Appendix T
Guidelines for Fraud Risks and Liabilities

1. Cardholders. A Navy Cash cardholder, either an individual or a merchant, who suspects there has been unauthorized activity on their Navy Cash card or account, should stop using the card and report the incident to the Disbursing Office and/or the Navy Cash Customer Service Center (CSC) (1-866-3NAVY CASH *(1-866-362-8922)*). Specific guidelines for reporting and handling problems with suspected fraudulent activity depend on the type of transaction involved. Information about cardholder rights, responsibilities, and liabilities can be found in the *Navy Cash Card and Navy Cash Visitor Card Cardholder Agreement* at Appendix U.

Table T-1 groups problems with Navy Cash transactions in four categories: debit transactions on shore, funds transfers at the Navy Cash Kiosk, closed-loop transactions, and home bank or credit union account transfers. The actions a cardholder should take for suspected fraudulent activity with each category of transactions are discussed in turn. Table T-2 summarizes these cardholder actions.

PROBLEMS WITH DEBIT TRANSACTIONS ON SHORE	PROBLEMS WITH FUNDS TRANSFERS AT KIOSK
1. ATM withdrawal – PIN required 2. PIN-based purchase – PIN required 3. Signature-based purchase – PIN not required	4. Open loop to home account – PIN required 5. Open to closed loop – PIN required 6. Closed to open loop – PIN required 7. Closed loop to home account – PIN required
PROBLEMS WITH CLOSED-LOOP TRANSACTIONS	**PROBLEMS WITH HOME ACCOUNT TRANSFERS**
8. POS purchase – PIN required 9. Vending purchase – PIN not required 10. Closed-loop-to-closed-loop transfer – PIN required	11. Home account to closed loop – PIN required 12. Home account to open loop – PIN required

Table T-1. Summary of Navy Cash Transactions

a. Cardholder Actions

(1) Problems with Debit Transactions on Shore. Withdrawals at Automated Teller Machines (ATMs) ashore and both PIN-based and signature-base purchases at stores, restaurants, gas stations, and other retail locations ashore are transacted as Mastercard® debit transactions from the Mastercard debit open-loop account.

(a) Actions. A cardholder who suspects someone made, or may make, an unauthorized ATM withdrawal or a PIN-based or signature-based purchase ashore using their Navy Cash card open-loop account without permission must notify the Treasury Agent AT ONCE, either by requesting their Disbursing Office contact the CSC immediately or by calling the CSC directly. The CSC will open a case in the ticketing system and forward the case to the Treasury Agent's transactions processor. Similarly, a cardholder who believes their Navy Cash card has been lost or stolen must notify the Treasury Agent AT ONCE, either by requesting their Disbursing Office contact the CSC immediately or by calling the CSC directly so they can assign

a case tracking number. In both cases, a telephone call is the preferred way to notify the CSC, but email notification is also acceptable.

If the Disbursing Office or cardholder elects to notify the CSC via email, they must restrict the Personally Identifiable Information (PII) they provide in the email. They should simply state either that they believe the card has been lost or stolen or that someone has transferred, or may transfer, money from the account without permission. They should include only the name, email address, and last four digits of the SSN to help the CSC in identifying the correct Navy Cash cardholder account and in responding to their email. They should also "cc" the Disbursing Officer on the email they send to the CSC. A cardholder's full SSN, Mastercard number, or PIN should never be included in an email to the CSC.

Phone: 1 866 3NAVY CASH *(also printed on the back of the Navy Cash card)*
1 (866) 362-8922

email: navycash@frb.org

Fax: 1 (813) 533-5711

(b) Dispute Form. To dispute a fraudulent or erroneous transaction, an individual must fill out, sign, and date a dispute form. There are two separate dispute forms, the Fraud Transaction Dispute Form and the Non-Fraud Transaction Dispute Form. The Disbursing Officer can provide a cardholder the appropriate form. The form must then be faxed or mailed to Treasury Agent's customer service facility in Tampa, Florida. Copies of the two dispute forms are included at Appendix I.

Address: FRB-TCC
Attention: Disputes
3913 Riga Blvd
Tampa, FL 33619

Fax: 1 (813) 533-5711

(2) Problems with Funds Transfers at the Kiosk on the Ship. Funds transfer requests at the kiosk from the open-loop account to a home bank or credit union account or to the closed-loop account on the Navy Cash card or from the closed loop to the open loop or from the closed loop to a home bank or credit union account also involve the Navy Cash card open-loop or closed-loop accounts and require a PIN.

