

VOLUME 5, CHAPTER 10: “SMART CARDS FOR FINANCIAL APPLICATIONS”**SUMMARY OF MAJOR CHANGES**

All changes are denoted by **blue font**.

Substantive revisions are denoted by an asterisk (*) symbol preceding the section, paragraph, table, or figure that includes the revision.

Unless otherwise noted, chapters referenced are contained in this volume.

Hyperlinks are denoted by **bold, italic, blue and underlined font**.

†The previous version dated March 2011 is archived.

PARAGRAPH	EXPLANATION OF CHANGE/REVISION	PURPOSE
All	†As part of the Under Secretary of Defense (Comptroller) Volume 5 Streamlining Initiative, this revision incorporated the archived version of Chapter 17 (March 2012). The content of the archived version of Chapter 10 (September 2011) was incorporated into the new Chapter 8 (June 2014).	Revision
Title	Changed the Chapter title to “Smart Cards for Financial Application.”	Revision
100102	Added new section called Purpose, incorporating paragraphs 100102 and 100103	Addition
100103	Added new section called Statutory Basis and renumbered the remaining chapter	Addition
100201	Added reference to new Treasury regulation	Revision
100204.A	Added Treasury suggestion of the designation of an alternate Smart Card Project Manager	Revision
100204.B	Added additional responsibility to maintain Agency network approvals	Revision
100205.A	Provided clarification for the appointment of Smart Card Accountable Officers	Revision
100205.B	Updated paragraph to include responsibility of delivering Personal Identification Numbers	Revision
100211	Added new paragraph on Theft, Fraud, Waste, and Abuse	Addition
100212	Updated verbiage on quarterly Smart Card verification, to include all programs, not just the US Debit Card	Revision
1007	Added new section on Direct Express	Addition
Figure 10-2	Removed DD Form 2887, Application For Department of Defense (DoD) Stored Value Card (SVC) Programs	Deletion

Table of Contents

VOLUME 5, CHAPTER 10: “SMART CARDS FOR FINANCIAL APPLICATIONS”	1
1001 GENERAL	4
100101. Overview	4
*100102. Purpose	4
*100103. Statutory Basis.....	5
1002 POLICY ON SMART CARD UTILIZATION	5
*100201. Overview	5
100202. Smart Card Program Approval.....	5
100203. Memorandum of Understanding (MOU)	6
*100204. Agency Smart Card Project Manager.....	7
*100205. Smart Card Accountable Officers	8
100206. Standard Operating Procedures (SOPs)	9
100207. Loss of Funds	9
100208. Smart Card Ordering	9
100209. Security and Storage.....	9
100210. Lost or Damaged Cards and Replacements.....	9
*100211. Theft, Fraud, Waste, and Abuse	9
*100212. Audit Requirements.....	10
1003 EZPAY STORED VALUE CARD.....	10
100301. Overview	10
100302. Card Issuance	11
100303. Activation and Accountability	11
100304. Residual Value on Expired/Cancelled Cards	11
1004 EAGLECASH STORED VALUE CARD.....	12
100401. Overview	12
100402. Card Issuance	12
100403. Activation.....	12
100404. Accountability	13
100405. Residual Value on Expired/Cancelled Cards	13
1005 NAVY CASH PROGRAM.....	13
100501. Overview	13
100502. Card Issuance	14
100503. Activation.....	15
100504. Accountability	15

Table of Contents (Continued)

100505. Residual Value on Expired/Cancelled Cards 15

1006 US DEBIT CARD PROGRAM..... 16

*1007 DIRECT EXPRESS 16

Figure 10-1. DoD Financial Smart Card Application (page 1 of 4)..... 17

CHAPTER 10

SMART CARDS FOR FINANCIAL APPLICATIONS

1001 GENERAL

100101. Overview

The Department of Defense (DoD) utilizes several Smart Card applications to conduct financial transactions in a number of settings. Smart Cards:

- A. Include stored value cards (SVC), debit cards, and combination cards (hybrids that contain both SVC and debit card features);
- B. Store or provide access to “electronic funds” and a more secure method of handling funds; and
- C. Alleviate the need to carry cash and provide electronic payment to vendors for items purchased or services rendered.

