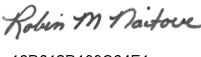


Approved:

Effective: February 7, 2022
Review: February 7, 2022
Office: Comptroller
Topic No.: 350-080-300-I

DocuSigned by:

18D012D189C64E1
Department of Transportation

RECEIPT PROCESSING

AUTHORITY

Sections 20.23(3)(a) and 334.048(3) Florida Statutes (F.S.)

REFERENCES

Sections 116.01, 215.26, 215.322, 215.34, 334.187, 337.17, 337.18, 339.04, 501.0118
Florida Statutes
Rule Chapter 14-96.008, 69C-4, Florida Administrative Code (F.A.C.)
Procedure No. 225-085-002, Submission and Recovery of Property Damage Claims
Procedure No. 325-000-002 Transportation Technology Manual
Procedure No. 350-020-300, Locally Funded Agreements Financial Provisions and
Processing
Procedure No. 350-060-303, Accounts Receivable
Procedure No. 350-080-303, Revolving Funds
Procedure No. 375-020-010, Resolution of Errors, Omissions, and Contractual
Breaches by Professional Engineers on Department Contracts
Procedure No. 575-000-000, Right of Way Manual

PURPOSE

It is the policy of the Florida Department of Transportation, Office of Comptroller, General Accounting Office to establish processes for securing, transmitting, depositing, and recording receipts.

SCOPE

This procedure sets forth the process for securing, transmitting, depositing, and recording receipts; provides internal controls to protect the security of receipts and accuracy of accounting; and sets forth the procedures for processing (or denying) requests for refund of receipts deposited into a Departmental Trust Fund. This procedure also includes the process for creating a merchant account for the acceptance

of payment card transactions and the Payment Card Industry's standards for securing cardholder data.

EXCLUSIONS

- (A) Deposits to Petty Cash Funds and other Revolving Funds are made by the offices responsible for those funds. Those deposits are in the form of either reimbursements or increases to the funds, and accordingly are not considered receipts within the scope of this procedure. See ***Procedure No. 350-080-303, Revolving Funds***.
- (B) The Turnpike Enterprise has its own established operations for submitting toll and SunPass receipts, including payment card transactions, and is exempt from using this procedure for those items.
- (C) SunRail has its own established operations for submitting toll fare receipts, including payment card transactions, and is exempt from using this procedure.
- (D) All receipts for damage claims are required to be sent to the Office of the General Counsel according to ***Procedure No. 225-085-002, Submission and Recovery of Property Damage Claims***.
- (E) Receipts associated with Locally Funded Agreements should be processed according to ***Procedure No. 350-020-300 Locally Funded Agreements Financial Provisions and Processing***.

DEFINITIONS

Cashier's Office: The unit within the Revenue Management Section of the Office of Comptroller, General Accounting Office, responsible for coordinating the receipt, accounting, and depositing of the Department's receipts.

Chargeback: A return of a previously approved payment card charge.

Department: Florida Department of Transportation

Electronic Funds Transfer (EFT): A transfer of funds between accounts by electronic means rather than conventional paper-based payment methods such as cash and check writing.

FLAIR: Florida Accounting Information Resource System; the accounting system used by all State of Florida agencies.

Internal Controls: Methods for safeguarding receipts to promote accuracy and reliability in accounting records and to ensure compliance with Department policies and procedures.

Journal Transfer (JT): A transfer of funds between two State of Florida agencies by electronic means rather than check writing.

OOC: Office of Comptroller within the Department of Transportation

OOC-DOO: Office of Comptroller – Disbursement Operations Office

OOC-GAO: Office of Comptroller – General Accounting Office

Payment Card: A credit card, charge card, debit card or any other card that is issued to a cardholder and allows the cardholder to obtain, purchase or receive goods, services, money or anything else of value from a merchant.

Payment Gateway: The process or system used to transmit payment card information to the acquiring bank.

Receipts: Any form of payment made to the Department. Receipts include, but are not limited to: cash, bank drafts or official bank checks, cashier's checks, money orders, certified checks, personal and business checks, journal transfers, electronic funds transfers (EFT), automated clearing house (ACH) deposits, wire transfers and payment card transactions.

Receipt Processing System (RPS): The Department's web-based system that processes receipts including tracking, transmitting, and depositing.

Refund of Revenue: Return of receipts paid into a Departmental Trust Fund.

Restrictive Endorsement: Wording that limits negotiability of a check or money order that is stamped or written on the back of a check or money order.

Stale Date: The date a receipt is no longer negotiable at a bank.