(a) Actions. A cardholder who suspects someone transferred, or may transfer, money from his/her Navy Cash card open-loop or closed-loop accounts without permission must notify the Customer Service Center (CSC) AT ONCE, either by requesting their Disbursing Office contact the CSC immediately or by calling the CSC directly so they can assign a open a case in the ticketing system. A telephone call is the preferred way to notify the CSC, but email notification is also acceptable (see paragraph 1.a.(1) above).

(3) Problems with Closed-Loop Account Transactions on the Ship. The closed loop on the Navy Cash card replaces cash for purchases on the ship. Funds in the closed-loop account are considered cash. Any loss of funds is similar to the loss of cash and may not be recoverable.

(a) Actions. A cardholder who suspects fraudulent activity on closed-loop purchases or closed-loop-to-closed-loop transfers should notify the Disbursing Office and the ship's Master at Arms immediately. Any loss of funds would need to be pursued via Navy investigative and judicial processes. The Commanding Officer (CO) may appoint an investigating officer/board to conduct a formal investigation or request a criminal investigation if one is warranted. If it becomes necessary to request account information, transaction history,

or any Personally Identifiable Information (PII) concerning a cardholder's Navy Cash account to support a formal or criminal investigation, refer to the guidance below in paragraph 4, Requests for Cardholder Information.

(4) Home Account Transfers at the Kiosk on the Ship. Funds transfer requests at the kiosk from the home bank or credit union account to the closed or the open loop are debited from the cardholder's bank or credit union account.

(a) Actions. Cardholders who suspect fraudulent activity on home account transfer requests should notify Disbursing and contact their bank or credit union directly to dispute any unauthorized transactions. For all calls received by the CSC from the cardholder or by the Navy Cash Central Support Unit (CSU) from Disbursing regarding disputes for these types of transactions, the caller will be referred to the individual cardholder's bank or credit union for resolution.

Transaction Types	Cardholder Actions
PROBLEMS WITH DEBIT TRANSACTIONS ON SHORE	
1. ATM withdrawal 2. PIN-based purchase 3. Signature-based purchase	• Call CSC immediately so a case can be opened 1-866-3NAVY CASH *(1-866-362-8922)* *(also printed on back of Navy Cash card).* • Fill out, sign, and date appropriate dispute form *(available at Disbursing)* and fax or mail to: Address: FRB-TCC Attention: Disputes 3913 Riga Blvd Tampa, FL 33619 Fax: 1-813-533-5711
PROBLEMS WITH FUNDS TRANSFERS AT KIOSK ON SHIP	
4. Open loop to home account 5. Open loop to closed loop 6. Closed loop to open loop 7. Closed loop to home account	• Call CSC immediately so a case can be opened 1-866-3NAVY CASH *(1-866-362-8922).*
PROBLEMS WITH CLOSED-LOOP TRANSACTIONS ON SHIP	
8. POS purchase 9. Vending purchase 10. Closed loop-to-closed loop transfer	• Notify Master at Arms and Disbursing immediately. • Funds in closed-loop account are considered cash and may not be recoverable if lost, so disputes must be pursued via Navy investigative/judicial processes.
PROBLEMS WITH HOME ACCOUNT TRANSFERS AT KIOSK ON SHIP	
11. Home account to closed loop 12. Home account to open loop	• Contact bank or credit union directly to dispute any unauthorized transactions.

Table T-2. Summary of Cardholder Actions

b. Safeguard Navy Cash Card and PIN. Remember, a cardholder is responsible for all debits they authorize using the card. Therefore, a cardholder must take precautions to safeguard the card and PIN at all times. A cardholder must not give his/her card or PIN, or make the card or PIN available, to any other person. If a cardholder permits other persons to use his/her card, the cardholder is responsible for any transactions they authorize from the cardholder's closed-loop or open-loop account.

2. Lost or Damaged POS or CAD

a. The Point Of Sale (POS) and Card Access Device (CAD) are used to process closed-loop purchase transactions at retail locations and vending machines on the ship. Any loss of funds is similar to the loss of cash and may not be recoverable if lost. In each instance of loss of funds due to a damaged or lost device, the liability will be determined on a case basis by the Fiscal Service and NAVSUP.

b. Merchant Actions. The POS and CAD devices can be used to store the value of sales transactions and should be protected like a cash box, particularly when the POS is operated in the off-line mode. When being transported off the ship or over water, these devices should be carried in a waterproof container equipped with a flotation device (see paragraph 8.7, Collections from Portable Point of Sale Devices). In the unlikely event that a POS is lost, damaged, or destroyed before the sales transaction data recorded in it are downloaded to the server, the CSU may be able to reconstruct the sales transactions from copies of the electronic records or manual logs of sales receipts kept by each merchant in accordance with this SOP.