*100102. Purpose

This chapter provides:

- A. Guidance for requesting approval to begin a Smart Card pilot program or to move from pilot to full roll-out, except when provided under the General Services Administration (GSA) Smartpay Contract, and
- B. High-level disbursing guidance for SVCs, combination cards, and debit cards.
 - 1. SVCs
 - a. The basic trainee SVC program (known as EZpay) is used as an advance of pay to basic trainees of the United States (US) Army, Air Force, and Marine Corps.
 - b. The [card used for US deployed forces](#), known as EagleCash, is used for electronic financial transactions in overseas [contingency](#) locations.
 - 2. Combination Cards. The Navy/Marine Cash Card is used aboard naval vessels.
 - 3. Debit Cards. Debit cards [are](#) used as an alternate device for payments made by [DoD](#) agencies.

*100103. Statutory Basis

In accordance with Title 31 Code of Federal Regulations (CFR), [31 CFR Part 208](#), Electronic Funds Transfer (EFT) is mandatory within the DoD, unless a waiver has been granted. Per Treasury Financial Manual (TFM) [Volume I, Part 4a, Chapter 3000](#), SVCs and debit cards are available mechanisms for working towards compliance with the EFT requirement.

1002 POLICY ON SMART CARD UTILIZATION

*100201. Overview

The policy and guidance set forth in this chapter, is in accordance with the Department of Treasury (Treasury), TFM [Volume I, Part 4, Chapter 9000](#). Treasury guidance supersedes any conflicting information provided in this chapter. The Defense Finance and Accounting Service (DFAS) has been assigned management and oversight responsibility for the functional aspects and the use of financial Smart Cards within the DoD, except for GSA Smartpay products. Written approval from DFAS is required for all pilot and full roll-out Smart Card usage (e.g., stored value or debit) that employ either single purpose or multifunctional applications (combined financial/non-financial applications).

100202. Smart Card Program Approval

A. General. If a DoD agency seeks to establish a new Smart Card program, the agency must submit a request for approval to the Director, Strategy, Policy & Requirements, Defense Finance and Accounting Service, DFAS-ZPFA/IN, 8899 East 56th Street, Indianapolis, IN 46249-0500. Separate requests are required for each financial application. DFAS must coordinate requests for concurrence of approval, with the Accounting and Finance Policy Directorate, Office of the Under Secretary of Defense (Comptroller) (OUSD(C)) and the appropriate technical authorities, depending upon the card used in the program. Electronic submissions may be sent to DFAS.bean.zpf.mbx.treasuryinitiativesmailbox@mail.mil.

B. Program Magnitude. Requests for approval must indicate whether the program is a pilot effort or a full roll-out program.

1. Pilot Programs. Pilot programs are temporary and must be in operation for no less than 90 days and not to exceed 180 days. Pilots should be used to test card programs prior to full roll-out.

2. Full Roll-Out Programs. Full roll-out programs are non-temporary and must be in operation longer than 180 days. Full roll-out of a card program should follow a pilot.

C. Smart Card Application Package. Requests for approval must be submitted as an application package to DFAS. The application package must be completed before approval of any pilot or full roll-out of a card program. Include the following items in the application package:

1. Requesting Memorandum. The agency headquarters, or designee, should request approval of the pilot or full roll-out program via memorandum. It should be addressed to Strategy, Policy & Requirements, DFAS.
2. Application. All pilot and full roll-out programs are required to submit a completed DoD Financial Smart Card Application (Figure 10-1).
3. Concept of Operations (CONOPS). The CONOPS document should contain guidance on the use of the [Smart Card](#) program by the agency.
4. Coordination. The package must contain copies of coordination documentation, including the agency or component leadership's and servicing Disbursing Officer's (DO) endorsement of memoranda.
5. Agency Smart Card Project Manager Documentation. A copy of the letter designating the agency Smart Card project manager must be submitted with each package. See paragraph 100204 for information on project managers.
6. Analysis for Full Roll-Out. If the request is to move from a pilot [Smart Card](#) program to a full roll-out, include an analysis showing:
 - a. How the pilot program is an improvement over the pre-pilot environment,
 - b. Any savings realized from the pilot program, and
 - c. The results of relevant performance measures used during the pilot and proposed for the full roll-out (item 18 of Figure 10-1).