Treasury Receipt: A document which confirms that the Department of Financial Services has verified the deposit. This document provides a treasury receipt number and date.

1. SECURING RECEIPTS

- (A) All receipts collected are the responsibility of the office that received the receipt. Internal controls must be in place to ensure that receipts are adequately safeguarded.
- (B) An office that receives a check should examine the check to ensure that it has been completed correctly. Ensure that the check has been signed and the check

is not post-dated, stale dated or void. The numerical dollar amount and the written dollar amount must agree.

- (C) All checks and money orders shall be restrictively endorsed as soon as they are received. The restrictive endorsement shall contain "Department of Transportation", the Department's account number and "For Deposit Only". Endorsement stamps can be obtained from the Cashier's Office.
- (D) Receipts must be deposited through the Cashier's Office or returned to the customer. All offices shall enter receipts in the Receipt Processing System (RPS) as soon as they are received and monitor the RPS until the receipt is deposited or returned to the customer. All offices shall use the RPS to record the disposition of any items not deposited.
- (E) Receipts shall be secured in a locked cash box or locked bank bag and further secured in a locked file cabinet or safe until transmitted to the Cashier's Office, Mail Station 42B.
- (F) A receipt that is to be held until a determination is made as to whether it will be deposited must be entered in the RPS. The receipt shall be secured until the receipt is returned to the customer or deposited. It is the responsibility of the office that holds the receipt to track the stale date of the receipt. Receipts should be deposited or returned before the stale date is reached.
- (G) The information on a check must be safeguarded from possible identity theft. The MICR code at the bottom of the check includes the account number and should not be copied or scanned. The MICR code can be covered by a piece of paper to hide the MICR code for scanning and copying. Do not mark through the MICR code. Scan copies and email attachments should not have the MICR code readable. Electronic devices used in copying or faxing a check must follow **Manual No. 325-000-002, Transportation Technology Manual, Chapter 11, Electronic Device and Media Sanitation**. Copies of checks shall be destroyed by shredding.

2. TRANSMITTING RECEIPTS

- (A) Receipts shall be deposited no later than seven (7) working days from the close of the week in which the funds were received according to **Section 116.01, F.S.** To ensure that the Department maximizes interest earnings, receipts shall be deposited promptly. All receipts shall be transmitted within two (2) business days of receipt.
- (B) All steps shall be taken to secure the transmission of all receipts. Receipts shall be transmitted by using a tracking mechanism or in a lock bag. Receipts may be transmitted via United States Postal Service or a parcel delivery company (e.g., UPS, Fed Ex) only if the delivery method provides a means of tracking the

receipt. Receipts can also be hand delivered to the Cashier's Office or to an office with a lock bag. For security purposes, do not send any receipts through the US Postal Service without using a tracking mechanism.

- (C) Receipts shall not be left on an unattended desk.
- (D) Receipts hand delivered must be given to a person. Receipts hand delivered to the Cashier's Office may be placed in the drop box.
- (E) At a minimum, each District Financial Services Office (FSO) shall be issued a lock bag to use for the transmission of receipts to the Cashier's Office. Offices that frequently receive and transmit receipts may also be issued a lock bag. Offices may purchase additional bags, contact the Cashier's Office for assistance.
- (F) Offices that have not been issued a lock bag may transmit receipts to the District FSO for inclusion in their transmission to the Cashier's Office. Offices that use a courier or parcel delivery company (e.g., UPS, Fed Ex) to transmit receipts to the District FSO may transmit the receipt directly to the Cashier's Office using a delivery service that can be tracked.
- (G) The employee who initially receives the receipt must make every effort to ensure that the receipt has been received and processed by the individual or office that the transmittal was sent to in the RPS. This includes using the RPS to record the transmission of the receipt and monitor the RPS to ensure the receipt is received by the Cashier's Office and deposited.
- (H) All offices shall use the RPS to transmit receipts between employees and offices. The person receiving the transmittal shall make the appropriate entry into the RPS to mark the receipt as received.

3. RECEIPT PROCESSING SYSTEM (RPS)

- (A) Contact the Cashier's Office by email to be given access to the RPS.
- (B) The RPS is the official Department receipt log, transmittal log and deposit log.
- (C) All employees that receive receipts shall use the RPS. The RPS creates a controlled identifier for each receipt and for each transmittal.
- (D) All employees that have lock bag responsibility shall use the RPS to transmit the receipts to the Cashier's Office and include the lock bag number in the RPS.
- (E) The RPS is located at the following web address:
<https://fdotwp2.dot.state.fl.us/receiptprocessingsystem/Default.aspx>

- (F) Consult the RPS desk procedures located on the Cashier's Office SharePoint site for detailed instructions on the use of the RPS.

