Information Security Safeguards Rule Policy

July 27, 2022

INFORMATION SECURITY

I. BACKGROUND

The Gramm-Leach-Bliley Act ("GLBA") requires "financial institutions" that collect nonpublic personal information about customers who obtain a financial product or service to implement policies and procedures to protect the information they collect. *See* 15 U.S.C § 6801(b). Pursuant to rulemaking authority granted by the GLBA, the Federal Trade Commission promulgated the Safeguards Rule, which requires financial institutions to develop a written information security plan that describes their program to protect customer information. *See* 16 C.F.R Pt. 314. The Company is deemed to be a "financial institution" for purposes of the GLBA and the Safeguards Rule and, as such, is subject to these federal information security provisions.

II. THE COMPANY'S INFORMATION SECURITY POLICY

The Company shall develop, implement, and maintain a comprehensive information security program ("Information Security Program") that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to Company's size and complexity, the nature and scope of activities, and the sensitivity of any customer information at issue. The Information Security Program shall include the elements set forth in the GLBA and the Safeguards Rule and shall be reasonably designed to achieve the objectives of applicable legal requirements.

A. Program Coordinator

The Company has appointed [PRIMARY COORDINATOR] as the Program Coordinator of the Company's Information Security Program. Under the Safeguards Rule, each Company must designate a Qualified Individual responsible for overseeing and implementing Company's Information Security Program. For GLBA compliance purposes, Company's Program Coordinator serves as the designated Qualified Individual. The Qualified individual shall have the skills and experience appropriate for overseeing such a program at a business of Company's size, and may be an employee of Company, its affiliates, or a third-party service provider. Company retains responsibility for any service provider acting as a Qualified Individual, and Company shall designate a senior staff member to oversee the service provider acting as a Qualified Individual.

In the event the Program Coordinator ceases to be employed by the Company or is unable to perform his/her responsibilities, [BACKUP COORDINATOR] shall take over the responsibilities of the Program Coordinator until a new permanent Program Coordinator is appointed.

It is the Program Coordinator's responsibility to design, implement, and maintain privacy policies, *see* Privacy of Consumer Financial Information Policy, and information security standards as he/she determines to be necessary from time to time and to seek approval

from the Board for such policies and standards. Specific responsibilities that have been delegated to the Program Coordinator include:

- Conducting risk assessments to: (i) identify and assess risks to customer information in each relevant area of the Company's operations, and (ii) evaluate the effectiveness of current safeguards that have been implemented to control these risks.

    - The goal of these risk assessments must be to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of customer information, and to assess the sufficiency of safeguards in place to control these risks.

    - These risk assessments shall be written, and must include the following:

        - criteria for the evaluation and categorization of identified security risks or threats;

        - criteria for the assessment of the confidentiality, integrity, and availability of Company information systems and customer information, (including the adequacy of the existing controls in the context of the identified risks or threats); and

        - requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the Information Security Program will address the risks.

    - Risk assessments shall be performed on a periodic basis to reexamine the reasonably foreseeable internal and external risks, as well as the sufficiency of existing safeguards.

- Designing and implementing privacy policies and information security standards in the Information Security Program based on the results of Company's risk assessments. This Information Security Program shall also be appropriate for the size and complexity of our Company and its operations, the nature and scope of our activities and the sensitivity of the customer information we collect, store, and share with others.

- Regularly monitoring and testing the Company's privacy policies and information security standards.

- Assisting with the selection and retention of appropriate service providers that are capable of maintaining safeguards to protect the relevant customer information and reviewing service provider contracts to ensure that each contract contains appropriate obligations with respect to the use of customer information

and the implementation and maintenance of such safeguards. The Program Coordinator should periodically reassess our service providers, considering the risk they present and the continued adequacy of their safeguards.

- Evaluating and adjusting the Company's Information Security Standards in light of relevant circumstances, including the results of the testing and monitoring; the results of risk assessments performed; any material changes to the Company's operations, business relationships, technological developments and/or other circumstances or matters that the Program Coordinator knows or has reason to know may have a material impact on Company's Information Security Program or may impact the security or integrity of the Company's customer information.

- Reporting to the Board (or equivalent governing body) on the overall status of the Information Security Program and the Company's compliance with the GLBA and the Safeguards Rule as well as any material matters related to the information security program. The report should address issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the Information Security Program. This report should be provided on at least an annual basis in writing.