100203. Memorandum of Understanding (MOU)

Following OUSD(C) concurrence, an MOU must be entered into between the [Bureau of the Fiscal Service \(Fiscal Service\)](#), Treasury, and the agency implementing the program, prior to a new card program being implemented. The MOU describes the terms of the agency's Smart Card program and the respective responsibilities of the agency and [Fiscal Service](#) for operation of the program. In addition, the MOU specifies the type of program and Smart Card(s) being implemented by the agency, the agency's funding schedule, and the fees and costs to be paid by the agency and [Fiscal Service](#).

*100204. Agency Smart Card Project Manager

A. Designation. The agency must designate a Smart Card project manager, and an alternate, in writing before implementing a Smart Card program.

B. Responsibilities. The agency must specifically identify the tasks for which the Smart Card project manager is responsible. The Smart Card project manager must manage the Smart Card program and the activities described in this chapter, in accordance with the MOU between the Fiscal Service and the agency, the Smart Card standard operating procedures (SOPs) and other instructional documents, and program-specific policies and procedures developed by the agency in consultation with Fiscal Service. The specific duties of the project manager include:

1. Acts as the agency's liaison among Fiscal Service, the agency, and other interested stakeholders;
2. Provides full support for the Smart Card program within the agency;
3. Develops and obtains agency approval for the concept of operation, Smart Card Application, and other related plans for the implementation of the agency's Smart Card program;
4. Secures agency funding approvals necessary for the Smart Card program;
5. Coordinates the agency's implementation of the Smart Card program, to include obtaining and maintaining the Security Assessment and Authorization, Authority to Operate, or similar approval for the SVC program to access the Agency's computer networks so that the SVC can be deployed and operate as designed;
6. Oversees and obtains agency approvals for changes to the program;
7. Transfers sufficient funds to Treasury's financial or fiscal agent to ensure full funding for the agency's obligations with respect to outstanding Smart Cards;
8. Maintains accurate, up-to-date lists of accountable officers; and
9. Along with the agency's accountable officers, complies with other Smart Card program policies and procedures as described in the MOU, SOPs, and other Smart Card instructional documents.

*100205. Smart Card Accountable Officers

A. Designation. The agency must designate one or more Smart Card accountable officers. If the agency Smart Card accountable officer has been previously appointed as a DO, Deputy DO (DDO), or Disbursing Agent, and the responsibilities of the card program are covered by the current appointment, then no additional documentation is necessary for appointment. However, if these requirements are not met, then the agency must provide a Letter of Appointment, assigning an individual or individuals as the Smart Card accountable officer(s). The Letter of Appointment will list the individual's responsibilities. An additional letter will be required when the individual no longer serves as the Smart Card accountable officer. In addition to this documentation, the accountable officer(s) must fill out the Financial Management Service (FMS) Form 2888, Accountable Official Application for US Department of the Treasury Stored Value Card; when directed by the agency Smart Card project manager.

B. Responsibilities. The agency must specifically identify the tasks for which the Smart Card accountable officers are responsible. The agency should segregate the duties appropriately in accordance with the agency's policies and procedures. As applicable and appropriate, accountable officers are responsible for the duties and responsibilities of a certifying officer or a disbursing officer, depending upon the designation of the accountable officer, as set forth in Title 31, U.S.C., Sections 3322, 3325, and 3528, and other applicable laws. The Smart Card accountable officers must manage the Smart Card program and the activities described in this chapter, in accordance with the MOU between Fiscal Service and the agency, the Smart Card SOPs and other instructional documents, and program-specific policies and procedures developed by the agency in consultation with Fiscal Service. The specific duties of the accountable officers may include:

1. Issuing Smart Cards and Personal Identification Numbers (PINs) to cardholders while following all enrollment processes;
2. Accounting for outstanding Smart Cards and the funds associated with each Smart Card, to the extent the Smart Cards and funds are within the control of the agency;
3. Providing instructions to Treasury's financial or fiscal agent as to the proper allocation of funds among the Smart Cards that are issued, by account number and, where feasible, cardholder name;
4. Maintaining accurate, up-to-date inventories of Smart Card program hardware and equipment, including point-of-sale (POS) terminals, laptops, kiosks, Smart Cards, and other items associated with the Smart Card program that are delivered to agency locations;
5. Safeguarding Smart Cards as sensitive items, to the extent the Smart Cards are within the control of the agency (the agency is accountable for Smart Cards issued by the agency at issuance locations); and

6. Along with the agency's Smart Card project manager, comply with other Smart Card program policies and procedures as described in the MOU, SOPs, and other instructional documents.