3.1 INSTRUCTIONS FOR THE RECEIPT PROCESSING SYSTEM

- (A) As soon as a receipt is received, the receipt information and the description of the transaction shall be entered into the RPS. Accounting information can be entered immediately or at a later time. If the person who received the receipt does not know the accounting information, the receipt shall be transmitted to the person who can make the accounting entry.
- (B) The accounting entries shall be completed with the proper FLAIR accounting codes (organization code, expansion option, object code and the financial project accounting data) or Accounts Receivable Invoice Number. If a project number is used on the FLAIR entry, the federal billing indicator and the external object code are required.
- (C) Backup documentation may be attached to the receipt in the RPS. The paper copy of the backup shall not be sent to the Cashier's Office. Do not attach documents with sensitive information (e.g., social security number, MICR code and primary account number).
- (D) If a receipt is duplicated in the RPS, the receipt status should be marked as a duplicate in the RPS. In the description field, include the Receipt ID number of the item that was duplicated.
- (E) The RPS shall be used to transmit the receipt to the appropriate office or employee. The transmitter shall enter the mainframe user id of the person who shall receive the receipt. The creator of the transmittal shall ensure that the receipt is received by the intended person. When transmitting receipts to the Cashier's Office, enter "cashier" in the sent to field on the transmittal log of the RPS.
- (F) The person who receives a transmittal shall enter the date the transmittal was received. The lock bag number shall be included in the RPS when a lock bag is used to send receipts between offices.
- (G) When the Cashier's Office receives a transmittal, they will enter the date that the transmittal was received into the RPS.
- (H) The Cashier's Office will verify the receipt and accounting information of transmittals received. Once the transmittal is verified, the receipt will be deposited within two business days.

3.2 RECONCILING RPS

If the accounting information needs to be changed after the receipt has been deposited in the RPS, the originator of the receipt shall provide documentation to the Cashier's Office. Email notification is acceptable. The Cashier's Office shall add the documentation to the receipt in the RPS.

4. DEPOSITING RECEIPTS – CASHIER'S OFFICE

The Cashier's Office shall make all deposits into the appropriate Departmental Trust Fund(s).

4.1 ENDORSING RECEIPTS

The Cashier's Office will ensure that all checks being deposited at the bank are endorsed with the proper information.

4.2 DEPOSIT REQUIREMENTS

- (A) Receipts will be entered into the RPS and include the FLAIR coding or the Accounts Receivable account number.
- (B) The total of the receipts and the total of the accounting entries shall both balance to the deposit slip prior to processing the deposit.
- (C) The deposit slip shall be retained for audit reference. This may be accomplished by attaching a copy to the deposit in the RPS.
- (D) The Treasury Receipt number and date shall be entered into the RPS.

5. ELECTRONIC FUNDS TRANSFERS

5.1 RECEIVING AN ELECTRONIC FUNDS TRANSFER

- (A) Offices wishing to receive an EFT should contact the Cashier's Office to receive the proper account information.
- (B) To help identify the office that requested the EFT, the reference line shall contain "DOT" and an abbreviated purpose. An example: "DOT-D7 sale of land".
- (C) For wires that are going to be deposited in the Department of Financial Services' Treasury Cash Deposit Trust Fund by the Bureau of Collateral Management (an escrow account), the reference line shall contain: "DOT – Type K11-78"
- (D) Offices receiving an EFT shall contact the Cashier's Office after they receive notification that the electronic funds transfer has been sent to the Department.

5.2 ELECTRONIC FUNDS TRANSFER – ACCOUNTING ENTRIES

- (A) The EFT information and accounting information must be entered into the RPS which records the entries into FLAIR.
- (B) The total of all entries reflected in the RPS must balance to the EFT notification that is received from the Department of Financial Services.

6. JOURNAL TRANSFERS FROM OTHER STATE AGENCIES

The Cashier's Office accepts journal transfers from other State of Florida agencies.

6.1 RECEIVING A JOURNAL TRANSFER

In order to receive a journal transfer from another agency, contact the Cashier's Office to receive the proper account code including the benefiting object code and category. The accounting codes will vary based on FLAIR fund and the type of revenue.

6.2 RECORDING A JOURNAL TRANSFER – ACCOUNTING ENTRIES

Journal Transfers will be entered into the RPS. The entry will include the FLAIR account codes or the Accounts Receivable account number. The FLAIR transactions and the Accounts Receivable account numbers must equal the total of the Journal Transfer before the deposit is made in the RPS.