(1) The Navy Cash closed-loop balance is essentially maintained in two places, physically on the chip and electronically in the database ashore. If sales transaction are not captured on the Navy Cash server on the ship, e.g., the POS is lost overboard before the transactions are downloaded to the server, then no transactions can be posted to the shore database, and the Navy Cash database ashore has no way of knowing the value to transfer to that particular merchant's account or the correct closed-loop balances on cardholders' cards. The balance on the closed loop on the card (the correct value) will be different from the closed-loop balance that is maintained in the shore database.

(2) The information required to reconstruct the sales transactions would need to be provided by whoever collected the transactions. It could come from the ROM reports, if it was the Ship's Store POS that was lost or damaged, or from a sales receipts log or copies of receipts given to customers, e.g., in the Wardroom, Chiefs Mess, or MWR. The amounts that were deducted from cardholders' cards and the customers' names or card numbers would be provided to the CSU. The CSU would then adjust each cardholder's closed-loop balance in the shore database. This should synchronize the closed-loop balance on the shore with the closed-loop balance on the cardholders' Navy Cash cards and enable the payment to the merchant account. The accuracy will only be as good as the information provided to the CSU.

3. Disbursing Office. If unauthorized activity on a Navy Cash card or account is suspected in the Disbursing Office, the guidelines described above for cardholders for debit transactions on shore, funds transfers at the kiosk, closed-loop transactions, and home bank or credit union account transfers apply.

a. However, Navy Cash also involves public money. Under Federal Law, 31 U.S.C. 3302, public money must be held either in the Treasury, by a Treasury-designated Financial Agent, or by a disbursing official. The Navy Cash funds pool holds a pool of funds that backs the electronic stored value that has been issued. The money in this pool falls into one of two categories. The first represents stored value which has been received by the Navy through the Ship's Store, vending machines, other retail operations, and Food Service. These funds constitute

receipts of the United States. The second represents stored value which "belongs" to individual Sailors. This money, while belonging to the Sailors, is under the control of the Government. Both categories of funds are public money.

b. Article 0814, U.S. Navy Regulations (1990), requires COs to recommend or convene an investigation under the provisions of the Manual of the Judge Advocate General (JAGMAN) into the circumstances of all losses or excesses of public funds or property in the custody of persons under their command, unless properly excused by higher authority.

c. According to the Department of Defense Financial Management Regulation (DoD FMR), Volume 5, Chapter 6, Irregularities in Disbursing Officer Accounts, any loss of funds where there is evidence of fraud within the Disbursing Office is considered a major loss, regardless of dollar amount. Any major loss requires a written report from the Disbursing Officer to the CO within 24 hours, who must in turn submit a written report through the chain of command within 24 hours via email or by mail to the Relief of Liability Section, Disbursing/ Debt Management Policy Division, Defense Finance and Accounting Service Indianapolis (DFAS-NPD/IN). The CO must appoint an investigating officer/board to conduct a formal investigation (the type of loss determines the type of investigation required) and request a criminal investigation if one is warranted. Responsibilities and procedures are detailed in DoD FMR Volume 5, Chapter 6.

d. In accordance with the JAGMAN, section 0249, Loss or Excess of Government Funds or Property, a consultation with an appropriate assist team and a prompt audit to verify the existence and amount of a loss of funds should normally precede the decision to convene a JAGMAN investigation. Criminal law enforcement investigations are required if there is any indication that the loss of funds was caused by fraud, embezzlement, theft, or other criminal act. In accordance with section 0201 of the JAGMAN, any such investigation should be coordinated with the Naval Criminal Investigative Service (NCIS).