100206. Standard Operating Procedures (SOPs)

This chapter contains higher level policy and disbursing accountability requirements for the use of various card programs that have been approved. DoD Agencies, responsible for programs listed within this chapter, are required to develop and maintain detailed SOPs that comply with all current applicable regulations, and cover all aspects of their card program for daily operations and/or contingencies.

100207. Loss of Funds

The DO is accountable for a physical loss of funds and for overage of Smart Card funds. Should a loss or overage occur, the DO or designee should follow the guidance prescribed in Chapter 6.

100208. Smart Card Ordering

Smart Cards are ordered through the applicable point of contact for the program (Fiscal Service or Fiscal Service's financial agent/fiscal agent) and delivered to the appropriate site. The point of contact and a designated agency representative(s) must establish procedures to determine card usage and a secure method of card delivery.

100209. Security and Storage

Smart Card stock must be treated like blank check stock. Storage and security requirements for blank check stock are prescribed in Chapter 3.

100210. Lost or Damaged Cards and Replacements

If a Smart Card is reported lost, damaged, or malfunctioning, follow procedures laid out in the applicable MOU and SOPs. For all stored value and combination cards reported lost, stolen, damaged, or malfunctioning, a locally produced list should be created and kept on hand for audit purposes. For the US Debit Card, contact Fiscal Service's financial agent.

*100211. Theft, Fraud, Waste, and Abuse

A. Agencies participating in a Smart Card program must:

1. Include a process for reporting and educating Smart Card cardholders on how to promptly report any loss, theft, or fraudulent or unauthorized use of Smart Cards, PINs, passwords, or other security breach or malfunction involving the Smart Card program to Treasury or Treasury's financial or fiscal agent, and to the Agency Smart Card Project Manager;

2. Aggressively investigate and prosecute (or assist in investigations, and prosecutions of) end-user theft, fraud, unauthorized use or improper use of the Smart Card service, that occur in agencies' areas of operation and assists in obtaining restitution for the party suffering the loss;

3. Ensure that appropriate anti-money laundering controls and procedures are in place, in order to document the flow of monies onto or off of a Smart Card; and

4. When a funds pool is used to fund an SVC, compensate the SVC funds pool for losses that result from theft, fraud, unauthorized or other improper use of SVC equipment or resources for which agencies are responsible, unless the funds pool has been reimbursed from other sources, or the Treasury determines that such compensation is unnecessary or does not serve the SVC program's best interests.

*100212. Audit Requirements

An initial inventory **must** be completed and recorded upon receipt of Smart Cards from the **Fiscal Service** or other designated representatives. After the **Smart Cards** are inventoried, a signed receipt **must** be provided to the issuing representative for **their** records. The DO or designee will complete an **SVC** inventory log when releasing **Smart Card** stock to authorized personnel and to monitor returns of all unused **Smart Cards**. The DO or designee **must** maintain a copy of the signed receipt for his or her records. At least once every calendar month, the DO or designee **must** inventory all Smart Cards secured in the vault. Any open container **must** be inventoried by individual count and by sequential serial numbers of the cards. All damaged containers, or those bearing evidence of having been tampered with, **must** be opened, and all cards **must** be individually counted and serial numbers verified. A detailed record of the inventory, to include total cards on hand and sequential serial numbers by card type, **must** be retained in the disbursing office. At least once during each calendar quarter, the agency's cash verification team **must** conduct a unannounced verification of **any Smart Card stock** (e.g. US Debit Cards, **EagleCash**, **EZPay**, etc.) to include cards received, issued, returned, and on hand. A copy of the inventory **must** be given to the agency's cash verification team as an attachment to their quarterly cash verification report.