7. PAYMENT CARDS

Acceptance and processing of payment cards requires the Department to have access to private and sensitive cardholder data (CHD) such as primary account number, payment card type, expiration date, etc. Protecting this sensitive information requires the development and maintenance of strong internal controls as well as compliance with Payment Card Industry Data Security Standards (PCI DSS). It is the responsibility of each office that accepts payment cards to establish these internal controls and to stay in compliance with PCI DSS requirements

7.1 PAYMENT CARD SECURITY

- (A) It is the responsibility of each cost center manager to ensure that all personnel with access to CHD environment understand and follow the PCI DSS. Each cost center manager shall annually ensure that those who come in contact with the CHD environment take PCI DSS training offered through the Department's learning management system. Each cost center manager should provide further training for their specific business model. Those employees who grant system/network access, install, design or program applications that include payment card processing should understand the PCI DSS.

- (B) Access to cardholder data shall be restricted in such a manner that only authorized personnel shall have access to the data.
- (C) Cost center managers of offices that accept payment cards must designate the responsibility of the payment gateway to an employee to oversee its use and security, as well as oversee the security of the associated cardholder data.
- (D) The employee responsible for the payment gateway must determine who has the authority to use the payment gateway and assign, establish, and maintain the passwords for those authorized users.
- (E) Records containing cardholder data must always be kept in a secure location.
- (F) Offices that accept payment cards shall not disclose or acquire any information concerning a cardholder's account without the cardholder's consent.
- (G) Cardholder data such as primary account number, payment card type, expiration date, etc., shall not be stored in any manner including, but not limited to, computers or computer networks, cell phones, or paper documents.
- (H) Cardholder data shall not be transmitted in an unsecure manner, for example, unencrypted email, unsecured fax, or U.S. mail.
- (I) Full contents of any track from the magnetic stripe on the back of a payment card shall not be stored under any circumstance.
- (J) The card validation code (the three-digit value printed on the signature panel of a Visa, MasterCard or Discover card, or the four digit code printed on the front of an American Express card) shall not be stored under any circumstance.
- (K) Faxes containing cardholder data shall not be sent or received by an email system. Fax machines that receive cardholder data must be secured in a manner that only those who process CHD have access. This can be accomplished using a fax machine that has password protection or the location of a fax machine in an office that has restricted access.
- (L) Once the cardholder data is no longer needed for business use, it shall be redacted. The information can be redacted by using a permanent marker to mask the cardholder data and then copying the document. The original shall be destroyed (cross-cut shredded) and the copy retained. Since the copy no longer contains cardholder data, it does not need to be stored securely. A copy with cardholder data redacted shall be retained in accordance with the records retention schedule.
- (M) The cardholder data must be safeguarded and all electronic devices used in copying or faxing cardholder data must follow the **Manual No. 325-000-002**,

Transportation Technology Manual, Chapter 11, Electronic Device and Media Sanitation.

7.1.1 REPORTING A CREDIT/DEBIT CARD SECURITY BREACH

In the event of a breach of cardholder data the following steps should be followed:

- (A) Immediately notify one of the following in this order:
 - (1) Deputy Comptroller, General Accounting Office at (850) 414-4864
 - (2) Cashier's Office at (850) 414-4860
 - (3) Revenue Management Administrator at (850) 414-4866.

- (B) The office where the breach occurred should immediately:
 - (1) Notify the Cost Center manager.
 - (2) Contain and limit the exposure by doing the following:
 - a) Stop the acceptance of payments cards.
 - b) Secure all cardholder data.
 - c) Stop receiving cardholder data. Offices that receive cardholder data by fax should turn off or disconnect the fax machine.
 - d) Secure the work area where cardholder data is processed, transmitted, or stored for investigation. Treat the area as a crime scene.
 - e) Log all actions taken.
 - (3) Customers desiring to pay with a payment card should be informed that payment cards cannot be accepted at this time, but other payment types (check or cash) will be accepted. Each office will notify their customers of the halt of acceptance of payment cards. Do not divulge information of the breach. The customer(s) whose information has been compromised will be contacted appropriately.

- (C) If an internet site is compromised or a computer is used in the breach:
 - (1) The internet site should be taken offline.
 - (2) Do not access or alter the compromised system.
 - (3) Do not turn off the compromised system, isolate the system from the network by disconnecting the network cable.
 - (4) Preserve all logs and electronic evidence.
 - (5) The system and work area should be secured for investigation.
 - (6) Log all actions taken.

