BUNCOMBE COUNTY

Request for Proposal

Payment Processing Services

Date of Issue: November 21, 2023

Proposal Submission Deadline: January 9, 2024

at 1:00 PM ET

TABLE OF CONTENTS

1.0 PURPOSE AND BACKGROUND

Buncombe County intends to establish a contract for Payment Processing Services for electronic data credit card and debit card payment services, including point-of-sale transactions, phone and internet transactions, and electronic check conversion.

Proposals shall be submitted in accordance with the terms and conditions of this RFP and any addenda issued hereto.

2.0 GENERAL INFORMATION

2.1 REQUEST FOR PROPOSAL DOCUMENT

The RFP is comprised of the base RFP document, any attachments, and any addenda released before Contract award. All attachments and addenda released for this RFP in advance of any Contract award are incorporated herein by reference.

2.2 NOTICE REGARDING RFP TERMS AND CONDITIONS

It shall be the Vendor's responsibility to read the Instructions, the County's terms and conditions, all relevant exhibits and attachments, and any other components made a part of this RFP and comply with all requirements and specifications herein. Vendors also are responsible for obtaining and complying with all addenda and other changes that may be issued in connection with this RFP.

If Vendors have questions, issues, or exceptions regarding any term, condition, or other component within this RFP, those must be submitted as questions in accordance with the instructions in Section 2.5 PROPOSAL QUESTIONS. If the County determines that any changes will be made as a result of the questions asked, then such decisions will be communicated in the form of an RFP addendum. The County may also elect to leave open the possibility for later negotiation and amendment of specific provisions of the Contract that have been addressed during the question and answer period. Other than through this process, the County rejects and will not be required to evaluate or consider any additional or modified terms and conditions submitted with Vendor's proposal. This applies to any language appearing in or attached to the document as part of the Vendor's proposal that purports to vary any terms and conditions or Vendors' instructions herein or to render the proposal non-binding or subject to further negotiation. Vendor's proposal shall constitute a firm offer. **By execution and delivery of this RFP Response, the Vendor agrees that any additional or modified terms and conditions, whether submitted purposely or inadvertently, shall have no force or effect, and will be disregarded. Noncompliance with, or any attempt to alter or delete, this paragraph shall constitute sufficient grounds to reject Vendor's proposal as nonresponsive.**

2.3 RFP SCHEDULE

The table below shows the *intended* schedule for this RFP. The County will make every effort to adhere to this schedule.

Event	Responsibility	Date and Time
Issue RFP	County	11/21/2023
Submit Written Questions	Vendor	12/01/2023
Provide Response to Questions	County	12/08/2023
Submit Proposals	Vendor	01/09/2023 by 1:00 PM
Contract Award	County	02/15/2024
Contract Effective Date	County	TBD: 07/01/2024 or later, depending on project needs.

2.4 PROPOSAL QUESTIONS

Upon review of the RFP documents, Vendors may have questions to clarify or interpret the RFP in order to submit the best proposal possible. To accommodate the Proposal Questions process, Vendors shall submit any such questions by the above due date.

Written questions shall be emailed to *nina.alexander@buncombecounty.org* by the date and time specified above. Vendors should enter "RFP Payment Processing Services Questions" as the subject for the email. Questions submittals should include a reference to the applicable RFP section.

Questions received prior to the submission deadline date, the County's response, and any additional terms deemed necessary by the County will be posted in the form of an addendum. No information, instruction or advice provided orally or informally by any Buncombe County personnel, whether made in response to a question or otherwise in connection with this RFP, shall be considered authoritative or binding.

2.5 PROPOSAL SUBMITTAL

Proposals will be received until 1:00 PM, 12/21/2023. All proposals may be submitted electronically submitted via email and properly identified with the title "RFP Payment Processing Services Proposal."

Proposals may be emailed to:
Nina Alexander

E-mail: nina.alexander@buncombecounty.org

The County's capacity for email attachments is 9mb. It is the bidder's responsibility to ensure the proposal is received prior to the proposal acceptance time. Late proposals will not be accepted. The County reserves the right to accept or reject all or any part of any proposal, waive informalities and award the contract to best serve the interest of the County. It is the responsibility of the applicant that their proposal is received. Receipt of proposals can be verified by calling 828-250-4311.

2.6 PROPOSAL CONTENTS

Vendors shall populate all attachments of this RFP that require the Vendor to provide information and include an authorized signature where requested. Vendor RFP responses shall include the following items and those attachments should be arranged in the following order:

a) Cover Letter

b) Title Page: Include the company name, address, phone number and authorized representative.

c) Describe the background, experience, and capabilities of your firm as it relates to the Scope of Work outlined in the RFP.

d) Identify all subcontractors you intend to use for the proposed scope of work. For each subcontractor listed, proposers shall indicate 1.) What products and/or services are to be supplied by that subcontractor and; 2.) What percentage of the overall scope of work that subcontractor will perform.

e) Identify each individual who will work as part of this engagement. Include resumes for each individual along with any certifications, licenses, etc.

f) List at least 3 government agency references of similar size for whom you have provided services in the past three years. Provide telephone numbers and contact names for references.

g) Provide specific costs for services.

h) Each Vendor shall submit with its proposal the name, address, and telephone number of the person(s) with authority to bind the firm and answer questions or provide clarification concerning the firm's proposal.