1003 EZPAY STORED VALUE CARD

100301. Overview

The EZpay SVC program utilizes a Smart Card with an embedded computer chip, which is preloaded with a specific amount of funds (e.g., \$300, \$350, \$400), that provides an electronic payment method for advance of pay to trainees of the US Army, Air Force, and Marine Corps. The SVC is a substitute for coin and currency transactions and is issued to alleviate cash or check payments to trainees during training. The card is designed to provide basic trainees with access to their initial advance pay, a more secure method of money handling, and electronic payments to vendors for essential items needed during the first few weeks of training (e.g.,

haircuts, stationery, stamps, and toiletries). Personnel involved with administering the EZpay program are encouraged to access [Fiscal Service's EZpay website](#). This website provides an overview of EZpay and also includes items such as: getting started, common questions, acceptance sites, SVC facts, and the EZpay User's Guide.

100302. Card Issuance

The DO or designee **must** maintain a vault inventory and issuance log for each denomination (**monetary amount**) of EZpay SVC stock received. This log **must** be used to maintain an inventory of card stock on hand and to control the release of cards to the issuing section or individual. When EZpay SVCs are issued, the DO or designee **must** examine the log to ensure that all cards issued, and cards returned unused, if any, are accounted for and that cards are not removed without authority. Use a separate log for cards with fixed monetary amounts. Do not mix card values on the same sheet with other card values. The SVC inventory log **must** contain the date of inventory, beginning card serial number, ending card serial number, number of cards returned, number of cards issued for the day, number of cards remaining in inventory, and the signature of the DO or designee.

100303. Activation and Accountability

Detailed procedures for activation of EZpay SVCs **must** be included in the agency's SOP for issuance. Once an EZpay SVC is activated, the DO or designated representative **must** ensure that each card number is indicated on the payroll document for tracking purposes and ensure the amount is reflected as an increase in the DO's accountability for that day's business. A payment in an amount equal to the total value of all EZpay SVCs activated that day will be forwarded to the Treasury's Fiscal Agent, which is the financial institution making restitution to the vendors for card usage. The payment will be in the form of an EFT. The fiscal agent will complete the required settlement action with vendors who accept the EZpay SVC. The total dollar value of the EZpay SVCs activated for that day, with the exception of replacement card(s) issued, will always match the total of the daily payroll document.

100304. Residual Value on Expired/Cancelled Cards

All personnel should cash out their EZpay SVC prior to departure from recruit training. If a trainee does not cash out, the Treasury fiscal agent **must** return the residual value remaining on the EZpay SVC to the DO or designee. The fiscal agent will not return any remaining balances until the EZpay SVCs expire. The DO or designee **must** collect any remaining balance into the correct military pay appropriation and provide the data to the military pay entitlement area for credit to the cardholder's military pay account. If systematic return is not possible, the agency and [Fiscal Service](#) **must** initiate good faith efforts to locate and return residual funds to the authorized EZpay cardholder. Should systematic or good faith return not be possible, residual funds greater than 1 year old, and less than \$25, are transferred to the Treasury [general fund receipt account **1060, Forfeitures of Unclaimed Money and Property](#), to be claimed with

supporting documentation by contacting [Fiscal Service](#). For amounts over \$25, credit 20X6133, Payment of Unclaimed Moneys. If the number of residuals received is significant, a review [must](#) be conducted by the military component to determine if the value of funds issued to recruits on the EZpay SVCs is in excess of the amount actually needed for the first few weeks of recruit training.

1004 EAGLECASH STORED VALUE CARD

100401. Overview

The EagleCash SVC is a re-loadable plastic card embedded with a computer chip that stores “electronic funds” in its memory. The card is issued to deployed service members, DoD civilians, and contractors. The card is used as a substitute for coins and currency transactions at concessions and for services at military installations overseas [during contingency operations](#) (e.g., barber and beauty shops, food court, post office, and Base Exchange). The card can be reloaded and continually used throughout the tour of duty. The cards are issued by a Finance Office (inside or outside the continental US) and may be funded through a [local](#) pay, cash, personal check, or through the EagleCash Kiosk. For more information visit [Fiscal Service’s EagleCash](#) website. This website provides an overview of EagleCash and also includes items such as: getting started, common questions, acceptance sites, SVC facts, the EagleCash User’s Guide, and the Kiosk User’s Guide.

100402. [Card](#) Issuance

The DO or designee will issue all cards used in this program. EagleCash cards with a zero dollar value may be issued to individuals who are authorized to receive check-cashing services as prescribed in Chapter 4. The name of the individual, appropriate identification number, length of deployment, and bank account information are all collected during the issuance process. EagleCash cards can be issued either at the deployed location or in advance of deployment by the Finance Office.

