Clerk of the Court and Comptroller

of

Miami Dade County

334: Credit Card Processing Procedures for Working Remotely

PCI Team 11/1/25 No. 334

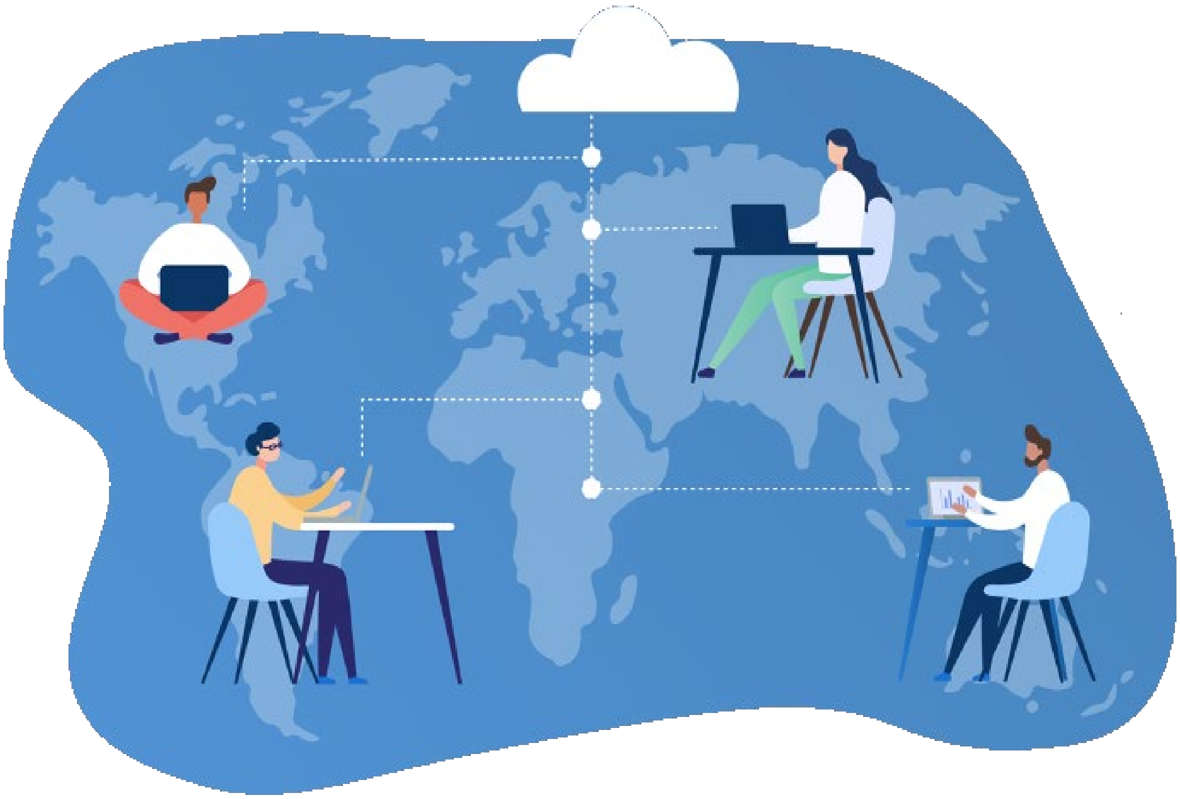

Table of Contents

I. **Procedures** 1-2

II. **Additional Requirements for Working Remotely** 3

Applicable Policies and Procedures 4

Miami-Dade Entities requesting approval to allow employees working remotely to process credit card transactions, will need to follow the procedures listed below:

I. Procedures

Prepare a **memorandum** from the **Department Director to the Chief Administrative Officer** requesting authority to process credit transactions for the specific section/unit/process to include the following:

1. Explain in detail the reason the Miami-Dade Entity is requesting this authority and length of request (if known) and acknowledge an understanding and acceptance of compliance for Working Remotely procedures as listed in the COCC Credit Card Processing Procedures #333 Section IV(B).
2. Include that the employee(s) will be provided with a Miami-Dade Entity laptop, cellphone, and Wi-Fi devices. Only Miami-Dade Entity approved equipment is allowed for processing credit card transactions. Provide a list (as an attachment to the memorandum) with the equipment provided and respective serial numbers.
3. Include the name and employee identification (ID) for the employee(s) that will be assigned to process payments remotely (those employees processing refunds and chargebacks must be at the accountant 2 or equivalent level, or above).
4. Confirm that the Miami-Dade Entities credit card processing procedures will be followed while processing remote transactions, including:
   A. Any deviations from the Miami-Dade Entity's current credit card processing policy.
      i. Including extra controls being implemented for terminal security, credit card processing over the phone, refund processing, reconciliations, etc.

   B. Approved cellular wireless terminals are allowed for remote payment processing.

   C. P2PE terminals is strongly recommended and is the preferred method for accepting the Payment Card information by the Miami-Dade Entity staff via the workstation.

   D. If P2PE terminals are not an option, Miami-Dade Entity will need to have a Miami-Dade Entity issued and managed device that connects securely to the eCommerce website or other payment application, and it is used solely for processing payments. Using a non-P2PE solution will need to be formally reviewed and approved through a risk acceptance memorandum detailing the risk mitigation process and justification, then reviewed by the PCI Team and executed between the Department Director and the Chief Administrative Officer.

      Note: Based on the above, workstations used for processing payments, should be built using Security Office approved and maintained configuration document. Staff should follow security requirements including restrict physical access to employee use only.