- Establishing and maintaining a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address, at a minimum, the following areas:

    - (1) The goals of the incident response plan;

    - (2) The internal processes for responding to a security event;

    - (3) The definition of clear roles, responsibilities, and levels of decision-making authority;

    - (4) External and internal communications and information sharing;

    - (5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

    - (6) Documentation and reporting regarding security events and related incident response activities; and

    - (7) The evaluation and revision as necessary of the incident response plan following a security event.

B. Employee Management and Training

All current employees and new hires, as well as independent contractors who perform services on behalf of the Company, should:

- Be subject to satisfactory reference and consumer/criminal report investigations, where appropriate.

- Only have access to customer information if they have a business reason for seeing such information.

- Undertake information security standards training and, as needed, participate in educational and training seminars provided.

- Be responsible for protecting the confidentiality and security of the customer information our Company collects and for using the information in accordance with our privacy policies and Information Security Standards.

- Not be permitted to post passwords near their computers or share passwords with any other person.

- Refer telephone calls or other requests for customer information to the Program Coordinator or appropriate manager when such requests are not received within the ordinary course of the Company's business or are for information that the employee is not authorized to provide.

- Disclose to service providers, marketers, or any other parties only that customer information which is necessary to complete a transaction initiated by the customer and/or as permitted by law. If an employee is unsure as to whether a specific disclosure is permitted, he or she will be instructed to check with the Program Coordinator or appropriate manager to verify that it is acceptable to release the information before doing so.

- Be required to notify the Program Coordinator or appropriate manager immediately of any attempts by unauthorized persons to obtain access to customer information and/or if any password or customer information is subject to unauthorized access.

The Program Coordinator should implement policies and procedures designed to ensure that all employees personnel are able to enact your information security program by receiving training regarding the foregoing when they begin employment and thereafter as needed. This includes security awareness training updated to reflect risks identified by Company's risk assessments.

Qualified information security personnel, employed by Company, affiliates, or service providers, should be retained by Company for the purposes of managing security risks and performing Company's Information Security Program. Such personnel should receive security updates and training sufficient to address the relevant security risks and to perform or oversee the Information Security Program. The Program Coordinator is responsible for verifying that key information security personnel take the steps necessary to maintain current knowledge of changing threats and countermeasures.

All new employees should sign the Employee Agreement to Comply with Information Security Standards set forth in Exhibit [X] and receive the Statement of Information Security Standards set forth in Exhibit [Y]. Any employee who fails to abide by the Company's Statement of Information Security Standards, whether such failure is intentional or unintentional, should be subject to appropriate disciplinary action, which may include termination of employment.

When an employee ceases to be employed by the Company, he/she should be required to turn in any keys in his/her possession that provide access to the Company and file cabinets, desks, and offices in the Company; passwords and security codes, if applicable, should be deleted; and employees should not be permitted to take any customer information from the Company.

C. Information Systems

The following information security standards should be implemented in order to protect customer information collected and maintained by our Company:

- The Company will authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information. Employees should have access limited only to that customer information which is necessary to complete their designated responsibilities or that they need to perform their duties and functions. Employees should not access or provide any other unauthorized person (including other employees who have no need for particular information) access to customer information that is obtained during the course of employment. Requests for customer information that are outside the scope of the Company's ordinary business or the scope of an employee's authorization should be directed to the Program Coordinator or designated individuals.

- Access to customer information should be controlled via appropriate technical and physical controls. Every employee with access to the Company's computer system and electronic records should have a unique password consisting of at least [INSERT LENGTH] characters, including numbers and letters. Only employees that need to access electronic records should be provided with passwords. The sufficiency of passwords and other controls should be periodically reviewed to ensure their effectiveness. Multi-factor authentication should also be utilized for all users accessing an information system unless the Program Coordinator has, in writing, approved the use of reasonably equivalent and/or more secure security controls.

- All paper and electronic records should be stored in secure locations to which only authorized employees will have access. Paper records should be stored in an office, desk, or file cabinet that is locked when unattended. Electronic records should be stored on a secure server that is located in a locked room and is accessible only with a password. Where appropriate, records should be maintained in a fireproof file cabinet and/or at an offsite location. Customers,

vendors and service providers should not be permitted access to or left in an area with insecure customer records.

- Backups of the computers and/or server should be made at least once each day, or at more frequent intervals as deemed necessary. At least once each month, an employee in the information technology department should confirm that backups are taking place and that backups are valid and accessible. Backup disks should be stored in a locked file cabinet.