100403. Activation

When an EagleCash card is issued, it may be loaded with funds drawn either by personal check, cash, or [local](#) pay. Additionally, a self-service card-processing device called the EagleCash Kiosk may be deployed in the field for the purpose of loading, [unloading, and transferring](#) funds to the EagleCash card. Before a cardholder uses a kiosk, he or she is required to complete the [FMS Form 2887, Application Form for US Department of the Treasury Stored Value Card Program](#). Completion of the [FMS 2887](#) gives the Treasury’s fiscal agent access to move money from the cardholder’s financial institution to the EagleCash card. Bank information (bank routing number, account number and type of account) is captured electronically or manually and embedded in the computer chip, and a PIN is assigned at the chip level for use

with the kiosk, or at a Finance Office. The completed and signed FMS 2887 must be forwarded to the Treasury's designated fiscal agent who is authorized to initiate debit and credit entries to the individual's financial institution. The FMS 2887 will allow the cardholder to transfer funds between his or her financial institution and the EagleCash account. The DO must retain a copy of all enrollment forms completed.

100404. Accountability

The accounting for entries of EagleCash must be recorded on the appropriate lines of the [DD Form 2657](#), Daily Statement of Accountability. On each business day, using the EagleCash laptop, DOs, DDOs, Finance Officers or their designees collect all new account transactions, create a compressed or "zipped" file, and email the file to the EagleCash Customer Service Center at eagle@bos.frb.org or deposit it at another agency designated location.

100405. Residual Value on Expired/Cancelled Cards

If a cardholder departs the area before cashing out their EagleCash card, the Finance Office must obtain the cardholder's direct deposit information from the FMS 2887. If the Finance Office does not return the residual value, the Fiscal Agent must deposit the funds to the cardholder's account on file after the card expires. A credit must be forwarded to the cardholder's bank account via an Automated Clearing House credit using information provided by the cardholder when signing up for EagleCash. If systematic return is not possible, the agency and Fiscal Service must initiate good faith efforts to locate and return residual funds to the authorized EagleCash cardholder. Should systematic or good faith return not be possible, residual funds greater than 1 year old, and less than \$25, are transferred to the Treasury general fund receipt account **1060, to be claimed with supporting documentation by contacting Fiscal Service. For amounts over \$25, credit 20X6133.

1005 NAVY CASH PROGRAM

100501. Overview

The Navy Cash program was developed in partnership with the US Navy and Marine Corps and the Treasury. The program is administered by the Fiscal Service, with assistance of Fiscal Service's designated financial agent. All personnel assigned to a ship are eligible to receive a Navy Cash card. Visitors may be issued a Navy Cash Visitor card while aboard the ship. The Marine Cash card is issued when Marines are assigned to or deployed aboard Navy ships and only when Marines participate in bulk enrollment, otherwise they are given a Navy Cash instant issue card.

A. Functionality. The Navy Cash and Marine Cash cards are combination cards. The card combines a chip-based electronic purse (stored-value function) with the traditional magnetic strip (debit card and automated teller machine (ATM) function). The electronic purse replaces currency aboard ship. The magnetic strip and branded debit features afford users access to funds in their Navy/Marine Cash accounts world-wide via ATMs and POS devices at merchants who accept debit cards. Kiosks aboard ships provide 24-hour-a-day, seven-

day-a-week access to Navy/Marine Cash accounts. The [kiosks](#) also provide access to accounts at financial institutions ashore and the ability to move money electronically to and from Navy/Marine Cash accounts and those financial institution accounts.

B. Split Pay. Sailors and Marines who elect the Split Pay Option may designate a portion of their pay to be sent directly to their Navy/Marine Cash accounts each payday.

C. Types of Navy Cash Cards

1. Instant Issue. The Navy Cash Instant Issue Cards provide access to all Navy Cash capabilities (i.e., the usage of the chip-based electronic purse and the magnetic strip). [These cards are typically used for new enrollees or as a replacement for lost, stolen, or damaged cards.](#)

2. Embossed Permanent. The Embossed Permanent Navy Cash cards also provide access to all the Navy Cash capabilities. These cards are personalized and embossed with the account holder's name. Generally, these cards are only issued as a part of bulk enrollment when Navy Cash is initially implemented on a ship.