- (D) If the cardholder data involved was processed by the Cashier's Office, all offices that send the Cashier's Office cardholder data will stop the acceptance of payment cards until notified by the OOC-GAO Deputy Comptroller.

- (E) The office(s) or internet site(s) involved in the breach will not be allowed to process payment cards until notified by the OOC-GAO Deputy Comptroller. The payment brands or merchant banks may halt all processing of payment cards throughout the Department.

- (F) The OOC-GAO Deputy Comptroller will notify the following:
- (1) Office of the Inspector General and the Comptroller
 - (2) The Department's Computer Security Incident Response Team
 - (3) Department of Financial Services
 - (4) The merchant bank
 - (5) Local office of the United States Secret Service
 - (6) Office accepting payment cards
 - (7) Central Office Public Information Office
 - (8) The individual payment brands (affected brands have the right to investigate the breach):
 - a) Visa Fraud Investigations (650) 432-2978
 - b) MasterCard (800) 622-7747
 - c) American Express (800) 297-2639
 - d) Discover (800) 347-3083
- (G) All offices accepting cardholder data will go on high alert to protect cardholder data.
- (H) In the case of an internet breach, the service provider for offices with internet websites shall be notified by the OOC-GAO Deputy Comptroller.
- (I) The merchant bank and each payment card brand may require the submission of reports of the incident.
- (J) Refer all inquiries of the breach to the Central Office Public Information Office who will be briefed by the OOC-GAO Deputy Comptroller.
- (K) Investigations into the breach may be carried out by the Office of the Inspector General, payment card brands, United States Secret Service or other law enforcement agencies. Offices involved shall not investigate the breach. Offices involved must cooperate with all investigations.

7.1.2 ANNUAL PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS) COMPLIANCE REVIEW

Each office that has a merchant account is required to perform an annual assessment to ensure compliance with PCI DSS. Each office will be responsible for completing the assessment and maintaining compliance with PCI DSS.

7.2 ADDITIONAL REQUIREMENTS

7.2.1 Use of Third Party Providers for Processing Payment Card Transactions

- (A) The cost center manager of an office that has a business need to accept payment cards shall follow **Section 7.3.1** of this procedure for setting up a merchant account.
- (B) The Cashier's Office and the Office of Information Technology shall be notified and included in interactions with third party service providers that are proposing or engaging in processing payment card transactions for the Department.
- (C) Each office that contracts with a third-party service provider to process payment card transactions for the Department shall ensure that the provider is compliant with PCI DSS, and all rules and regulations governing cardholder data security. The service provider must provide the certificate of PCI compliance or a completed Self-Assessment Questionnaire (SAQ) and any required PCI documentation.
- (D) Offices that contract with a third-party service provider to process payment card transactions for the Department shall ensure that effective language is included in the contractual documents with the provider stating that PCI DSS compliance is a requirement of the agreement.

7.2.2 Annual Report to the Chief Financial Officer for Electronic Receipts

Each office that accepts payment cards is required to comply with the requirements as outlined in **Section 215.322, F.S.**, and **Rule 69C-4, FAC**. Rule 69C-4, FAC, also requires the submission of an annual report to the Chief Financial Officer by July 30 of each year providing information on payment card transactions for the fiscal year.

7.2.3 Merchant Service Fees

Service fees may be charged by the payment card companies to the offices that process transactions. These fees include equipment rentals and per transaction processing fees.

7.2.4 Payment Card Chargebacks

- (A) A chargeback is a dispute/return of a payment card charge. Common chargebacks include customer disputes, returns and processing errors.
- (B) The Cashier's Office will process the FLAIR entries for all payment card chargebacks.
- (C) The originating office shall attempt to determine and validate the chargeback. Notification shall be sent to the customer if any discrepancies are found. If any money is owed, it must be collected or the item purchased must be returned to

the Department. If collection is not successful, further collection efforts can be made in accordance with ***Procedure No. 350-060-303, Accounts Receivable.***

7.2.5 Record Retention for Payment Card Records

- (A) All records containing cardholder data shall be kept in a secure location at all times. Only authorized personnel shall have access to the records. The cost center manager must approve the moving of any and all media from a secured area (especially when media is distributed to individuals).
- (B) See ***Section 15*** of this procedure for additional record retention requirements.
- (C) After the record retention period is over, all records containing cardholder data shall be cross-cut shredded, not discarded in the trash.
- (D) Forms that must be filed for general office use shall have the cardholder data redacted from the form. Redaction can be accomplished by marking through all cardholder data with a permanent marker and making a copy. The copy can be filed for office use and the original destroyed by cross-cut shredding or securely stored.