- Virus protection software should be installed on the computers and new virus updates should be uploaded at least once each day. All computer files should be scanned at least once each month, or at more frequent intervals as deemed necessary.

- Firewalls and security patches from software vendors should be downloaded or updated on a daily basis.

- The Company will develop, implement, and maintain procedures for the secure disposal of customer information in any format. All data should be erased from computers, disks, hard drives or any other electronic media that contain customer information before disposing of them and, where appropriate, hard drives should be removed and destroyed. Any paper records awaiting disposal should be stored in a secure area until [an authorized shredding service] [an employee of the Company] picks them up.

    - All customer information must be disposed of no later than two years after it was last used in connection with the provision of Company's products and services to the customer to which it relates.

    - Such information may be retained if: (i) necessary for business operations or for other legitimate business purposes, (ii) required by law or regulation, or (iii) where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

    - Company's data retention policy should be periodically reviewed by the Program Coordinator to minimize the unnecessary retention of data.

- Employees should be required to log off of all Internet, E-mail and other accounts when they are not being used. Employees should not be permitted to download any software or applications to Company computers or open e-mail attachments from unknown sources. Electronic records should not be downloaded to a disk or individual computer without explicit authorization from the Program Coordinator.

- Electronic records containing customer data should not be directly accessible from the Internet once received by the Company. All customer information held or transmitted by Company (both in transit over external networks and at rest) shall be encrypted.

    - To the extent that encryption is infeasible, Company may instead secure customer information using effective alternative compensating controls reviewed and approved by the Program Coordinator.

- Neither current nor former employees should be permitted to remove any customer information from the Company, whether contained in paper records or electronic records, or to disclose our information security standards to any person without authorization from the Program Coordinator.

- Software should be employed to monitor and track all attempts to access electronic records containing confidential information. Such software should be able to generate a trail of employee activities on the Company's systems.

- The Company should employ technology that monitors its information systems for intrusions, notifies employees when intrusions occur and defends against intrusions.

- The Company will limit customers' access to only their own information.

- To the extent Company develops its own software, secure development practices should be adopted for the development of software that will be used to access, transmit, or store customer information.

- The Company should adopt procedures for evaluating, assessing, or testing the security of externally developed applications used to transmit, access, or store customer information.

- The Company should develop change management procedures, which apply when elements of any information systems are added to, removed, or otherwise modified.

- The Company should identify and manage the data, personnel, devices, systems, and facilities that enable it to achieve business purposes in accordance with their relative importance to business objectives and Company's risk strategy.

- The Company should implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access, use of, or tampering with, customer information by all users.

- The Company should engage in continuous monitoring of its systems. If effective continuous monitoring is not possible, Company should:

    - On an annual basis, conduct penetration testing of information systems as determined each given year based on relevant identified risks in accordance with the Company's risk assessment.

- Conduct vulnerability assessments of all systems, including any systemic scans or reviews of information systems reasonably designed to identify publicly-known security vulnerabilities in your information systems based on the Company's risk assessment or at least every six months.

    - Company should also complete vulnerability assessments in instances in which there have been material changes to operations or business arrangements and whenever there are circumstances the Company knows or has reason to know could have a material impact on the Information Security Program.

- The Company should regularly test and monitor the effectiveness key controls, systems, and procedures, including those designed to detect actual and attempted attacks on Company's information systems.

D. Selection and Oversight of Service Providers

In order to protect the customer information the Company collects, the Company should take steps to evaluate and oversee its service providers. The following evaluation criteria should be utilized in selecting service providers:

- Compatibility and willingness to comply with the Company's privacy policies and information security standards and the adequacy of the service provider's own privacy policies and information security standards.

- Records to be maintained by the service provider and whether the Company will have access to information maintained by the service provider.

- The service provider's knowledge of regulations that are relevant to the services being provided, including privacy and other consumer protection regulations.

- Experience and ability to provide the necessary services and supporting technology for current and anticipated needs.

- Functionality of any service or system proposed and policies concerning maintaining secure systems, intrusion detection and reporting systems, customer authentication, verification, and authorization, and ability to respond to service disruptions.

- Service and support that will be provided in terms of maintenance, security, and other service levels.

- Financial stability of the service provider and reputation with industry groups, trade associations and other lenders.

- Contractual obligations and requirements, such as the term of the contract; prices; software support and maintenance; training of employees; customer

service; rights to modify existing services performed under the contract; warranty, confidentiality, indemnification, limitation of liability and exit clauses; guidelines for adding new or different services and for contract re-negotiation; compliance with applicable regulatory requirements; records to be maintained by the service provider; notification of material changes to services, systems, controls and new service locations; insurance coverage to be maintained by the service provider; and use of the Company's data, equipment, and system and application software.