i) Absorbed and pass-thru rate schedules for each of the scenarios you're submitting a proposal for, if different

j) Provide a detailed fee schedule for discount fees and all other charges and expenses. Include any applicable gateway fees, set up fees, monthly account fees, transaction fees for processing, interchange fees, risk assessment fees, and reporting all transactions. Specify all other fees and charges, included, but not limited to, implementation and conversion costs, chargebacks, voice and offline authorizations, devices, etc.

k) Specify differences in discount rates and fees for each type of card and each type of transaction, i.e.: debit vs. credit; point-of-sale terminal transaction vs. phone transaction vs. internet transaction.

l) Specify all applicable fees associated with electronic check conversion, including but not limited to set up fees, monthly access fees, per ACH transaction fees, ACH per item return fees.

m) Implementation timeline and details of the support provided by vendor.

n) Example reports, details regarding the ability and extent of report customization, and report accessibility (sent daily or accessed online).

o) Provide details regarding the ability to customize product to meet County needs (e.g. website, transaction, phone, etc.).

p) Describe settlement process (timing, reporting, deposits, etc.).

q) Demos of the service will be requested during the review stage.

3.0 METHOD OF AWARD AND PROPOSAL EVALUATION PROCESS

3.1 METHOD OF AWARD

All qualified proposals will be evaluated, and awards will be made to the Vendor(s) meeting the RFP requirements and best fits the needs of the County.

Buncombe County reserves the right to reject any and/or all submittals, and to waive defects, technicalities and/or irregularities in any submittal. The County reserves the right to finalize a contract with one or more firms based on all factors involved in the written qualification submittal without further discussion or interviews.

Proposals will generally be evaluated according to completeness, content, and experience with similar projects, ability of the Vendor and its staff, and cost.

Vendors are cautioned that this is a request for offers, not an offer or request to contract, and the County reserves the unqualified right to reject any and all offers at any time if such rejection is deemed to be in the best interest of the County.

3.2 EVALUATION CRITERIA

Following the deadline for submittals, a selection committee will review the submitted proposals. The selection committee will review, analyze, and rank all submittals based on their response to the information requested. The selection process will include the following criteria in the evaluation of proposals. These criteria are not necessarily listed in order of importance.

1. Technical Capabilities:

Integration Options: Compatible with existing systems (Workday, WasteWorks, Accela, NCPTS, etc.).

Technical and Nontechnical Security Measures: Offers encryption, tokenization, and certification/compliance with industry standards (e.g., PCI DSS), organizational policies and procedures, personnel security considerations, incident response and data breach plans. The county will be permitted to audit the technical protections in place.

2. Functionality and Features:

- Payment Methods: Processor supports various payment methods (credit cards, digital wallets, ACH, etc.).

- Recurring Billing
- Ability to customize the product to meet County needs (including additional information during check-out, customizing phone messages, etc.)
- Data entry validation

3. Reliability and Uptime:

- Service Level Agreements (SLAs): Uptime guarantees and responsiveness during outages.
- Redundancy: Backup systems and disaster recovery plans.

4. Pricing and Fees:

- Transaction Fees: Competitive rates for different transaction types (e.g., card-present vs. online).
- Setup Costs
- Monthly Fees
- Hidden Fees

5. Customer Support and Service:

- 24/7 Support: Consistent availability and responsiveness
- Technical Assistance: Prompt issue resolution
- User Training

6. Reporting and Analytics:

- Transaction Reporting: Ability to access reports online. Thorough transaction details (status, date, etc.).
- Customizable Reports: Offers flexibility to create custom reports.

7. Compliance and Legal Considerations:

- PCI Compliance: Adheres to Payment Card Industry Data Security Standard (PCI DSS) requirements.
- Data Privacy: Complies with data protection laws (e.g., GDPR).
- Contract Terms
- Access to department/merchant ID information secured by user, as well as the ability to make actions.

4.0 REQUIREMENTS

4.1 CONTRACT TERM

The Contract shall have an initial term of three years, beginning on the date of contract award (the “Effective Date”).

4.2 PRICING

Proposal price shall constitute the total cost to Buyer for complete performance in accordance with the requirements and specifications herein, including all applicable charges handling, administrative and other similar fees. Vendor shall not invoice for any amounts not specifically allowed for in this RFP.

4.3 VENDOR EXPERIENCE

In its Proposal, Vendor shall demonstrate experience with public and/or private sector clients with similar or greater size and complexity to Buncombe County. Vendor shall provide information as to the qualifications and experience of all

executive, managerial, legal, and professional personnel to be assigned to this project, including citing experience with similar projects and the responsibilities to be assigned to each person.

4.4 VENDOR'S REPRESENTATIONS

a) Vendor warrants that qualified personnel shall provide Services under this Contract in a professional manner. "Professional manner" means that the personnel performing the Services will possess the skill and competence consistent with the prevailing business standards in the industry. Vendor agrees that it will not enter any agreement with a third party that may abridge any rights of the County under this Contract. Vendor will serve as the prime contractor under this Contract and shall be responsible for the performance and payment of all subcontractor(s) that may be approved by the County. Names of any third party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).

b) If any Services, deliverables, functions, or responsibilities not specifically described in this Contract are required for Vendor's proper performance, provision and delivery of the service and deliverables under this Contract, or are an inherent part of or necessary sub-task included within such service, they will be deemed to be implied by and included within the scope of the contract to the same extent and in the same manner as if specifically described in the contract. Unless otherwise expressly provided herein, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and Deliverables.

c) Vendor warrants that it has the financial capacity to perform and to continue perform its obligations under the contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of this Contract; and that entering into this Contract is not prohibited by any contract, or order by any court of competent jurisdiction.

