POLICIES & PROCEDURES MANUAL
OF
[INSERT VENDOR NAME]

[INSERT DATE]

TABLE OF CONTENTS

It is the responsibility of all employees and agents to review, understand, and ensure compliance with the following policies and procedures as a condition of their employment or contract:

1.0 Criminal Background Checks

(a) [INSERT VENDOR NAME] will perform a legally permissible criminal background check prior to employment on every prospective full- or part-time employee who will have access to Consumer Data to determine the following:

(1) Whether the prospective employee has been convicted of any criminal felony involving dishonesty, fraud, deceit, misrepresentation, or any misappropriation of confidential data or information; and

(2) Whether the prospective employee has been charged with any crime involving dishonesty, fraud, deceit, misrepresentation, or any misappropriation of confidential data or information such that the facts alleged support a reasonable conclusion that the acts were committed and that the nature, timing, and circumstances of the acts may place consumers in jeopardy.

(b) The [President/Human Resources Department] shall maintain a list of positions that have access to consumer financial data.

(c) The [President/Human Resources Department] shall maintain the results of the criminal background checks in a secured location with access limited to [INSERT JOB TITLE(S)].

(d) Employment decisions are made on a case-by-case basis based on the totality of the application and capabilities of the prospective employee. The results of a criminal background check may have the following consequences on the offer of employment:

[INSERT CONSEQUENCES, IF ANY, AND THE CRITERIA FOR THOSE CONSEQUENCES – DRAFTER IS ENCOURAGED TO SEEK ADVICE OF EMPLOYMENT COUNSEL FROM THEIR JURISDICTION TO DETERMINE LEGALITY OF POLICY AND IMPACT ON EMPLOYMENT]

Basis of Policy: RMAI Certification Program, Appendix B, Standard # 102 (v8.0)
[List any other basis]

2.0 Data Security

[**OPTION # 1** – THE FOLLOWING IS A SAMPLE POLICY IF YOUR COMPANY DOES NOT REVIEW, STORE, TRANSFER, OR OTHERWISE COME INTO CONTACT WITH CLIENT'S CONSUMER DATA OR DOCUMENTS.]

[INSERT VENDOR NAME] does not review, store, transfer, or otherwise come into contact with any client's consumer data or documents as part of its services. If any employee and/or agent intentionally or unintentionally reviews, stores, transfers, or otherwise comes into contact with any client's consumer data or documents, he or she is required to immediately inform [INSERT JOB TITLE]. The [INSERT JOB TITLE] shall document the violation of the policy, inform the purchaser and seller of the violation, and work with the Chief Compliance Officer to ensure that policies and procedures are adopted to prevent a similar violation from occurring in the future.

OR

[**OPTION # 2** – THE FOLLOWING IS A SAMPLE POLICY IF YOUR COMPANY DOES REVIEW, STORE, TRANSFER, OR OTHERWISE COME INTO CONTACT WITH CLIENT'S CONSUMER DATA OR DOCUMENTS.]

(a) [INSERT VENDOR NAME] requires all of its employees and/or agents to adhere to the following requirements in order to ensure the protection of consumer data from reasonable foreseeable internal and external risks:

(1) **STORAGE OF PHYSICAL DATA & DOCUMENTS** – The following procedures shall be taken to ensure the safe and secure storage of physical data and documents that contain personally identifiable information of a confidential nature:

[LIST THE PROCEDURES THE EMPLOYEE/AGENT SHOULD FOLLOW]

(2) **STORAGE OF ELECTRONIC DATA & DOCUMENTS** – The following procedures shall be taken to ensure the safe and secure storage of electronic data and documents that contain personally identifiable information of a confidential nature:

[LIST THE PROCEDURES THE EMPLOYEE/AGENT SHOULD FOLLOW]

(3) **ANTIVIRUS SOFTWARE** – The following procedures shall be followed to ensure that the company uses, maintains, and regularly updates antivirus software on company computers that have access to consumer data:

[LIST THE PROCEDURES THE EMPLOYEE/AGENT SHOULD FOLLOW]

(4) **SYSTEM FIREWALLS** -- The following procedures shall be followed to ensure that the company implements and maintains a network security system firewall for the monitoring of incoming and outgoing system network traffic:

[LIST THE PROCEDURES THE EMPLOYEE/AGENT SHOULD FOLLOW]

(5) **MARKETING & ADVERTISEMENT** – The following procedures shall be followed to ensure receivable portfolios are not advertised or marketed in such a manner that would allow consumer data and original account level documentation to be available to or accessible by the public:

[LIST THE PROCEDURES THE EMPLOYEE/AGENT SHOULD FOLLOW]

(6) **DATA & DOCUMENT DESTRUCTION** – The following procedures shall be used to determine the appropriate timeframe and methodology to safely and securely destroy specific categories of data and documents and to ensure those timelines and methodologies are compliant with applicable laws and contractual obligations:

[LIST THE PROCEDURES THE EMPLOYEE/AGENT SHOULD FOLLOW]

(7) **DATA BREACH** – The following action plan shall be followed if a data breach is discovered that is in accordance with applicable laws and regulations and contains any required disclosures of such breach:

[INSERT ACTION PLAN]

(b) The Chief Compliance Officer shall perform or have performed an annual risk assessment of the company's protection of consumer data from reasonably foreseeable internal and external risks on or before the [INSERT NUMBER] day of [INSERT MONTH] of every year. The results of the risk assessment along with any recommendations for improvements to the data security policy shall be provided to [INSERT JOB TITLE OR GOVERNING BOARD/COMMITTEE] within 30 days of the assessment. [INSERT JOB TITLE OR GOVERNING BOARD/COMMITTEE] shall review the results of the risk assessment and recommendations for improvements and authorize adjustments to the policy, as appropriate.

Basis of Policy: RMAI Certification Program, Appendix B, Standard # 105 (v8.0)
[List any other basis]

3.0 Employee Training Programs

[INSERT VENDOR NAME] requires all of its employees and/or agents to participate in mandatory annual employee training program(s) that educate its employees and/or agents on: (i) the policies and procedures contained in this manual, (ii) RMAI certification standards, (iii) laws and regulations, and (iv) client-mandated compliance requirements. Each training program shall indicate the possible consequences for failing to comply with them.

The [INSERT JOB TITLE] shall document on or before the [INSERT NUMBER] day of [INSERT MONTH] of each year the names of employees who have and have not taken the required annual employee training within the prior 12 months. The [INSERT JOB TITLE] shall contact any employee identified as not having completed his or her training and arrange for such training within 30 days.

Basis of Policy: RMAI Certification Program, Appendix B, Standard # 103 (v8.0)
[List any other basis]

4.0 Vendor Management

[INSERT VENDOR NAME] requires its employees and/or agents who are responsible for the negotiation of contracts with vendors to adhere to the following policies and procedures:

(1) [INSERT VENDOR MANAGEMENT POLICIES WITH DEFINED DUE DILIGENCE AND/OR AUDIT CONTROLS]

(2) [INSERT VENDOR MANAGEMENT PROCEDURES WITH DEFINED DUE DILIGENCE AND/OR AUDIT CONTROLS]

(3) The Chief Compliance Officer shall perform or have performed an annual assessment of the company's vendor management policies and procedures and prior year contracts to confirm compliance as well as identify areas which may require strengthening based on prior experiences and best practices. This annual assessment shall take place on or before the [INSERT NUMBER] day of [INSERT MONTH] of every year. The results of the assessment along with any recommendations for improvements to the vendor management policies and procedures shall be provided to [INSERT JOB TITLE OR GOVERNING BOARD/COMMITTEE] within 30 days of the assessment. [INSERT JOB TITLE OR GOVERNING

BOARD/COMMITTEE] shall review the results of the assessment and recommendations for improvements and authorize adjustments to the policy, as appropriate.

(4) The Chief Compliance Officer shall perform or have performed an annual assessment of the company's third party vendors to determine whether they continue to meet or exceed the requirements and expectations of the company. As part of the annual assessment, the company may need to perform additional due diligence, including by way of example rather than limitation, confirmation of certification status, vendor audits, review of policies and procedures maintained by vendors, and review of consumer complaints related to the vendor. This annual assessment shall take place on or before the [INSERT NUMBER] day of [INSERT MONTH] of every year. The results of the assessment along with any recommendations for improvements to the vendor management policies and procedures shall be provided to [INSERT JOB TITLE OR GOVERNING BOARD/COMMITTEE] within 30 days of the assessment. [INSERT JOB TITLE OR GOVERNING BOARD/COMMITTEE] shall review the results of the assessment and recommendations for improvements and authorize adjustments to the policy, as appropriate.

Basis of Policy: *RMAI Certification Program, Appendix B, Standard # 107 (v8.0)*
[List any other basis]

v.20200508