3. Visitor Navy Cash Card. These cards have chip-only access with the intention only to make purchases on the ship. The cards do not have a Navy Cash account associated with them and do not have a magnetic strip. Also, Visitor Navy Cash cards can only have funds loaded by the disbursing office.

D. Additional Information. Personnel involved with the administering of the Navy Cash program are encouraged to access [Fiscal Service's Navy Cash/Marine Cash](#) website. This website provides an overview of Navy/Marine Cash and includes items such as: Cardholder Basics, Functional Training, common questions, SVC facts, and the Navy Cash SOP.

100502. [Card Issuance](#)

The DO or designee may issue the Navy Cash card to newly enrolled account holders from the stock of "instant issue" Navy Cash cards. In order to obtain a fully functioning card, a FMS 2887 must be completed and signed before the card will be issued. The DO or designated representative [must](#) annotate appropriate information on the Bulk Card Log when the Navy Cash card is removed from the safe. The DO or designated representative [must](#) also annotate appropriate information on the Bulk Card Log when he or she issues the card to an individual. If the Bulk Card Log is produced locally, then it [must](#) contain the date the cards are issued, the card numbers, name and last 4 digits of each cardholder's social security number, signature of the cardholder, and the issuing DO or designee's name. Each operator using the Navy Cash system (e.g., in the ship's store, post office, chief's mess, wardroom, disbursing office or Morale Welfare and Recreation facilities) must be identified by a four-digit operator Identification number that is unique within the Navy Cash system on each ship.

100503. Activation

When a Navy/Marine Cash card is issued, it may be loaded with funds drawn either by personal check, cash, split pay option, or transfer of funds from the card holder's financial institution. Additionally, a self-service kiosk aboard the ship may be used for the purpose of loading and unloading funds to the card. Cardholders are required to complete the FMS 2887. In addition to serving as the application form for a fully functioning card, completion of the FMS 2887 gives the Treasury's financial agent access to move money from the cardholder's financial institution to the Navy/Marine Cash card. Bank information (bank routing number, account number, and type of account) is stored on the Navy Cash server on the ship. A PIN is associated with both the chip and the magnetic strip. On the ship, the PIN is required for use with the kiosk and for all purchases with the exception of vending items. Off the ship, the PIN is required for ATM withdrawals and for debit purchases at merchants who accept debit card. The completed and signed FMS 2887 must be forwarded to the Treasury's designated financial agent who is authorized to initiate debit and credit entries to the individual's financial institution. The FMS 2887 will allow the cardholder to transfer funds between his or her financial institution and the Navy/Marine Cash account. The DO must retain a copy of all enrollment forms completed.

100504. Accountability

The DO controls access to the various functions within the Navy/Marine Cash System. Individual operators are assigned to one of six user groups that represent six levels of access rights: DO/DDO, Marine DO/DDO, Agent Cashier, Duty Person, Refunds, and Duty Automatic Data Processing. The access rights for each user group are initially set to default settings. The issues associated with accountability for cash management of public funds are addressed in Chapter 3. Navy/Marine Cash transactions, such as increasing amounts in either the chip or strip accounts, with funds drawn either by personal check or cash, or giving cash for amounts drawn off a loaded card, occur at the disbursing office. All funds associated with these transactions are part of the DO's accountability. At the end of month reporting, the DO will be responsible for creating an electronic Deposit Ticket or Debit Voucher, and forwarding it to the Treasury financial agent. The copy of the Deposit Ticket or Debit Voucher must be included with the appropriate financial documents for retention.

100505. Residual Value on Expired/Cancelled Cards

Prior to transferring from the ship or being separated from active duty, a cardholder may transfer any remaining value to their home financial institution by using the Cashless ATM or request a cash-out from the DO paid in cash or by US Treasury check. All Visitor Navy Cash cards should be cashed out and returned to the DO before a visitor departs ship since they are reusable. If the cardholder is absent or in a non-active status, then the DO must contact the financial agent and request that any residual value in the Navy/Marine Cash account be transferred to the home financial institution of the cardholder. If systematic return is not

possible, the agency and [Fiscal Service](#) initiate good faith efforts to locate and return residual funds to the authorized Navy/Marine Cash cardholder. Should systematic or good faith return not be possible, residual funds greater than 1 year old, and less than \$25, are transferred to the Treasury [general](#) fund receipt account **1060, to be claimed with supporting documentation by contacting [Fiscal Service](#). For amounts over \$25, credit 20X6133.