7.3 PAYMENT CARD PROCESSING

7.3.1 Setting Up A Merchant Account

- (A) Per ***Section 215.322, F.S.***, prior approval from the State's Chief Financial Officer (Department of Financial Services) is required prior to contracting for and accepting payment via payment cards. The Department of Financial Services has adopted ***Rule 69C-4, FAC***, governing the establishment and acceptance of payment cards.
- (B) The Cashier's Office shall coordinate the establishment of all merchant accounts according to ***Rule 69C-4, FAC***. The cost center manager of an office that has a business need to accept payment cards shall contact the Cashier's Office to start the process.
- (C) The Department of Financial Services must approve all merchant accounts and contracts with service providers according to ***Rule 69C-4, FAC***.
- (D) According to ***Rule 69C-4, FAC***, the State's contracted vendor shall be used for the processing of all payment card transactions accepted by the Department. If circumstances dictate that the State's contracted vendor is not to be used, an exemption must be obtained from the Department of Financial Services before the contract is put out for bid.

7.3.2 Settlement of Payment Card Transactions

- (A) Each office shall process or transmit its transactions daily. If a transaction is received after normal working hours or on a non-business day, the office may process the transaction on the following business day.
- (B) Offices that process transactions should perform a batch closing and settlement each day. A fee is assessed by the payment card companies for processing payment card transactions when a terminal does not transmit payment card transactions the same day the transactions were entered into the terminal.
- (C) If the payment card transactions are occurring on a website, the software should be programmed for batch closing and settlement at the latest time allowed by the payment card processor, preferably just before midnight.

7.3.3 Reporting Payment Card Transactions

- (A) Payment card transaction totals must be reported the following day to the Cashier's Office with the appropriate accounting information.
- (B) Do not send cardholder data to the Cashier's Office.

7.3.4 Depositing Payment Card Receipts

- (A) The Cashier's Office will make all deposits into the appropriate Departmental Trust Fund.
- (B) The total of all accounting entries must balance to the EFT notification that is received from the Department of Financial Services prior to processing the deposit.

7.3.5 Refunding Payment Card Receipts

- (A) **Section 215.26(3), F.S.**, states that refunds will not be initiated for amounts under \$1.00.
- (B) Under no circumstances shall a refund ever exceed the original sale amount.
- (C) Offices that process their own transactions are responsible for either processing the refund through their terminal or completing **Form No. 350-080-14, Application for Refund of a Deposited Receipt**. If a refund is to be processed using **Form No. 350-080-14, Application for Refund of a Deposited Receipt**, see **Section 10** of this procedure for further instructions.
- (D) A refund shall not be made on the same day as the sale. If the sale has not been closed (batch not yet settled), the transaction shall be voided instead of refunding

it. It is always preferable to void a transaction rather than refund it because a voided transaction is treated as if it never occurred. However, transactions can only be voided on the same day the transaction was processed, before closing the batch; otherwise a refund must be processed. The payment card companies charge a processing fee on refunds but not for voided transactions.

8. REFUNDS FOR OVERPAYMENTS FROM A VENDOR OR EMPLOYEE

- (A) All refunds to the Department shall be made payable to the Florida Department of Transportation.
- (B) If the refund is a repayment of an expenditure that was made out of a petty cash fund or local revolving fund, then the payment shall be sent to the originating office that made the expenditure.
- (C) All other refunds shall be submitted to the Cashier's Office for processing.
- (D) Refunds that are a reimbursement of a current fiscal year expenditure may be eligible for budget restoration. See **Section 9** of this procedure for further instructions.
- (E) Financial project information should be provided with the refund when it is sent to the Cashier's Office for deposit. If the financial project information is not known, the refund should still be submitted, but it should include a statement indicating that the financial project information will be provided within the following two weeks. If the financial project information is not provided in two weeks, an email with justification of the delay and the anticipated date of submission will be required from the originating office.

9. BUDGET RESTORATIONS

- (A) Budget restorations, also referred to as expenditure refunds, are made when appropriated funds are spent in error such as overpaying a vendor, paying the wrong vendor, or appropriated funds are spent for unintended use such as extending the utilization of a rental vehicle for personal usage. When a budget restoration is processed, the budget is restored and the expenditure is reduced. The Department is not authorized to restore budget for reimbursements of utilities, guardrail damage claims, operating costs, etc., as these types of expenses are expected and should have been included in the annual budget request. Not including these expenses in the legislative budget process and subsequently restoring budget and reducing expenditures when payment is received, circumvents the legislative budget process and is contrary to law and, therefore, not allowed.

