CATIC FINANCIAL COMPREHENSIVE WRITTEN INFORMATION SECURITY PLAN

Effective November 19, 2013

Updated 2/28/2018, 3/27/2018, 11/14/2019, 9/1/2020, 10/15/2020, 03/10/2021

CATIC Financial Headquarters

101 Corporate Place, Rocky Hill, Connecticut 06067 T: (860) 257-0606 Toll Free: (800) 676-0619 F: (860) 563-4833

CATIC FINANCIAL COMPREHENSIVE WRITTEN INFORMATION SECURITY PLAN

I. OBJECTIVE:

The objective of CATIC Financial and its affiliates (collectively the "Companies" or the “Company”), in developing and implementing this comprehensive written information security plan ("Plan"), is to create effective administrative, technical and physical safeguards for the security and confidentiality of personal information of consumers and employees of the State of Connecticut (Public Act 19-117, § 230), of the Commonwealth of Massachusetts (201 CMR 17.00), of the State of New Hampshire (NH Rev. Stat. §420:P), of the State of New York (23 NYCRR 500), of the State of Rhode Island (RIGL § 11-49.3-1) and for any other applicable state for compliance with any and all applicable laws and regulations therein (collectively “the Regulations”). The Plan sets forth the Companies’ procedure for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting such personal information. For purposes of this Plan, examples of "personal information" include, but are not limited to, an individual’s name, like first name and last name or first initial and last name, or a number, personal mark, or other identifier that can be used to identify such individual, in combination with, for example, any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number, state-issued identification card number or tribal identification number; (c) financial account number, or credit or debit card number; (d) any security code, access code, personal identification number or password, that would permit access to an individual’s financial account; (e) medical or health insurance information; (f) username or email address in combination with security code, access code or password or security question and answer that would permit access to an online account; (g) biometric records; or (h) any other information that may be required by law; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public. The Company retains personal information for as long as is needed to fulfill its stated purpose.

II. PURPOSES:

The purpose of the Plan is to:

a. Protect the security and confidentiality of personal information;

b. Protect against any anticipated threats or hazards to the security or integrity of such information; and

c. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE:

In formulating and implementing the Plan, the Company has and will continue to (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (3) evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks; (4) design and implement a plan that puts safeguards in place to minimize those risks, consistent with the Regulations; and (5) regularly monitor the effectiveness of those safeguards.

IV. DATA SECURITY COORDINATOR:

The Company has designated Richard Hogan, Esq. to implement, supervise and maintain the Plan. That designated employee (the "Data Security Coordinator") will be responsible for:

a. Implementation of the Plan;

b. Training employees;

c. Regular testing of the Plan's safeguards;

d. Evaluating the ability of third-party service providers to comply with the Regulations in the handling of personal information for which we are responsible;

e. Reviewing the scope of the security measures in the Plan at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information, and modifying the Plan accordingly;

f. Conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information, on the elements of the Plan. All attendees at such training sessions will certify their attendance at the training and their familiarity with the Company's requirements for the protection of personal information; and

g. Taking appropriate action in response to the misuse of personal information by third parties.

V. INTERNAL RISKS:

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures will be implemented.

Internal Threats

- A copy of the Plan will be distributed to each employee who will, upon receipt of the Plan, acknowledge in writing that he/she has received a copy of the Plan.

- There will be training of employees on the detailed provisions of the Plan.

- Employment contracts will be amended (1) to require all employees to comply with the provisions of the Plan, and to prohibit any nonconforming use of personal information during or after employment; and (2) to provide that disciplinary action will be taken for violation of security provisions of the Plan. (*The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the personal information affected by the violation.*)

- The amount of personal information collected will be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to comply with other state or federal regulations.

- Access to records containing personal information will be limited to those persons who are reasonably required to know such information in order to accomplish our legitimate business purpose or to enable us to comply with the Regulations.

- Electronic access to user identification after multiple unsuccessful attempts to gain access will be blocked.

- All security measures will be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal information. The Data Security Coordinator will be responsible for this review and will fully apprise management of the results of that review and any recommendations for improved security arising out of that review.

- Terminated employees will return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).

- A terminated employee's physical and electronic access to personal information will be blocked. Such terminated employee will surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information will be disabled;

- His/her voicemail access, e-mail access, internet access, and passwords will be invalidated. The Data Security Coordinator or his designee will maintain a secured master list of all lock combinations, passwords and keys.

- Current employees' user-IDs and passwords will be changed periodically.

- Access to personal information will be restricted to active users and active user accounts only.

- Employees are encouraged to report any suspicious or unauthorized use of personal information.

- Whenever there is an incident that requires notification under the Regulations there will be a post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible.

- Employees will not keep open records containing personal information on their desks when they are not at their desks.

- At the end of the work day, all files and other records containing personal information will be secured in a manner that is consistent with the Plan.

- Employees are prohibited from removing personal information from the Company’s premises or systems, unless authorized to remove by the Company as a part of the employee’s work functions.

- Each department will develop processes and guidelines (bearing in mind the business needs of that department) that put in place reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to

such records in that department is to be restricted; and each department will store such records and data in locked or secure facilities, drawers, storage areas or containers.

- Access to electronically stored personal information will be electronically limited to those employees having a unique log-in ID; and re-log-in will be required when a computer has been inactive for more than a few minutes.

- Employees will encrypt their electronic communications of personal information through applications identified by the Information Technology Department of the Company.

- Visitors' access will be restricted to one entry point for each building in which personal information is stored, and visitors will sign in and wear a plainly visible "GUEST" badge or tag. Visitors will not be permitted to visit unescorted any area within our premises that contains personal information.

- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information will be disposed of only in a manner that complies with the Regulations.

VI. EXTERNAL RISKS:

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures will be implemented.

External Threats

- There will be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing and/or storing personal information.

- There will be reasonably up-to-date versions of system security agent software which will include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information.

- To the extent technically feasible, all personal information stored on laptops or other portable devices will be encrypted, as well as all records and files transmitted across public networks or wirelessly, to the extent technically feasible.

- Encryption in this Plan means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by the Regulations.

- All computer systems will be monitored for unauthorized use of or access to personal information.

- There will be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords so that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (4) restriction of access to active users and active user accounts only; and (5) blocking of access to user identification after multiple unsuccessful attempts to gain access.

- The secure access control measures in place will include assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to personal information.

- The Company will exercise due diligence in selecting third-party providers. Any third-party provider that maintains, processes, stores, or has access to personal information through its provision of services to the Company is required to have data security measures in place satisfactory to the Company. Such measures must include appropriate administrative, technical, and physical security measures to protect and secure the information systems that are, and personal information that is, accessible to, or held by, the third-party provider. All third-party providers will be required to provide the Company with a copy of their Soc 1 and Soc 2 test or written information security program, along with a copy of any applicable cybersecurity insurance policy the third-party provider has in place. All third-party providers will also be contractually obligated to comply with all applicable federal and state statutes, regulations, and other requirements relative to data security. The Company will conduct an annual assessment of third-party providers to ensure they maintain sufficient security protocols.