4. Restitution. A court martial has no power to adjudge civil remedies. For example, a court martial may not adjudge the payment of damages, collect private debts, order the return of property, or order a criminal forfeiture of seized property.

a. When the U.S. Government, e.g., the Treasury's Navy Cash funds pool (see paragraph 2.a), has suffered any loss of money through unlawful acts, e.g., larceny, fraud, etc., for which persons, other than accountable officers as defined in DoD FMR Volume 5, Chapter 2, section 0203, have been convicted by court-martial or competent authority has determined that the loss occurred through fraud, forgery, or other unlawful acts, the amount of such loss constitutes an indebtedness to the U.S. Government. That indebtedness will be set off against the final pay and allowances due such persons at the time of dismissal, discharge, or release from active duty, if necessary without the member's consent, to make the Treasury's Navy Cash funds pool whole. Immediate recovery action against current pay may be instituted without the member's consent if such recovery is authorized by statute (see DoD FMR Volume 7A, Chapter 50) or on the basis of a voluntary offer from the member, i.e., with the member's consent, to make restitution of all or part of any indebtedness to the Government to make the Treasury's Navy Cash funds pool whole. The voluntary offer constitutes assumption of pecuniary responsibility for the loss and, as such, is sufficient to authorize checkage of current pay. (See JAGMAN, section 0167, Setoff of Indebtedness of a Person Against Pay.)

b. For accountable individuals, the ideal method for resolving a loss of funds is recovery from the beneficiary of the loss, e.g., recovery of missing cash from the finder, or, in cases where the accountable individual is denied relief of liability, collection from the accountable individual (see DoD FMR Volume 7A, Chapter 50) to make the Treasury's Navy Cash funds pool whole.

When losses cannot be recovered (including those instances where relief of liability has been denied and recoupment cannot be made from the accountable individual) or relief of liability is granted to the accountable individual, appropriated funds shall be made available to remove the deficiency from the Disbursing Officer's Statement of Accountability, SF 1219, i.e., the Navy shall identify the appropriation and funding necessary to resolve the loss (see DoD FMR Volume 5, Chapter 6) and to make the Treasury's Navy Cash funds pool whole.

c. When an individual cardholder has suffered any loss of money, Article 139, Uniform Code of Military Justice (UCMJ), can be a valuable tool for COs (see JAGMAN, Chapter IV, Article 139 Claims—Redress of Damage to Property). Article 139 provides an opportunity to force the wrongdoer to compensate victims for property damage or destruction. A wrongful taking is essentially theft. Claims for property that was taken through larceny, forgery, embezzlement, misappropriation, fraud, or similar theft offenses are normally payable. Command emphasis is required to ensure these investigations are completed quickly. Article 139 claims operate independently of any criminal action, and should not be delayed pending the outcome of adverse criminal or administrative initiatives. The claim must be submitted to the CO within 90 days of the incident. However, the CO can extend this time period if there is good reason for the delay. In addition, since respondents are often pending separation, it is crucial that Article 139 claims be filed and processed as quickly as possible to ensure valid claims are paid before the respondent is separated and no longer subject to military pay withholding (see DoD FMR Volume 7A, Chapter 50). Once the offender is no longer receiving military pay, the claimant may have no effective remedy for his loss.

5. Requests for Cardholder Information.

a. Navy Cash Account Statements. Individual Navy Cash cardholders do not need to submit a written request to obtain their own account information. Cardholder can access their account information on the Navy Cash Cardholder Website at any time (www.navycash.com). To log in to the website, cardholders need a username and password. The first time cardholders access the website, they use their 16-digit Mastercard® card number and PIN. They are then asked to set up a username and password and set up answers to two security questions. Once a cardholder has logged in to the website, they can view account information, list both ship and shore transactions, and print an account statement for the current month and the last six months.

b. Requested by Cardholder or Individual with a Current Power of Attorney. If a Navy Cash cardholder, or an individual who provides the Treasury Agent with an appropriate and current power of attorney form, submits a request for account information, transaction history, or any PII concerning her/his own Navy Cash account, the Treasury Agent may provide such information. This information may NOT be provided to anyone other than the cardholder, or an individual who provides the Treasury Agent with an appropriate and current power of attorney form, without prior written approval from the U.S. Treasury. To authorize disclosure of account information, transaction history, or any PII concerning his/her own Navy Cash account information, e.g., to a military or civilian law enforcement agency, a cardholder, or an individual who provides a current power of attorney form, must fill out, sign, and date an FS Form 5752, Authorization to Disclose Information Related to Stored Value Account (see enclosure (1)).

c. Requested by Other Than Cardholder Without a Subpoena.

(1) If someone other than the Navy Cash cardholder submits a request for account information, transaction history, or any PII concerning Navy Cash accounts, e.g. NAVSUP, NCIS investigators, other state or police agencies, the Treasury Agent may NOT provide such information. This information may NOT be provided to anyone other than the cardholder without prior written approval from the U.S. Treasury. When approval is received, the Treasury Agent

will provide such information to the U.S. Treasury or an approved agent of the Treasury for further distribution.

