Miami Dade County

Credit Card Processing Procedures for Working Remotely 334

Updated 09/2023

Departments requesting approval to allow employees working remotely to process credit card transactions on behalf of Miami Dade County, will need to follow the procedures listed below:

I) 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:

   - Explain in detail the reason the department 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 County policy #333 Section IV. B.
   - Include that the employee(s) will be provided with County laptop, cellphone, and Wi-Fi devices. Note that only County approved equipment is allowable for processing credit card transactions. Provide a list (as an attachment to the memorandum) with the equipment provided and respective serial numbers.
   - 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).
   - Confirm that the departments credit card processing procedures will be followed while processing remote transactions, including:
     - Any deviations from the department's current credit card processing policy.
       - Including extra controls being implemented for terminal security, credit card processing over the phone, refund processing, reconciliations, etc.
     - Approved analog or cellular wireless terminals are allowed for remote payment processing.
     - P2PE terminals is strongly recommended and is the preferred method for accepting the Payment Card information by MDC staff via the workstation.
     - If P2PE terminals are not an option, departments will need to have a County 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 County's 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.*

- **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 Department needs to specify who will have this access and at what location.

o Send the memo (which can be routed through ADOBE Sign) to the Finance Department Administrative & Compliance Services Division, copy the following individuals on the memo:

- Barbara.Gomez@Miamidade.gov
- Vivian.Delgado@miamidade.gov
- Alvaro.Carcache@miamidade.gov
- Christopher.Hill@miamidade.gov
- Lars.Schmekel@miamidade.gov
- Lawrence.Embil@miamidade.gov
- Jeremy.Clark@miamidade.gov
- Ranjana.Warier@miamidade.gov
- Andrea.Hankerson@miamidade.gov
- Cristina.Perez@miamidade.gov
- Maria.Torres@miamidade.gov

II) Along with memo, include the Departmental procedures, which includes the Working Remotely process Refer to procedure #333 Credit Card Acceptance and Processing Procedures for further guidance.

III) The employee(s) that 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 (which can be found at https://intra.miamidade.gov/finance/payment-card-industry.asp. 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.

IV) Once approval is received, Finance Cash Management Division will provide an order form (for those departments requesting terminal rentals) to the department to fill-in information on shipping, contacts, etc. Cash Management Division will then forward the form to Elavon and advise the department of shipping details.

V) Once the terminal is received, the user will call Elavon 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).

VI) The PCI Liaison will update the departments' equipment inventory list/MID Listing and provide a copy to the Information Technology Department Security Division and the Finance Administrative & Compliance Services Division.

VII) Once the terminal is no longer needed, The PCI liaison will contact the Finance Cash Management Division for directions on returning the terminal to Elavon.

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 MDC Equipment:** Staff may only use County 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 periodically check POS terminals for any skimmers; a log should be maintained of the review. POS terminals 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 departmental PCI Liaison. Any suspected breaches should be reported immediately by completing an on-line incident reporting form.

   Note: In the event the terminal is broken, the employee shall report it to their supervisor and PCI Liaison. Thereafter, the liaison will inform Finance Department Cash Management Division for replacement/disposition instructions.

4. **Workspace Area**: Employee may be asked to turn the camera function on, so the PCI Compliance Team can 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

Applicable Policies and Procedures

- 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: http://www.miamidade.gov/aopdfdoc/aopdf/pdffiles/AO5-5.pdf

- Payment Card Industry Executive Charter and Compliance Policy (Policy #332) https://www.miamidade.gov/managementandbudget/library/procedures/333.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 http://intra.miamidade.gov/technology/library/guidelines/security-policy-manual.pdf

- Payment Card Industry Data Security Standards Incident Response Plan http://intra.miamidade.gov/finance/library/guidelines/incident-response-plan.pdf

- Miami Dade County Identity Theft Prevention Program (Red Flags-Resolution R-580-10 http://www.miamidade.gov/govaction/legistarfiles/Matters/Y2010/101045.pdf