- (B) Below are examples of acceptable and unacceptable requests for budget restorations, these examples are not all inclusive:

Acceptable:

- Refund from a vendor where the vendor was overpaid, paid twice or the wrong vendor was paid.
- Salary refund for employee overpayment.
- P-card reimbursement for personal use. For example, an employee uses the P-card to rent a vehicle for state business, extends the usage of the vehicle for personal use, and reimburses the state for the personal usage.
- Refunds for unused airline tickets or seminars that were cancelled or not attended.
- Department of Financial Services and Department of Management Services insurance reimbursements to the Department where the Department replaced or repaired the item that was destroyed or stolen.

Unacceptable:

- Payments for public records requests.
- Reimbursements for telecommunications, utilities, maintenance, etc.
- Salary reimbursement from an outside entity such as the federal government.
- Damage claim reimbursements for guardrails, etc.

- (C) The Department does not initiate budget restorations under \$100.00.
- (D) The refund must be a reimbursement of a current fiscal year expenditure to be eligible for restoration.
- (E) Form **No. 350-080-09, Restoration to Current Year Appropriation**, is used to request the restoration. The office that collected the refund is responsible for completing the application.
- (F) The entire form must be completed in order to process the restoration. Requesting offices should consult their District Financial Services Office or the OOC – Disbursement Operations Office if any assistance is needed in completing the original disbursement coding section.
- (G) The application must be signed and certified by the preparer.
- (H) After the application is completed, it should be sent to the Cashier's Office via email.
- (I) When the Cashier's Office approves the application, they will deposit the receipt and complete the FLAIR entries to restore the cost center's budget.

- (J) Applications that are not approved will be deposited as a refund into the appropriate Departmental Trust Fund and the cost center's budget will not be restored.
- (K) All receipts for damage claims must be sent to the Office of the General Counsel in Central Office.
- (L) All receipt information shall be entered into the RPS and the receipt transmitted to the Cashier's Office.

10. REFUND OF DEPOSITED RECEIPTS

- (A) **Section 215.26(3), F.S.**, states that refunds will not be initiated for amounts under \$1.00. This statute also limits the filing of refunds within three years after the right to the refund has accrued.
- (B) An application for a refund, **Form No. 350-080-14, Application for Refund of Deposited Receipt**, is used to request a refund. The office that collected the receipt being refunded is responsible for completing the application.
- (C) A refund cannot be processed without a current vendor number. Requesting offices should consult their District Financial Services Office or the OOC – Disbursement Operations Office to establish or verify vendor numbers.
- (D) The application shall be signed and certified by the preparer and an approver.
- (E) The person preparing and approving the application shall not be the same person.
- (F) After the application is completed, it shall be sent to the Cashier's Office for processing.
- (G) Once the Cashier's Office confirms the deposit of the receipt, it shall be returned to the originating office or sent to OOC – Disbursement Operations Office upon the request of the originator for payment.
- (H) The Cashier's Office maintains a refund log and verifies the refund request to this log to ensure that duplicate refunds are not issued.

11. ITEMS RETURNED BY THE DEPARTMENT OF FINANCIAL SERVICES FOR COLLECTION

- (A) Items returned unpaid by the Department of Financial Services shall be collected in accordance with **Section 215.34(2), F.S.**

- (B) The Cashier's Office will make the appropriate accounting entries to reflect the returned item.
- (C) Whenever a check, draft or other order for the payment of money is returned, the Department shall add to the amount due, a service fee of \$15.00 or 5% of the face amount of the check, draft or other order, whichever is greater. The amount of the service fee shall not exceed \$150.00.
- (D) Collection efforts should follow ***Procedure No. 350-060-303, Accounts Receivable***.
- (E) Successful collections of returned items and the required service fees shall be transmitted to the Cashier's Office. The Accounts Receivable Section should be notified of successful collection.
- (F) For items collected, the service fees shall be deposited into the same trust fund as the collected item using the appropriate object code for returned check fees.