- The right of the Company to audit the service provider's records, to obtain documentation regarding the resolution of disclosed deficiencies, and to inspect the service provider's facilities.

Service providers with access to customer information should be required to agree contractually to be responsible for maintaining an information security program that protects Company in accordance with any applicable legal requirements; securing and maintaining the confidentiality of customer information, including agreement to refrain from using or disclosing the Company's information, except as necessary to or consistent with providing the contracted services; to protect against unauthorized use or disclosure of customer and Company information; to comply with applicable privacy regulations; to implement and maintain safeguards appropriate for the customer information at issue; and to fully disclose breaches in security resulting in unauthorized access to information that may materially affect the Company or its customers and to notify the Company of the services provider's corrective action. *See* Third-Party Service Provider Policy.

Exhibit [Z] includes an Addendum that may be used to amend an existing agreement with a third party service provider (or may be used as a starting point for any amendment) in the event that the existing agreement does not address data security.

Service providers should be subject to ongoing assessment to evaluate their consistency with selection criteria, performance and financial conditions, and contract compliance, including continued adequacy with these safeguards.

E. Managing System Failures

The Program Coordinator should implement audit and oversight procedures as he/she deems necessary to detect the improper disclosure or theft of customer information and to ensure that employees, independent contractors, and service providers are complying with our Company's Information Security Standards.

If the Company's Information Security Standards are breached, the Program Coordinator should immediately inform the Board and shall implement the Company's written incident response plan. The Program Coordinator should take appropriate steps to notify counsel, service providers, customers, and/or law enforcement authorities of any breach, damage, or loss of information and the risks associated with the same and

should immediately take measures to limit the effect of the breach, identify the reason for the breach, and implement procedures to prevent further breaches.

In the event of a breach, or at any other time as the Program Coordinator deems appropriate, the Program Coordinator should modify or supplement our Company's Information Security Standards and discuss the need for such modification or supplement with the Board.

EXHIBIT [X]

EMPLOYEE AGREEMENT TO COMPLY WITH INFORMATION SECURITY STANDARDS

Federal law requires that the Company implement policies and procedures to protect the information on consumers that the Company collects. As a condition of your employment with the Company, you agree to:

1. Read the “Statement of Information Security Standards” and familiarize yourself with the information contained therein.

2. Follow our procedures for safeguarding and protecting customer information in accordance with the “Statement of Information Security Standards.”

BY SIGNING BELOW, YOU ACKNOWLEDGE THAT YOU HAVE RECEIVED AND READ THE COMPANY’S STATEMENT OF INFORMATION SECURITY STANDARDS AND AGREE TO COMPLY WITH THE STANDARDS AS SET FORTH THEREIN AS A CONDITION OF YOUR EMPLOYMENT. YOU FURTHER UNDERSTAND THAT THE FAILURE TO FOLLOW THE COMPANY’S INFORMATION SECURITY STANDARDS MAY RESULT IN DISCIPLINARY ACTION, INCLUDING THE TERMINATION OF YOUR EMPLOYMENT.

_____

EMPLOYEE DATE

EXHIBIT [Y]

STATEMENT OF INFORMATION SECURITY STANDARDS

Our Program Coordinator

We have appointed [PRIMARY COORDINATOR] as the Program Coordinator of the Company's Information Security Program. The Program Coordinator will report directly to the Board of Directors. In the event the Program Coordinator ceases to be employed by the Company or is unable to perform his/her responsibilities, [BACKUP COORDINATOR] shall take over the responsibilities of the Program Coordinator until a new permanent Program Coordinator is appointed.

Based upon the Program Coordinator's risk assessment of the Company's operations, including employee management and training and our information systems (i.e., information collection, processing, storage, transmission and disposal, and potential system failures), the following information security standards have been adopted for all employees and any independent contractors. Individual employees may be given additional responsibilities as well. Compliance with the Company's information security standards is a condition of your employment with us.

Employee Interviewing, Hiring, and Training

All current and new employees, as well as independent contractors who perform services on behalf of the Company, should:

1. Be subject to satisfactory reference and consumer/criminal report investigations.

2. Participate in the Company's information security standards training program and attend any subsequent training provided by the Company.

3. Sign and acknowledge agreement to the Company's Statement of Information Security Standards.

4. Be responsible for protecting the confidentiality and security of the customer information the Company collects and for using the information in accordance with our privacy policies and information security standards.

