HOUSTON COMMUNITY COLLEGE

Procurement Operations
3100 Main St.
Houston, TX 77002

Solicitation Amendment No. 003

To: Prospective Bidder / Offeror:	**Date:**
Prospective Proposers	July 31, 2018
Project Title:	**Project No.:**
Merchant Services	RFP 18-32

The Request for Proposals (Project RFP No. 18-32) is hereby amended to include clarifications as set forth in the attached clarifications.

Except as provided herein, all terms and conditions of the solicitation remain unchanged and in full force and effect.

Company Name (Bidder / Offeror):	
Signed by:	**Date:**
Name (Type or Print):	**Title:**

Clarifications

July 31, 2018

Respondent must provide evidence of their PCI DSS compliance, including evidence for any subcontractors, third party processors and any other involved parties.

1. SOC 2 Type II reports for the application and any third party hosting and/or equivalent audited security controls assurance documents shall be provided as a part of the solution proposal. Address the levels of security, types of access permitted, who controls security, and how security interacts with LAN and WAN security elements and data sharing transactions. Each user shall have a secure, separate login with centralized authentication to HCC's Identity Management platform. Vendor agrees to complete an Application Security Assessment with HCC IT Security to validate data flows and controls prior to system implementation.

2. The College is currently developing plans for converting to EMV hardware.

3. Describe your PCI-DSS compliance status and program.

4. How do you maintain your continued compliance with the PCI standards?

5. Is your organization and all of your contractors, subcontractors and third-party processors, in compliance with all applicable PCI DSS standards. Has a qualified third-party assessor certified you as compliant. Please name the assessor.

6. What is your role in supporting merchant PCI compliance and how do you help a merchant like the Houston Community College Finance and Administration office maintain its compliance.

7. Describe in detail how your services are integrated to/with third party software, websites and gateways.

8. List all fees associated with implementation and interfacing with CashNetUSA application used by HCC.

9. Describe support provided after implementation.

10. Respondent will be responsible for safeguarding all stored data, particularly files that contain cardholder information, so as to be compliant with all state and federal laws and regulations, and in the case of Credit Cards, individual card brand requirements.

11. Provide the completed PCI DSS AOC v 3.2. Form, this will be used to ensure respondents are compliant with Payment Card Industry Data Security Standards (PCI DSS) and used as proof of such certification in accordance with the policies, standards and guidelines.

12. Respondents must be able provide an electronic monthly summary report to the Houston Community College Finance and Administration office summarizing the activity for all College locations by department name, with monthly sales, transaction counts and a breakdown of the transactions by all card types. It should also include the number of monthly authorizations, PIN debits, and any other transaction services fees by category.