5.0 SCOPE OF WORK

General

Buncombe County intends to establish a contract for Payment Processing Services for electronic data credit card and debit card payment services, including point-of-sale transactions, phone and internet transactions, and electronic check conversion.

Nature of Services Required:

- Electronic payment processing
- Funding, refunding, and settlement
- Customer Service
- Reporting capabilities

Scenarios

We are exploring vendors for multiple scenarios. A payment processor will be selected to provide services in alignment with one or more of the following options:

Scenario 1. Payment processor will provide services for web-based property tax payments.

FY23 Property Tax Web Transactions		
Month	Transaction Amount	Number of Transactions
Jan	$15,301,139	7,702
Feb	$2,276,252	1,861

Mar	$1,115,220	1,228
Apr	$622,908	1,436
May	$253,100	744
Jun	$132,635	391
Jul	$69,149	143
Aug	$4,047,972	2,113
Sep	$2,850,517	2,143
Oct	$2,477,186	1,558
Nov	$4,029,582	1,927
Dec	$24,128,824	6,626
Grand Total	**$57,304,484**	**27,872**

Requirements:

1. Vendor will keep website updated daily to show all bills with unpaid balances contained in our daily file. Bills with a zero balance will not be selectable for payment.
2. Meet the current North Carolina Property Tax System (NCPTS) file format structure for ad valorem property tax payments received by vendor.
3. Vendor must provide a daily report to indicate expected payment files for same day funds deposited and sent to County Finance and Tax Collections.
4. Real-time web based reporting of transactions.
5. Fully PCI Compliant at all levels and can provide evidence of compliance along with conduct regular security audits and vulnerability assessments.
6. Be compliant with all applicable state, federal, and industry regulations, including NACHA, PCI-DSS, Red Flag rules, Federal E-Signature Act and any other applicable paper billing and payment laws.
7. Vendor will update website daily when county sends new file. (Additionally, please indicate vendor's ability to update website multiple times daily if needed).
8. Vendor must provide the file format necessary for the daily and monthly files that are to be provided by the County.
9. Accept major credit cards, branded debit cards, digital wallet, e-checks, and phone payments.
10. Vendor must be able to process full and partial refunds in the same method as the original payment (e.g. if original payment was made by credit card then refund is processed by credit card).
11. Vendor must inform the County of all planned changes to the website in advance of implementation.
12. Vendor should not allow a process which allows the same bill to be paid twice. Non-sufficient funds can only be charged to the specific check, not multiple items in one transaction.
13. Vendor must have an online bill search that accommodates Parcel Number, Bill Number, Owner #1 Name, Owner #2 Name, Sanitation Lien # (any alpha search should not be case sensitive, and bill number search should only require base bill number and provide all year's unpaid balances and full complete unique bill number for selection).
14. Vendor must have website and phone systems available for use 24/7/365 with minimal downtime for maintenance. Contact County staff if there are unavoidable issues with downtime due to weather events or unforeseen circumstances.
15. Vendor must include plan and amount of downtime anticipated for maintenance.
16. Have a disaster recovery/service interruption plan.
17. Vendor must provide procedure for unexpected issues with data integrity, service interruptions, and/or software functionality and include response/resolution timeline.
18. Have a method for the County to view and void payments that are not in processed status.
19. Meet all County minimum insurance requirements.

20. Provide process for handling disputes and chargebacks to include information regarding weekends and holidays in timeline.
21. Have a method for the County to search transactions, individually or by date range, and to export results in either csv or xlsx format.
22. Ability to absorb or pass through processing fees at the discretion of the department.
23. Provide enrollment capabilities and allow guest check-out.
24. Supporting recurring payments/automatic charges.
25. Deposit payments electronically into specified bank accounts by merchant ID.
26. Be compatible with existing software (including but not limited to Workday and NCPTS).
27. Allow for limits on transaction amount.
28. Upon mutual agreement, Vendor must be able to add in other County Department(s) electronic payment services during the contract period.
29. Access to merchant ID/department accounts and ability to view site, pull reports, search transactions, and make actions (e.g. voiding, refunding, etc.) restricted by user.
30. Vendor will provide responsive customer service to individuals with questions regarding payment submittal or other questions/concerns.
31. Cybersecurity Requirements:
    a. Data Encryption / Data in Flight - All data transmitted over networks (data in flight) must be encrypted to safeguard against eavesdropping and interception. The county mandates adherence to stringent standards for certificate management, and the encryption utilized for data in flight must conform to recognized protocols and encryption strengths. Acceptable methods include Secure File Transfer Protocol (SFTP), HyperText Transfer Protocol Secure (HTTPS), Secure Sockets Layer (SSL), and Advanced Encryption Standard (AES) with a minimum of 1024-bit encryption.
    b. Data Encryption / Data at Rest - All data stored within our systems (data at rest) must be encrypted to prevent unauthorized access, theft, and misuse. This encryption is crucial when data is moved between organizations to ensure continuous protection. The encryption methods should align with industry best practices and should be regularly reviewed to maintain efficacy against evolving threats.
    c. Secure Authentication and Authorization - Robust mechanisms for authentication and authorization are required to control access to sensitive data and systems. This includes multi-factor authentication (MFA), strong password policies, role-based access control (RBAC), and regular reviews of access privileges. The process should ensure that only authorized individuals have access to specific data and systems based on their roles and needs.
    d. Input Validation and Sanitization - All inputs into applications, systems, or databases must undergo thorough validation and sanitization to prevent common vulnerabilities like SQL injection, cross-site scripting (XSS), and others. This includes checking for data types, lengths, formats, and ranges. Sanitization involves removing or encoding unwanted characters that could be used in attacks.
    e. API Error Handling and Logging - APIs must have robust error handling to prevent leakage of sensitive information through error messages. Error handling should be designed to provide necessary information for debugging while masking details that could be exploited by attackers. Comprehensive logging of all API transactions is required for audit trails, which are crucial for identifying and investigating suspicious activities.
    f. Ongoing Vulnerability/Bug Test and Patch Management Practice - Regular vulnerability assessments and penetration testing should be conducted to identify and rectify security weaknesses. A systematic patch management practice must be in place to ensure that all software is kept up-to-date with the latest security patches. This process includes timely application of patches, verification of patch success, and documentation of the patching activity.
    g. Incident Response Plan - An Incident Response Plan (IRP) is required to effectively handle security incidents. The plan should outline roles and responsibilities, response procedures, communication protocols, and recovery steps. It must be regularly reviewed, updated, and tested through drills to ensure readiness in the event of a cybersecurity incident. The plan should also include procedures for legal compliance, data breach notifications, and post-incident analysis for continuous improvement of security postures.
    h. Audit - Regular audits are essential to ensure compliance with cybersecurity standards and to identify areas for improvement. Audits should encompass both internal and external assessments of security policies, procedures, systems, and controls. This includes:

i. Compliance Audits: Verifying adherence to applicable laws, regulations, and standards, such as PCI DSS, SOC2 and other applicable frameworks.
ii. System and Network Audits: Examining the security of physical and digital infrastructures to identify vulnerabilities.
iii. Access Control Audits: Reviewing user access rights to ensure adherence to the principle of least privilege.
iv. Data Protection Audits: Ensuring that data encryption, both in flight and at rest, is effectively implemented and managed.
v. Incident Response and Recovery Audits: Evaluating the effectiveness of incident response plans and recovery procedures post-implementation.
vi. Audit Trail and Logging Audits: Assessing the completeness, accuracy, and integrity of logs to ensure they provide a reliable record for forensics and analysis.

Scenario 2. Payment processor will provide services for point-of-sale payments.

FY23 Point-of-sale Transactions		
Month	Transaction Amount	Number of Transactions
Jan	$1,884,490	7,291
Feb	$526,280	6,508
Mar	$574,142	7,742
Apr	$427,731	7,190
May	$411,514	8,077
Jun	$381,533	7,774
Jul	$337,051	7,216
Aug	$1,013,073	8,217
Sep	$660,418	7,324
Oct	$828,683	7,166
Nov	$1,173,633	6,749
Dec	$3,195,924	7,178
Grand Total	**$11,414,472**	**88,432**

Requirements:

1. Vendor will keep website updated daily to show all bills with unpaid balances. The County expects to be able to see bills paid up to a 3 year period visible on the website. Bills with a zero balance will not be selectable for payment.
2. Meet the current North Carolina Property Tax System (NCPTS) file format structure for ad valorem property tax payments received by vendor.
3. Vendor must provide a daily report to indicate expected payment files for same day funds deposited and sent to County Finance and Tax Collections.
4. Real-time web based reporting of transactions by department, location, payment type.
5. Fully PCI Compliant at all levels and can provide evidence of compliance along with conduct regular security audits and vulnerability assessments.
6. Be compliant with all applicable state, federal, and industry regulations, including NACHA, PCI-DSS, Red Flag rules, Federal E-Signature Act and any other applicable paper billing and payment laws.

7. Vendor will update website daily when county sends new file. (Additionally, please indicate vendor's ability to update website multiple times daily if needed).
8. Vendor must provide the file format necessary for the daily and monthly files that are to be provided by the County.
9. Accept major credit cards, branded debit cards, digital wallet, e-checks, and phone payments.
10. Vendor must be able to process full and partial refunds in the same method as the original payment (e.g. if original payment was made by credit card then refund is processed by credit card).
11. Vendor should not allow a process which allows the same bill to be paid twice. Non-sufficient funds can only be charged to the specific check, not multiple items in one transaction.
12. Vendor must have an online bill search that accommodates Parcel Number, Bill Number, Owner #1 Name, Owner #2 Name, Sanitation Lien # (any alpha search should not be case sensitive, and bill number search should only require base bill number and provide all year's unpaid balances and full complete unique bill number for selection).
32. Vendor must supply all POS terminal/printers, which are compatible with the County hardware and software at the beginning of the contract and update as necessary. All equipment must be point to point encrypted and have encryption keys injected on the devices. Costs and fee schedules associated with the use of these devices must be communicated as part of the RFP response.
33. Vendor must have website and phone systems available for use 24/7/365 with minimal downtime for maintenance. Contact County staff if there are unavoidable issues with downtime due to weather events or unforeseen circumstances.
13. Vendor must include plan and amount of downtime anticipated for maintenance.
14. Have a disaster recovery/service interruption plan.
15. Vendor must provide procedure for unexpected issues with data integrity, service interruptions, and/or software functionality and include response/resolution timeline.
16. Have a method for the County to view and void payments that are not in processed status.
17. Meet all County minimum insurance requirements.
18. Provide process for handling disputes and chargebacks to include information regarding weekends and holidays in timeline.
19. Have a method for the County to search transactions, individually or by date range, and to export results in either csv or xlsx format.
20. Ability to absorb or pass through processing fees at the discretion of the department.
21. Deposit payments electronically into specified bank accounts by merchant ID.
22. Be compatible with existing software (including but not limited to Workday, Wasteworks, Accela, NCPTS) and able to interface using API. If an integration solution cannot be provided for the aforementioned software, please propose an alternate solution and the cost associated. The County reserves the right to add or remove software systems at any period during the contract term at no additional cost to the County.
23. Allow for limits on transaction amount.
24. Upon mutual agreement, Vendor must be able to add in other County Department(s) electronic payment services during the contract period.
25. Access to merchant ID/department accounts and ability to view site, pull reports, search transactions, and make actions (e.g. voiding, refunding, etc.) restricted by user.
26. Vendor will provide responsive customer service to individuals with questions regarding payment submittal or other questions/concerns.
27. Cybersecurity Requirements:
    a. Secure POS Devices, Including Chain of Custody - Secure handling and management of Point of Sale (POS) devices are crucial. This includes maintaining a documented chain of custody for all devices, certificates, and keys. It involves strict controls over the distribution, storage, and disposal of POS devices. Procedures should be in place for tracking device movement, managing updates, and handling device decommissioning to ensure the integrity and security of these devices throughout their lifecycle.
    b. Strong Cryptographic Technology - Utilize strong cryptographic technologies to secure data. This includes employing advanced encryption algorithms for protecting data in transit and at rest, ensuring the use of cryptographic keys is managed securely. Cryptographic methods should be regularly reviewed and updated to align with current best practices and standards in the industry.

c. Point-to-Point Encryption Over Unsecured Networks - Implement Point-to-Point Encryption (P2PE) for all data transmitted over unsecured networks, including public or wireless networks. This ensures that cardholder data is encrypted from the moment it is captured at the POS device and remains encrypted until it reaches the secure decryption environment. Where wireless technology is used, ensure that it is secured with robust encryption and authentication protocols.
d. Full Compliance with PCI-DSS and Subordinate Standards - Ensure full compliance with the Payment Card Industry Data Security Standard (PCI-DSS) and any applicable subordinate standards. This involves adhering to all relevant requirements for protecting cardholder data, maintaining a secure network, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.
e. Testing and Compliance Audit Program - Develop and maintain a testing and compliance audit program. This program should include regular internal and external audits to assess compliance with PCI-DSS and other relevant security standards. Additionally, conduct regular vulnerability assessments and penetration testing to identify and mitigate potential security weaknesses.
f. Incident Response Plan - Establish and maintain a comprehensive incident response plan tailored to address potential security incidents, including data breaches. This plan should outline roles, responsibilities, procedures for detection, reporting, and responding to security incidents. It should also include communication strategies for internal and external stakeholders, containment strategies, and processes for post-incident analysis and recovery.
g. Audit - Implement a thorough and systematic audit program to regularly assess and verify the security of the POS environment and related processes. This includes:
    i. Security Audits: Conducting comprehensive reviews of all POS systems and related technologies to ensure they meet security standards.
    ii. Chain of Custody Audits: Verifying the integrity of the chain of custody process for POS devices, certificates, and keys, ensuring all movements and changes are properly documented and authorized.
    iii. Compliance Audits: Ensuring adherence to PCI-DSS standards and any other relevant regulations. This should include periodic external audits by qualified security assessors (QSAs).
    iv. Cryptographic Audits: Reviewing the implementation and management of cryptographic technologies to ensure they remain strong and effective against current threats.
    v. Network Security Audits: Examining network configurations, especially those involving wireless technology, to ensure they are secure and compliant with best practices.
    vi. Incident Response Audits: Testing the effectiveness of the incident response plan through drills and reviews, ensuring the organization is prepared to handle and recover from security incidents effectively.

Scenario 3. Payment process will provide services for all payments not covered by 1 and 2 (non-property tax web-based payments, APIs, phones, etc.)

FY23 Other Transactions		
Month	Transaction Amount	Number of Transactions
Jan	$3,868,300	3,228
Feb	$2,528,634	2,344
Mar	$2,190,180	2,341
Apr	$2,611,541	2,404
May	$2,675,656	2,362
Jun	$2,783,938	2,175
Jul	$2,915,090	2,122

Aug	$3,320,554	2,257
Sep	$3,061,338	2,267
Oct	$3,081,280	2,258
Nov	$3,907,014	2,103
Dec	$3,261,463	2,192
Grand Total	**$36,204,986**	**28,053**

Requirements:

1. Vendor will keep website updated daily to show all bills with unpaid balances contained in our daily file. The County expects to be able to see bills paid up to a 3 year period visible on the website. Bills with a zero balance will not be selectable for payment.
2. Meet the current North Carolina Property Tax System (NCPTS) file format structure for ad valorem property tax payments received by vendor.
3. Vendor must provide a daily report to indicate expected payment files for same day funds deposited and sent to County Finance and Tax Collections. Report should indicate what was paid by Web or, IVR, and eCheck or credit/debit card.
4. Real-time web based reporting of transactions by department, location, payment type (web, IVR, ePay, etc.).
5. Fully PCI Compliant at all levels and can provide evidence of compliance along with conduct regular security audits and vulnerability assessments.
6. Be compliant with all applicable state, federal, and industry regulations, including NACHA, PCI-DSS, Red Flag rules, Federal E-Signature Act and any other applicable paper billing and payment laws.
7. Vendor will update website daily when county sends new file. (Additionally, please indicate vendor’s ability to update website multiple times daily if needed).
8. Vendor must provide the file format necessary for the daily and monthly files that are to be provided by the County.
9. Accept major credit cards, branded debit cards, digital wallet, e-checks, and phone payments.
10. Vendor must be able to process full and partial refunds in the same method as the original payment (e.g. if original payment was made by credit card then refund is processed by credit card).
11. Phone recorded message must be approved by the County.
12. Vendor must inform the County of all planned changes to phone recorded messages or to the website in advance of implementation.
13. Phone messages should only provide amount due for specific year of bill entered.
14. Phone payment needs to have option to add other bills to the payment transaction. Vendor should not allow a process which allows the same bill to be paid twice. Non-sufficient funds can only be charged to the specific check, not multiple items in one transaction.
15. Vendor must have an online bill search that accommodates Parcel Number, Bill Number, Owner #1 Name, Owner #2 Name, Sanitation Lien # (any alpha search should not be case sensitive, and bill number search should only require base bill number and provide all year's unpaid balances and full complete unique bill number for selection).
16. Vendor must have website and phone systems available for use 24/7/365 with minimal downtime for maintenance. Contact County staff if there are unavoidable issues with downtime due to weather events or unforeseen circumstances.
17. Vendor must include plan and amount of downtime anticipated for maintenance.
18. Have a disaster recovery/service interruption plan.
19. Vendor must provide procedure for unexpected issues with data integrity, service interruptions, and/or software functionality and include response/resolution timeline.
20. Have a method for the County to view and void payments that are not in processed status.
21. Meet all County minimum insurance requirements.
22. Provide process for handling disputes and chargebacks to include information regarding weekends and holidays in timeline.

23. Have a method for the County to search transactions, individually or by date range, and to export results in either csv or xlsx format.
24. Telephone payments (IVR) in both English and Spanish.
25. Ability to absorb or pass through processing fees at the discretion of the department with the option to be conditional (e.g. IVR, POS, online, etc.).
26. Provide enrollment capabilities and allow guest check-out.
27. Supporting recurring payments/automatic charges.
28. Deposit payments electronically into specified bank accounts by merchant ID.
29. Be compatible with existing software (including but not limited to Workday, Wasteworks, Accela, NCPTS) and able to interface using API. If an integration solution cannot be provided for the aforementioned software, please propose an alternate solution and the cost associated. The County reserves the right to add or remove software systems at any period during the contract term at no additional cost to the County.
30. Allow for limits on transaction amount.
31. Upon mutual agreement, Vendor must be able to add in other County Department(s) electronic payment services during the contract period.
32. Access to merchant ID/department accounts and ability to view site, pull reports, search transactions, and make actions (e.g. voiding, refunding, etc.) restricted by user.
33. Vendor will provide responsive customer service to individuals with questions regarding payment submittal or other questions/concerns.
34. Cybersecurity Requirements: In addition to the requirements identified above, API security has additional requirements related to protecting PCI-DSS information, including:
    a. Authentication and Authorization: Enforce strong authentication and authorization for all API access. Use secure methods like OAuth, API keys, or client certificates to ensure that only authorized applications and users can access the API.
    b. Encryption: Ensure that all data transmitted via APIs is encrypted using strong encryption standards such as TLS.
    c. Input Validation and Sanitization: Implement rigorous input validation and sanitization to prevent common vulnerabilities like SQL injection and cross-site scripting (XSS).
    d. Rate Limiting and Throttling: Apply rate limiting and throttling to APIs to prevent abuse and potential denial-of-service attacks.
    e. API Gateway Security: Use API gateways to manage, monitor, and secure API traffic. This includes implementing policies for request/response transformations, CORS management, and IP whitelisting.
    f. Logging and Monitoring: Maintain comprehensive logs of all API activity and monitor these logs for suspicious activities. This is critical for early detection of potential security incidents.
    g. Regular Security Testing: Conduct regular security assessments of APIs, including penetration testing and vulnerability scanning, to identify and remediate potential security issues.
    h. Version Management: Properly manage API versions, ensuring that outdated APIs with known vulnerabilities are deprecated in a controlled manner.

6.0 GENERAL TERMS AND CONDITIONS

1. **READ, REVIEW AND COMPLY:** It shall be the Vendor's responsibility to read this entire document, review all enclosures and attachments, and any addenda thereto, and comply with all requirements specified herein, regardless of whether appearing in these Instructions to Vendors or elsewhere in this RFP document.

2. **LATE PROPOSALS**: Late proposals, regardless of cause, will not be considered, and will automatically be disqualified from further consideration. It shall be the Vendor's sole responsibility to ensure the timely submission of proposals.

3. **ACCEPTANCE AND REJECTION:** Buncombe County reserves the right to reject any and all proposals, to waive any informality in proposals and, unless otherwise specified by the Vendor, to accept any item in the proposal.

4. **INFORMATION AND DESCRIPTIVE LITERATURE:** If required elsewhere in this proposal, each Vendor shall submit with its proposal any sketches, descriptive literature and/or complete specifications covering the products

and Services offered. Reference to literature submitted with a previous proposal or available elsewhere will not satisfy this provision. Failure to comply with these requirements shall constitute sufficient cause to reject a proposal without further consideration.