1006 US DEBIT CARD PROGRAM

The US Debit Card (USDC) program is administered by the [Fiscal Service](#), with the assistance of [Fiscal Service](#)'s designated financial agent. The USDC provides Federal agencies with the ability to deliver Federal payments through debit cards, as an alternative to checks, drafts, cash, and other non-electronic mechanisms. The USDC is a flexible payment mechanism that can be used to deliver miscellaneous or nonrecurring payments to individuals, or to allow Government employees or military personnel access to cash in their official duties. Examples of the types of Federal payments that can be delivered via a debit card include benefit, payroll, stipend, employee awards, and survey incentives. After implementation of the USDC program, the Agency disburses payments to a card account and the funds are accessed via a debit card issued to a Federal payment recipient. The cardholder may use the USDC to access authorized Federal payments at ATMs, POS terminals, bank tellers, and other locations where access is permitted. If the USDC is MasterCard- or Visa-branded, the cardholder may use the USDC anywhere the applicable brand is accepted. For more information, visit [Fiscal Service](#)'s [US Debit Card](#) website and the [US Debit Card Program](#) website.

*1007 DIRECT EXPRESS

Direct Express Debit MasterCard is a prepaid debit card offered to Federal benefit recipients who wish to receive their benefits electronically. The debit card offers the convenience and security of using electronic transactions to spend and access money rather than using cash for purchases. Recipients do not need to have a bank account to sign up for the card. The Direct Express Debit MasterCard is available only to individual Federal benefit recipients. For more information on the [Direct Express](#) Debit MasterCard, see the website.

Figure 10-1. DoD Financial Smart Card Application (page 1 of 4)

DEPARTMENT OF DEFENSE (DoD) FINANCIAL SMART CARD APPLICATION		
SECTION I - GENERAL INFORMATION		
1. Program Title:		
2. Program Description:		
3. Sponsoring Organization:		
4a. Name of Smart Card Project Manager (Primary or Alternate):		b. Telephone:
c. E-Mail:		d. Fax:
5. Program Magnitude (Check one):	Pilot []	Full Roll-out []
6. Supporting Disbursing Station Symbol Number (DSSN):		
7. Implementing Location(s):		
8. Duration and Start Date Requested:		
9. Financial Applications(s) (e.g., Debit, Stored Value, Other):		
10. Purpose/Objective (Include improvements/changes to official DoD functions (e.g., disbursing and paying, if any)):		
11a. Anticipated Future Deployment:	Yes []	No []
b. If yes, explain:		

Figure 10-1. DoD Financial Smart Card Application (page 2 of 4)

12. Alternatives Considered (e.g., EFT, Travel Card):	
13. Other Non-Financial Applications on Card:	
14a. Total Population Served:	b. Number of Cards:
c. Projected Annual Dollar Amount Deposited on Cards (US Debit Card Program Only):	
15. Other Known Location(s)/Installation(s) Where Card Could be Used:	
16. Projected Savings and Budget Impact:	
17. Anticipated Benefits:	
18. Performance Measures of Pilot:	
19. Barriers to Implementation:	

Figure 10-1. DoD Financial Smart Card Application (page 3 of 4)

SECTION II - CARD/VENDOR INFORMATION
20. Issuing Financial Institution Provider/Sponsor and POC:
21. Type of Card Technology/Platform and Size:
22. How Funds Will be Loaded on Cards:
23. Source of Funds to be Loaded on Cards:
24. Security and Privacy Factors:
25. Accountability Controls (including Funds Pool), Auditable Features, and Collateralization/Warranty Issues:
26. Frequency of In Progress Reviews (e.g., monthly, quarterly):
27. Authorization/Dispute Processes:

Figure 10-1. DoD Financial Smart Card Application (page 4 of 4)

28. Association Brand Affiliation (e.g., VISA/MASTERCARD):
29. Network Used, if any (Cirrus, Plus):
30. On-base Merchants Where Card is Accepted:
31. Cost of Cards:
32. Type and Number of Equipment:
33. Cost of Equipment: