

Third Party Due Diligence Questionnaire

|  |  |
| --- | --- |
| Name of Company |  |
| DBA or Associated Trade Names |  |
| Physical Street Address |  |
| Mailing Address (if applicable) |  |
| Business Tax ID |  |
| Company Website |  |
| Primary Nature of the Business |  |
| Purpose of Relationship to CNB |  |

|  |  |  |  |
| --- | --- | --- | --- |
| State of Organization | |  | |
| Date of Organization  Number of Years in Business | |  | |
| Ownership Structure (Corporation, Limited Liability Company, Partnership, etc) | |  | |
| Number of Locations and all Addresses of Operations | |  | |
| Number of Employees | |  | |
| Number of Clients | |  | |
| Contact Person |  | | | |
| Contact Phone Number | | |  | |
| Contact Email |  | | | |

Due Diligence Accreditation Questionnaire

Please complete all sections, including all requested documentation as attachments to this questionnaire. If you need additional space for explanation, please attach.

|  |  |  |
| --- | --- | --- |
| **Section I -- Financial & Corporate Information** | | |
| **Item Number** | **Question** | **Response** |
|  | Has the company recently merged or acquired another entity or is it in the process of merging or acquiring another entity?  If Yes, provide a summary of the transaction, if disclosure is appropriate. |  |
|  | Have you had any economic loss due to fraud to date?  If yes, please describe. |  |
|  | Do you have any processes in place to detect suspicious activity and minimize risk? If yes, please specify. |  |
|  | Does your company have outstanding obligations to contract third parties that might materially impact your financial position? If yes, please explain. |  |
|  | Describe your insurance coverage including general liability, crime, errors & omissions, worker’s compensation and data security insurance. |  |
|  | Have any claims been asserted against your company that could have a materially adverse effect on your company’s financial position? If yes, please explain. |  |
|  | Are there now, or have there been within the past three (3) years…  i.) Any inquiries regarding consumer protection laws or unfair and deceptive trade practices?  If Yes, attach an explanation and final disposition.  ii.) Any governmental, regulatory or administrative investigations, proceedings, complaints or lawsuits commenced against the company or any or its officers or employees challenging the way in which it conducts business including, without limitation, the manner in which it fulfills obligations to persons who purchase its services or products? |  |
|  | Are there now or have there been within the past three (3) years…  Any complaints made by customers about the company to any regulatory authority or consumer complaint agency by whatever name?  If Yes, attach an explanation and final disposition. |  |

|  |  |  |
| --- | --- | --- |
| **Section II -- Systems & Data Security** | | |
| **Item Number** | **Question** | **Response** |
|  | Does the company’s information security program address administrative, technical and physical safeguards to protect the security, confidentiality and integrity of all nonpublic personal information? This includes any records, data, and file whether paper, electronic or other forms that may be maintained. If not, specify. | Yes |
|  | How is nonpublic personal information stored?  Who has access to this information? | Our office is locked and monitored by a security system. Only the employees are allowed keys. |
|  | Identify the method(s) and connection(s) used by the Bank for sending secure information (email, SMTP, etc…?). | The Bank has not made this information available to us. |
|  | What security system(s) do you support? | We use Guardian Security Systems for office security and all workstations require password access |
|  | Have you ever experienced a security breach in your system?  If yes, please describe. | No |
|  | Please describe your data center facility(s). | N/A |
|  | Do you track Service Levels? If yes, what are your benchmarks? | No |

|  |  |  |
| --- | --- | --- |
|  | Please describe your information security training programs for new and existing employees. | Employees understand the sensitive nature of keeping our data secure. Meetings and correspondence are used to enforce this concept. |

|  |  |  |
| --- | --- | --- |
| **Section III -- Privacy Policy** | | |
| **Item Number** | **Question** | **Response** |
|  | Do you have a corporate privacy policy? | yes |
|  | Is there a program in place designed to teach employees to recognize and respond to fraudulent attempts to obtain non-public personal information and report any attempt to management? | yes |
|  | Are employees held accountable to ensure that all non-public information is protected? Describe how? (i.e. do you use non-disclosure agreements or do you apply disciplinary measures for any violation or breach to the policy?) | Yes |
|  | Are employee exit procedures in place to verify that customer nonpublic information is no longer available to terminated employees? | yes |

|  |  |  |
| --- | --- | --- |
| **Section IV -- Third Party Compliance** | | |
| **Item Number** | **Question** | **Response** |
| 1. | What functions are outsourced to third parties? Please list third parties performing critical functions including those third parties used for storing secure/nonpublic customer information. | We utilize a software platform designed to automate marketing campaigns. See next question. |
| 2. | Identify all third party software. | Mindfire Studio |
| 3. | Please describe your due diligence process for engaging and monitoring third parties that perform critical functions. (IT service provider, critical vendors, vendors with access to customer information, collection agencies, etc. | See attached questionnaire |

|  |  |  |
| --- | --- | --- |
| **Section V -- Audit** | | |
| **Item Number** | **Question** | **Response** |
| 1. | Has your company been audited in the past year for:   1. Privacy 2. Compliance 3. Information Security 4. Disaster Recovery 5. Operations 6. Technology | **No** |
| 2. | Have these audits resulted in:   1. material internal audit findings 2. material external audit findings 3. material regulatory findings 4. SSAE 16 (or equivalent) exceptions | N/A |
| 3. | Does your company use or continue to use an internal control mechanism with the responsibility to identify and track resolution of outstanding internal audit, external audit or regulatory examination issues? | **N/A** |
| 4. | Has your company reported all material outstanding issues to your organization’s audit committee and CEO? | N/A |
| 5. | Provide a copy of a current SSAE-16 SOC2 and/or PCI Compliance, if applicable. (If not available please provided most recent Audit of Controls) | N/A |
| 6. | Describe your company’s penetration testing procedures. | n/a |
| 7. | Describe your company’s vulnerability testing procedures. | n/a |

|  |  |  |
| --- | --- | --- |
| **Section VI – Risk Management** | | |
| **Item Number** | **Question** | **Response** |
| 1. | Does your company have a written policy and program for risk assessment and risk mitigation? | yes |

|  |
| --- |
| **Section VII – Requested Items** |
| **Provide the following policies/procedures:**   * Code of Ethics policy/procedures * Corporate Privacy policy and procedures * Information Security Policy/Procedures meeting objectives, regulations, and guidelines of GLBA (including Employee Exit Procedures) * Background check procedures * Insurance policies * Past 3 years financials * Ownership information |

|  |  |  |  |
| --- | --- | --- | --- |
| **Section VIII – Signature of Company Officer** | | | |
| By signing below, I certify that the above application and attachments were completed to the best of my knowledge. | | | |
| 1. Printed Name of Company Officer | 2. Signature of Company Officer | 3. Title of Company Officer | 4. Date |