12. SECURITY INSTRUMENTS AND OTHER TYPES OF RECEIPTS

- (A) **Bid Guaranty Receipts:** When received, the bid guaranty receipt shall be entered into RPS and deposited within 60 days of receipt. Extended time may be allowed to deposit these receipts, at the discretion of the Districts, if the probability is high that the receipt will be returned soon after this 60-day time frame. Controls must be in place to ensure the accountability and security of the receipts at all times. If not immediately deposited, they must be locked in a secure location and monitored. If there is any likelihood that the receipt will be deposited, they must be deposited before the expiration date in accordance with this procedure; see **Sections 1, 2 and 3** of this procedure for further instructions. **Section 337.17, F.S.**, establishes the types of acceptable bid guaranties which do not include cash, personal checks or business checks.
- (B) **Contract Performance Receipts:** When received, contract performance receipts from vendors to whom the contracts are awarded, shall be entered into the RPS and deposited within 30 days of the execution of the contract. A contract expected to take more than 30 days to complete shall have the performance receipt deposited in accordance with this procedure; see Sections 1, 2 and 3 of this procedure for further instructions. This time may be briefly extended to allow for completion of very small projects and the subsequent return of the receipts at the District's discretion. Controls shall be in place to ensure the accountability and security of the receipts at all times. If not immediately deposited, the receipt shall be locked in a secure location and shall be monitored. If there is any likelihood that the receipts will be deposited, they shall be deposited before the expiration date. **Section 337.18, F.S.** establishes the types of acceptable contract performance receipts which do not include cash, personal checks or business checks.

- (C) **State Highway System Connection Permit Performance Receipts:** In accordance with Rule 14-96.008(3)(a), FAC, prior to the issuance of a permit, the applicant shall provide a security instrument (letter of credit or surety bond) pursuant to Section 334.187, F.S. The security instrument shall be valid for a sufficient time to cover the construction and inspection of the permitted work but not for less than 18 months. The security instrument shall be returned to the applicant when final inspection by the Department shows that the work has been completed as permitted. Letters of credit must be approved by the Department's Comptroller or designee prior to acceptance. All letters of credit must be transmitted to the OOC-General Accounting Office (MS 42B) upon receipt for safekeeping.
- (D) **Unsolicited Proposal Fees:** Unsolicited Proposal checks received are to be submitted to the Cashier's Office to be held until executive direction is received regarding disposition of the fee in accordance with the Public Private Partnership (P3) Handbook located on the OOC SharePoint site.

13. SALES TAX

- (A) The Department is required by Florida law to collect the proper state and discretionary sales taxes on all required sales and leases. Although the OOC-GAO has general knowledge of the taxability of general sales and leases, given the numerous varieties and complexity of Right of Way (ROW) sales and leases, the District Right of Way Office may be the best source for taxability information.
- (B) Monthly, the Cashier's Office remits sales tax collected by the Department during the prior month to the Department of Revenue. This includes both the state sales tax and the discretionary sales surtax (county tax).
- (C) The Department of Revenue's website contains the county discretionary sales surtax rates along with the effective dates and expiration dates.

14. REVENUE REPORTS

The Cashier's Office sends out monthly revenue reports showing the revenue that was received and deposited for the prior reporting period. The reports should be reviewed monthly for accuracy by the responsible collecting office and any discrepancies should be reported immediately.

14.1 REVENUE BY OBJECT REPORT

This report shows revenues that were collected during the fiscal year that may be allocated back to the Districts in accordance with **Section 11.1.4 of Procedure No. 575-000-000, Right of Way Manual** and **Section 28 of Procedure No. 375-020-010, Resolution of Errors, Omissions and Contractual Breaches by Professional Engineers on Department Contracts.**

15. RECORD RETENTION FOR CASH COLLECTION RECORDS

- (A) Documentation included with a receipt for deposit will follow the retention schedule for cash collection records. If documents included with receipts follow a longer retention schedule, it shall be the originating office's responsibility to maintain these records according to any applicable retention schedules.
- (B) The required retention period for cash collection records (including but not limited to cash and check logs, payment card information, transmittals, electronic fund transfer records, deposit slips, refunds of receipts deposited, and bad check records) shall be five (5) years provided all applicable audits, if any, have been released. Offices may choose to keep information for a longer period if desired or until they are obsolete, superseded or administrative value is lost.
- (C) Records containing payment cardholder data are considered to contain sensitive information. After the retention period is over, all records should be cross-cut shredded
- (D) Check copies contain bank account information, which is considered sensitive information. These records should be cross-cut shredded after the retention period is over.

16. TRAINING

Training sessions are provided upon request by the appropriate District Financial Services Office or the Cashier's Office.

17. FORMS

- Form No. 350-080-09, Restoration to Current Year Appropriation
- Form No. 350-080-14, Application for Refund of a Deposited Receipt