5. **SUSTAINABILITY**: To support the sustainability efforts of the State of North Carolina we solicit your cooperation in this effort. Pursuant to Executive Order 156 (1999), it is desirable that all print responses submitted meet the following:

   - All copies of the proposal are printed double sided.
   - All submittals and copies are printed on recycled paper with a minimum post-consumer content of 30%.
   - Unless absolutely necessary, all proposals and copies should minimize or eliminate use of non-recyclable or non-reusable materials such as plastic report covers, plastic dividers, vinyl sleeves, and GBC binding. Three-ringed binders, glued materials, paper clips, and staples are acceptable.
   - Materials should be submitted in a format which allows for easy removal, filing and/or recycling of paper and binder materials. Use of oversized paper is strongly discouraged unless necessary for clarity or legibility.

6. **HISTORICALLY UNDERUTILIZED BUSINESSES:** Buncombe County is committed to retaining Vendors from diverse backgrounds, and it invites and encourages participation in the procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. In particular, the County encourages participation by Vendors certified by the State Office of Historically Underutilized Businesses, as well as the use of HUB-certified vendors as subcontractors on County contracts.

7. **INELIGIBLE VENDORS:** As provided in G.S. 147-86.59 and G.S. 147-86.82, the following companies are ineligible to contract with the State of North Carolina or any political subdivision of the State: a) any company identified as engaging in investment activities in Iran, as determined by appearing on the Final Divestment List created by the State Treasurer pursuant to G.S. 147-86.58, and b) any company identified as engaged in a boycott of Israel as determined by appearing on the List of restricted companies created by the State Treasurer pursuant to G.S. 147-86.81. A contract with the Buncombe County by any company identified in a) or b) above shall be void *ab initio*.

8. **CONFIDENTIAL INFORMATION:** To the extent permitted by applicable statutes and rules, the County will maintain as confidential trade secrets in its proposal that the Vendor does not wish disclosed. As a condition to confidential treatment, each page containing trade secret information shall be identified in boldface at the top and bottom as "CONFIDENTIAL" by the Vendor, with specific trade secret information enclosed in boxes, marked in a distinctive color or by similar indication. Cost information shall not be deemed confidential under any circumstances. Regardless of what a Vendor may label as a trade secret, the determination whether it is or is not entitled to protection will be determined in accordance with G.S. 132-1.2. Any material labeled as confidential constitutes a representation by the Vendor that it has made a reasonable effort in good faith to determine that such material is, in fact, a trade secret under G.S. 132-1.2. Vendors are urged and cautioned to limit the marking of information as a trade secret or as confidential so far as is possible. If a legal action is brought to require the disclosure of any material so marked as confidential, the County will notify Vendor of such action and allow Vendor to defend the confidential status of its information.

9. **MISCELLANEOUS:** Any gender-specific pronouns used herein, whether masculine or feminine, shall be read and construed as gender neutral, and the singular of any word or phrase shall be read to include the plural and vice versa.

10. **INFORMAL COMMENTS:** Buncombe County shall not be bound by informal explanations, instructions or information given at any time by anyone on behalf of the County during the competitive process or after award. The County is bound only by information provided in writing in this RFP and in formal Addenda issued through IPS.

11. **COST FOR PROPOSAL PREPARATION:** Any costs incurred by Vendor in preparing or submitting offers are the Vendor's sole responsibility; Buncombe County will not reimburse any Vendor for any costs incurred or associated with the preparation of proposals.

12. **AVAILABILITY OF FUNDS:** Any and all payments to the Vendor shall be dependent upon and subject to the availability of funds to the agency for the purpose set forth in The Contract.

13. **SITUS AND GOVERNING LAWS:** This Contract is made under and shall be governed and construed in accordance with the laws of the State of North Carolina, without regard to its conflict of laws rules, and within which State all matters, whether sounding in Contract or tort or otherwise, relating to its validity, construction, interpretation and enforcement shall be determined.

14. **PAYMENT TERMS:** If a payment schedule is not part of The Contract then payment terms will be Net 30 days after receipt of a correct invoice or acceptance of goods, whichever is later.

15. **NON-DISCRIMINATION:** The Vendor will take necessary action to comply with all Federal and State requirements concerning fair employment and employment of people with disabilities, and concerning the treatment of all employees without regard to discrimination on the basis of any prohibited grounds as defined by Federal and State law.

16. **ADVERTISING:** Vendor agrees not to use the existence of The Contract or the name of Buncombe County as part of any commercial advertising or marketing of products or Services. A Vendor may inquire whether the County is willing to act as a reference by providing factual information directly to other prospective customers.

17. **INSURANCE:**

    COVERAGE - During the term of the Contract, the Vendor at its sole cost and expense shall provide commercial insurance of such type and with such terms and limits as may be reasonably associated with the Contract. As a minimum, the Vendor shall provide and maintain the following coverage and limits:

    Commercial General Liability insurance in an amount not less than $1,000,000 each occurrence/$2,000,000 annual aggregate. Coverage shall not contain any endorsement(s) excluding nor limiting Product/Completed Operations or Contractual Liability.

    Business Automobile Liability insurance covering all owned, non-owned, and hired vehicles with a minimum combined single limit of $1,000,000 each occurrence and shall include uninsured/underinsured motorist coverage per NC General Statute 20-279-21.

    Workers Compensation coverage at the statutory limits in compliance with applicable State and Federal laws. Supplier shall ensure that any subcontractors also have workers compensation coverage at the statutory limits.

    Employer's Liability coverage with minimum limits of $500,000 each accident and $500,000 each employee disease.

