. Acronym Listing

Acronym	Definition
AAFES	Army & Air Force Exchange Service
ABA	American Bankers Association
ACH	Automated Clearing House
ABA RTN	ABA Routing and Transit Number
AMPO	Army Military Pay Office
COPE	Custodian of Postal Effects
CPS	Card Processing Station
CSC	Customer Service Center
DA	Disbursing Agent
DFAC	Dining Facilities
DO	Disbursing Office
DDL	Daily Download Limit
DDO	Deputy Disbursing Officer
DoD	Department of Defense
ECAS	EagleCash Agent SVC Cards
FinCEN	Financial Crimes Enforcement Network
FMR	Financial Management Regulation
FO	Finance Office
FS	Fiscal Service
FRBKC	Federal Reserve Bank of Kansas City
HW	Hardware
ICF	Intelligence Contingency Funds
IMO	Information Management Office/Officer
IR	Incident Report
ISPP	Information Security Program Plan
IT	Information Technology
LAN	Local Area Network
LCR	Life Cycle Replacement
LRC	Logistical Readiness Centner
MP	Military Police
MPSA	Military Postal Service Agency

MWR	Morale, Welfare, and Recreation
NAVSUP	Naval Supply Systems Command
NEX	Navy Exchange
NSF	Non-Sufficient Funds
OCONUS	Outside of the Continental United States
OTCnet[SM]	Web-based successor application that integrates the functionality of Paper Check Conversion Over the Counter (PCC OTC) and Treasury General Account Deposit Reporting Network (TGAnet)
PC	Personal Computer
PCC	Paper Check Conversion
PII	Personally Identifiable Information
PIN	Personal Identification Number
PO	Post Office
POC	Point of Contact
POP	PIN on POS
POS	Point-of-Sale
PX	Post Exchange
RFC-KCI	Resources Fiscal Finance, Kansas City/Indianapolis
RIP/TOA	Relief in Place/Transfer of Authority
RTN	Return Tracking Number
S&A	Settlement and Accounting
SA&A	Security Assessment and Authorization
SAF/FMP	United States Air Force Deputy Assistant Secretary for Financial Operations
SOP	Standing Operating Procedures
SRP	Soldier Readiness Preparation
SSN	Social Security Number
SVC	Stored Value Card
SW	Software
TIN	Tax Identification Number
TR	Transaction Report
USAFMCOM	United States Army Financial Management Command