E. Reminder: The employee processing regular sale transactions cannot also process refunds or reconciliations. Therefore, if refunds need to be processed remotely, an additional terminal, laptop, cellphone, and/or Wi-Fi device will need to be issued to someone at the supervisory level. The Miami-Dade Entity needs to specify who will have this access and at what location.

5. Send the memo (which can be routed through ADOBE Sign) to the CFO's Administrative & Compliance Services Division, copy the following individuals on the memo:
   - Barbara.Gomez@Miamidadeclerk.gov
   - Vivian.Delgado@miamidadeclerk.gov
   - Alvaro.Carcache@miamidadeclerk.gov
   - Christina.Torres@miamidadeclerk.gov
   - Katherine.Sosa@miamidadeclerk,gov
   - Jorge.Mederos@miamidade.gov
   - Lawrence.Embil@miamidade.gov
   - Jeremy.Clark@miamidade.gov

6. Along with memo, include the Miami-Dade Entity procedures, which includes the Working Remotely process. *Refer to procedure #333 Credit Card Acceptance and Processing Procedures for further guidance.*

7. The employee(s) whom the terminal, laptop, cellphone, and/or Wi-Fi device is assigned to, will need to have taken or take the latest PCI Course, provide proof of completion, and sign the Working Remotely Attestation annually. The employee will send the attestation form along with the supporting documentation via email at (FIN-Compliance@miamidade.gov).

   The Working Remotely Attestation can be found at https://intra.miamidade.gov/finance/payment-card-industry.asp.

8. Once approval is received, Comptroller Finance Operations Department's (CFO) Cash Management Division will provide an order form (for those Miami-Dade Entities requesting terminal rentals) to the Miami-Dade Entity to fill-in information on shipping, contacts, etc. CFO's Cash Management Division will then forward the form to Elavon and advise the respective Miami-Dade Entity of shipping details.

9. Once the terminal is received, the user will call the merchant processor terminal support to setup a terminal password, and the user conducting refunds will also call terminal setup to setup a refund password (For terminals used to process refunds).

10. The PCI Liaison will update the equipment inventory list/MID Listing and provide a copy to the CITD's Security Division and CFO's Administrative & Compliance Services Division.

11. Once the terminal is no longer needed, The PCI liaison will contact CFO's Cash Management Division for directions on returning the terminal to the merchant processor.

Exemption: *Constitutional Offices would only need a memorandum from Elected Officer or Delegated Authority to Comptroller Finance Operations Department Director authorizing staff to process credit card transactions while working at home along with the required information stated above.*

II. ADDITIONAL REQUIREMENTS FOR WORKING REMOTELY

Those employees involved with credit card functions while working remotely are required to adhere, comply, and acknowledge all applicable policies and procedures. Refer to additional requirements below:

1. **Approved Equipment:** Staff may only use Miami-Dade Entity approved equipment, (i.e., laptop, cellphone, POS terminals and Mi-Fi) to process payments.

2. **Physical Control:** To safeguard home workspace the area should be securely maintained and inaccessible to unauthorized individuals. Employees should disable camera or recording functions when processing credit card transactions. Computer screens and authorized area should be locked when leaving workspace area and all passwords secured.

3. **Terminal Inspections:** Supervisory Staff should check POS devices **monthly** for any skimmers; a log should be maintained of the review. POS devices should be in a physically secure location when not in use. Employees who work remotely and are using POS devices must periodically check devices for skimmers and maintain a tampering log, which will be reviewed by the PCI Liaison. Any suspected breaches should be reported immediately by completing an on-line incident reporting form. ***(Refer to Payment Device Inspection Log for instructions)***

   Note: In the event the POS device is broken, the employee shall report it to their supervisor and PCI Liaison. Thereafter, the liaison will inform CFO's Cash Management Division for replacement/disposition instructions.

4. **Workspace Area**: Employee may be asked to turn the camera function on for the PCI Team to be able to virtually review the devices serial number workspace area, if needed.

   Note: Any materials or equipment taken home and/or to the approved designated remote work location must be kept in the designated work area and not be made accessible to others.

5. PCI -DSS Protecting Payments While Working Remotely handout should be reviewed and acknowledged. Information on handout can be found at: https://blog.pcisecuritystandards.org/protecting-payments-while-working-remotely

6. The following training for PCI Liaisons is recommended. Information on the training can be found at: https://www.pcisecuritystandards.org/program_training_and_qualification/work_from_home_security_awareness

III. APPLICABLE POLICIES AND PROCEDURES

- Payment Card Industry Executive Charter and Compliance Policy (Policy #332) https://www.miamidade.gov/managementandbudget/library/procedures/332.pdf
- 333 - Credit Card Acceptance and Processing Procedures
  https://www.miamidade.gov/managementandbudget/library/procedures/333.pdf
- Miami Dade County Enterprise Information Security Policy Manual https://intra.miamidade.gov/finance/library/security-policy-manual.pdf
- Payment Card Industry Data Security Standards Incident Response Plan http://intra.miamidade.gov/finance/library/guidelines/incident-response-plan.pdf
- Employee Telecommuting – AO 7-46: https://documents.miamidade.gov/ao-io/AO/AO-07-46.pdf
- Acquisition, Assignment and Use of Telecommunication Devices and Network Resources, AO No. 5-5: https://documents.miamidade.gov/ao-io/AO/AO-05-05.pdf
- Miami Dade County Identity Theft Prevention Program (Red Flags-Resolution R-580-10) http://www.miamidade.gov/govaction/legistarfiles/Matters/Y2010/101045.pdf