    Vendor shall agree these General Conditions constitute an insured contract and shall name Buncombe County as an additional insured under the Commercial General Liability policy. Before commencing work and for any subsequent renewals, Vendor shall furnish the County with certificates of insurance evidencing the above coverages and amounts on an approved form. Vendor hereby grants the County a waiver of any right of subrogation which any insurer of said Vendor may acquire against the County by virtue of payment of any loss under such insurance. Vendor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation. Each insurance policy required above shall state that coverage shall not be canceled, except with written notice to the County and delivered in accordance with the policy provisions. All insurance shall be procured from reputable insurers authorized and qualified to do business in North Carolina and in a form acceptable to the County. The limits of coverage under each insurance policy maintained by the Vendor shall not be interpreted as limiting the Supplier's liability and obligations. Nothing in this section is intended to affect or abrogate Buncombe County's governmental immunity.

18. **GENERAL INDEMNITY:** The Vendor shall hold and save Buncombe County, its officers, agents, and employees, harmless from liability of any kind, including all claims and losses accruing or resulting to any other person, firm, or corporation furnishing or supplying work, Services, materials, or supplies in connection with the performance of The Contract, and from any and all claims and losses accruing or resulting to any person, firm, or corporation that may be injured or damaged by the Vendor in the performance of The Contract and that are attributable to the negligence or intentionally tortious acts of the Vendor provided that the Vendor is notified in writing within 30 days from the date that the County has knowledge of such claims. The Vendor represents and warrants that it shall make no claim of any kind or nature against the County's agents who are involved in the delivery or processing of Vendor deliverables or Services to the County. The representation and warranty in the preceding sentence shall survive the termination or expiration of The Contract.

19. **CONFLICT OF INTEREST:** Per N.C. General Statute 14-234, no public officer or employee who is involved in making or administering a contract on behalf of a public agency may derive a direct benefit from the contract.
The statute defines "public officer" as an individual who is elected or appointed to serve or represent a public agency, other than an employee or independent contractor of a public agency.
A public officer or employee is involved in administering a contract if he or she oversees the performance of the contract or has authority to make decisions regarding the contract or to interpret the contract; or if he or she participates in the development of specifications or terms or in the preparation or award of the contract. A public officer is also involved in making a contract if the board, commission, or other body of which he or she is a member takes action on the contract, whether or not the public officer actually participates in that action, unless the contract is approved under an exception to this section under which the public officer is allowed to benefit and is prohibited from voting.
There is a conflict of interest when a public officer or employee derives a direct benefit from a contract if the person or his or her spouse: (i) has more than a ten percent (10%) ownership or other interest in an entity that is a party to the contract; (ii) derives any income or commission directly from the contract; or (iii) acquires property under the contract.

20. **CONFIDENTIALITY:** Any County information, data, instruments, documents, studies or reports given to or prepared or assembled by or provided to the Vendor under The Contract shall be kept as confidential, used only for the purpose(s) required to perform The Contract and not divulged or made available to any individual or organization without the prior written approval by Buncombe County.

21. **COMPLIANCE WITH LAWS:** Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and its performance in accordance with The Contract, including those of federal, state, and local agencies having jurisdiction and/or authority.

22. **ENTIRE AGREEMENT:** This RFP and any documents incorporated specifically by reference represent the entire agreement between the parties and supersede all prior oral or written statements or agreements. This RFP, any addenda hereto, and the Vendor's proposal are incorporated herein by reference as though set forth verbatim.

    All promises, requirements, terms, conditions, provisions, representations, guarantees, and warranties contained herein shall survive the contract expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable Federal or State statutes of limitation.

23. **AMENDMENTS:** This Contract may be amended only by a written amendment duly executed by the County and the Vendor.

24. **NO WAIVER:** Notwithstanding any other language or provision in The Contract, nothing herein is intended nor shall be interpreted as a waiver of any right or remedy otherwise available to the County under applicable law. The waiver by the County of any right or remedy on any one occasion or instance shall not constitute or be interpreted as a waiver of that or any other right or remedy on any other occasion or instance.

25. **FORCE MAJEURE:** Neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

26. **SOVEREIGN IMMUNITY:** Notwithstanding any other term or provision in The Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of sovereign immunity or state or federal constitutional provision or principle that otherwise would be available to the County under applicable law.

27. **DATA BREACH NOTIFICATION:**

a) Within one (1) day (twenty-four (24) hours of discovering System Breach or Data Breach, information that leads the Contractor to reasonably believe that a Breach may have occurred, it shall alert the County that Systems/Data may have been breached and specifics known at the time.
b) The Notification should include sufficient information for the County to understand the nature of the Breach and provide a starting point for County IT and Privacy resources to respond.
c) The Notification shall not include any specific regulated or sensitive information.
d) Send notification to: securityincident@buncombecounty.org
e) Include the following information as part of the Notification:
    1. General Incident Information:
        - Date and time of incident detection and notification
        - Incident detector's name and contact information
        - Physical and Logical Location of the incident
        - Systems, applications, services, data, and networks possibly at risk
        - Type of incident detected
        - General description of incident
        - Names and contact information of others involved
        - Any actions taken since incident discovery
        - Any additional relevant information known at the time
f) The Contractor shall supplement the information contained in the Notification as it becomes available and cooperate with County Incident Response.
g) Additional requirements will be required for Regulated data types, including ePHI, CJI, PCI, FTI, etc. as defined in their associated regulatory frameworks (ex. ePHI/HIPAA will require a Business Associates Agreement).