Appendix B
NHCPL Self-Checkout RFP PCI Questionnaire

The following questions are pursuant to the PCI Security Council Publication: "Payment Protection Resources for Small Merchants – Questions to Ask Your Vendors"

1. Does your solution/product ensure the secure capture and transmission of cardholder data?
   - ☐Yes
   - ☐No

   If No, will New Hanover County's (NHC) agreement with you (the vendor) include clauses that state that you will maintain PCI DSS compliance for your product/service (or become PCI DSS validated)?
   - ☐Yes
   - ☐No

2. Does your product/solution store payment card information locally?
   - ☐Yes
   - ☐No

   If Yes, please provide confirmation that the data is stored per PCI DSS requirements.

3. Does your product/solution protect payment card information with strong encryption?
   - ☐Yes
   - ☐No

   If Yes, what type of encryption is used.

4. Does your solution use a payment application listed with the PCI council's "List of Validated Payment Applications"? (https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement)
   - ☐Yes (If Yes, proceed to question 4a.)
   - ☐No (If No, proceed to questions 4b-4d.)

   4a. Are you a Qualified Integrator or Reseller (QIR)?
   - ☐Yes
   - ☐No

   4b. Do you provide support during the installation to ensure NHC implementation meets PCI DSS requirements?
   - ☐Yes
   - ☐No

   4c. Do you provide an implementation guide?
   - ☐Yes
   - ☐No

   4d. Do you provide installation guidance on how to ensure card data is protected wherever it is stored, processed, or transmitted?
   - ☐Yes
   - ☐No

5. Is your product/solution installed on NHC network/systems?
   - ☐Yes (If Yes, proceed to questions 5a-5c)
   - ☐No

   5a. Do you install patches and updates to the system/solution?
   - ☐Yes
   - ☐No

5b. Do you do this in a manner that aligns with PCI DSS requirements?

☐Yes

☐No

5c. How do you notify us, how are patches made available, and what support do you provide?

6. Is the solution installed on systems owned and operated by the service provider?

☐Yes (If yes, proceed to question 6a)

☐No

6a. Is the service provider PCI DSS compliant?

☐Yes

□No

7. Do you require remote access to NHC payment system/solution to support it?

☐Yes (If Yes, proceed to question 7a)

☐No

7a. What steps do you take to secure remote access?

8. Is the solution/product required to integrate with other systems?

☐Yes

☐No

9. In the event there is a data breach and your product/solution is involved:

9a. If I experience penalties, do you offer support and protection?

☐Yes

☐No

9b. How and when do you notify NHC if there is a breach?

9c. What monitoring for data breaches and suspicious activities do you provide?

10. Does the service provider carry insurance to cover data breaches related to their product/service?

☐Yes

☐No

11. Does the service provider assist with the notification of NHC customers in the event of a data breach and your solution/product is the root cause?

☐Yes (If yes, proceed to questions 11a-11c)

☐No

11a. Do you cover the cost?

☐Yes

☐No

11b. Do you send the notifications?

☐Yes

☐No

11c. Do you provide credit monitoring for the customers impacted?

☐Yes

☐No