(2) The U.S. Treasury may grant release of account information, transaction history, or other PII concerning Navy Cash accounts to DoD law enforcement agencies for a civil or criminal law enforcement activity, if the activity is authorized by law and if requested in writing by the head of the agency specifying the particular information desired and the law enforcement activity for which the information is sought.

(3) In a single exception to this procedure, the U.S. Treasury has granted approval for the Treasury Agents to provide account information, transaction history, or PII to a Disbursing Officer who is acting as an agent of the U.S. Treasury in collecting and clearing negative balances. This approval has been granted under exemption (b)(1) of the Privacy Act, and that information can be provided routinely without written approval from the U.S. Treasury.

d. Requested by a Subpoena. If account information, transaction history, or any PII concerning a Navy Cash account is requested by a valid subpoena, such information may only be provided after the Treasury Agent receives confirmation of the validity of the subpoena from internal legal counsel. Upon confirmation of the validity of the subpoena, The Treasury Agent will notify the U.S. Treasury of the information requested in the subpoena.

FOR OFFICE USE ONLY: Cardholder Name	Cardholder No.

FS FORM 5752
Department of the Treasury
Bureau of the Fiscal Service

OMB No. 1530-0013

AUTHORIZATION TO DISCLOSE INFORMATION RELATED TO STORED VALUE ACCOUNT

IMPORTANT: You should be aware that the making of any false, fictitious, or fraudulent claim or statement to the United States is a crime that is punishable by fine and/or imprisonment.

PRINT IN INK OR TYPE ALL INFORMATION

1. AUTHORITY

A. I, _____ (the "Cardholder"), authorize the U.S. Department of the Treasury, Bureau of the Fiscal Service ("Fiscal Service") and the U.S. Department of Defense ("DoD") and Fiscal Service's and DoD's subordinate departments or agencies, along with their employees, agents, and contractors (the "Disclosing Parties") to disclose any and all information related to my EagleCash, Navy Cash, Marine Cash, or EZpay Stored Value Card account(s) ("SVC Account") to the following:

- ☐ Military and civilian law enforcement agencies and prosecutors
- ☐ Other _____

B. Information related to my SVC Account includes, but is not limited to, my Stored Value Card number and associated account number; my name, addresses, and other contact information; my social security number, other identifying numbers and types of identification, date of birth, and other demographic information about me; information about bank account(s), including routing and account numbers, which I have linked to my SVC Account or from which I have transferred funds to or from my SVC Account; my balance and transaction history, including the amount, date, time, tracking numbers, location, merchants, and payees; website usage; and other information associated with my SVC Account.

C. The Disclosing Parties are not required to give me notice of disclosures made under this authorization.

D. A photocopy, facsimile, or electronic copy of this signed authorization shall have the same force and effect as the original.

2. TERM AND DURABILITY

This authorization to disclose information is valid for one year from the date indicated below, unless it is revoked sooner by sending written notice by e-mail to svc@fiscal.treasury.gov. Revocation will be effective as of the date the notice is received and processed by the Fiscal Service.

3. SIGNATURE

I certify I am the Cardholder or am legally authorized to sign on behalf of the Cardholder.

Sign Here: _____ _____

Signature of Cardholder or Legal Representative | Date

_____ _____

Print Name of Cardholder or Legal Representative | E-Mail Address (Optional)

NOTICE UNDER PRIVACY ACT AND PAPERWORK REDUCTION ACT

AUTHORITY: 5 U.S.C. 552a; 31 CFR 210; and E.O. 9397.

PRINCIPAL PURPOSE(S): To obtain authorization to disclose information considered private under Treasury regulations and Privacy Act.

ROUTINE USE(S): The information on this form may be disclosed as generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act of 1974, as amended. It may be disclosed outside of the U.S. Department of the Treasury to its Fiscal and Financial Agents and their contractors involved in providing SVC services or to the Department of Defense (DoD) for the purpose of administering the Treasury SVC programs. In addition, other Federal, State, or local government agencies that have identified a need to know may obtain this information for the purpose(s) as identified by the Bureau of the Fiscal Service (Fiscal Service) Routine Uses as published in the Federal Register.

DISCLOSURE: Furnishing the information is voluntary; however, failure to furnish requested information may significantly delay or prevent disclosure of the information you have requested.

We estimate it will take about 1 minute to complete this form. However, you are not required to provide the information requested unless a valid OMB control number is displayed on the form. Any comments or suggestions regarding this form should be sent to the U.S. Department of the Treasury, Bureau of the Fiscal Service, 401 14th Street SW, Washington DC 20227.

FS Form 5752