Protecting the Confidentiality and Security of Customer Information

Each employee is responsible for protecting the confidentiality and security of the customer information the Company collects. The following security procedures must be followed in order to protect our customer information:

1. ***Employees must not access customer information which is not necessary to complete their designated responsibilities.*** Employees should not access or provide

any other unauthorized person access to customer information that is obtained during the course of employment for any other purpose. Employees should refer requests for customer information to the Program Coordinator or appropriate manager when such requests are not received within the ordinary course of the Company's business or are for information that the employee is not authorized to provide.

2. All paper and electronic records should be stored in secure locations to which only authorized employees will have access. Paper records should be stored in an office, desk, or file cabinet that is locked when unattended. Electronic records should be stored on a secure server that is located in a locked room and is accessible only with a password. Where appropriate, records should be maintained in a fireproof file cabinet and/or at an offsite location. Customers, vendors, and service providers should not be allowed access to or be left in an area with insecure customer records.

3. Access to electronic customer information should be password controlled. Every employee with access to the Company's computer system and electronic records should have a unique password consisting of at least [INSERT LENGTH] characters, including numbers and letters. Only employees that need to access electronic records should be provided with passwords. ***Passwords should not be posted near computers or shared with any other person.***

4. ***Employees who have access to the computer system and electronic records must not download any software or applications to Company computers or open e-mail attachments from unknown sources. Employees should log off of any Internet, E-mail, or other account when it is not in use.***

5. ***Electronic records must not be downloaded to a disk or individual computer without explicit authorization from the Program Coordinator. If customer information is transmitted electronically over external networks, employees must encrypt the information both at the time of transmittal and at rest.***

6. All data should be erased from computers, disks, hard drives or any other electronic media that contain customer information before disposing of them and, where appropriate, hard drives should be removed and destroyed. Any paper records awaiting disposal should be stored in a secure area until an authorized shredding service picks it up.

7. ***Employees must not remove any customer information, whether contained on paper records or electronic records from the Company or disclose our security standards to any person who is not employed by the Company without authorization from the Program Coordinator.***

8. Only that information which is necessary to complete a transaction initiated by the customer is specifically authorized to be disclosed by the customer and/or is permitted to be disclosed by law should be provided to service providers, marketers, or any other parties. If you are unsure as to whether a specific disclosure is permitted, you should

check with the Program Coordinator or your manager to verify that it is acceptable to release the information before doing so.

9. Neither current nor former employees may remove any customer information from the Company, whether contained in paper records or electronic records, or disclose our information security standards to any person without authorization from the Program Coordinator.

10. ***The Program Coordinator or appropriate manager must be notified immediately of any attempts by unauthorized persons to obtain access to customer information and/or if any password or customer information is subject to unauthorized access.***

11. When an employee ceases to be employed by the Company, he/she must turn in any keys that provide access to the Company and file cabinets, desks, and offices in the Company; passwords and security codes, if applicable, will be deleted.

Disciplinary Action

Any employee who fails to abide by our Statement of Security Standards, whether such failure is intentional or unintentional, will be subject to appropriate disciplinary action, which may include termination of employment.

EXHIBIT [Z]

ADDENDUM

This Addendum modifies each and every agreement (collectively, "Agreement") entered into between _____ or any affiliate ("Service Provider"), and _____ or any affiliate ("Company"). By executing this Addendum, Service Provider and Company acknowledge and agree that this Addendum is incorporated into and made a part of the Agreement, the terms and provisions of which, except as expressly modified in this Addendum, are hereby affirmed and ratified by Service Provider and Company and remain in full force and effect.

It is agreed between the parties to the Agreement and this Addendum that, notwithstanding anything to the contrary contained in the Agreement or in any other documents pertaining to the Agreement, Company is a financial institution and Service Provider shall comply with all privacy and data protection laws, rules and regulations applicable now and in the future to the nonpublic personal information of Company's customers. Without limiting the generality of the preceding sentence, Service Provider agrees that it will implement and maintain appropriate safeguards to protect all nonpublic personal information it receives pursuant to the Agreement and will not use or disclose such information to any other party, except as is reasonably necessary to fulfill the purposes for which such information was provided and as otherwise permitted by applicable law, and will not use or disclose such information in violation of Company's privacy policy, as provided to Service Provider from time to time. For purposes of this Addendum, the terms "nonpublic personal information" and "financial institution" shall have the meanings set forth in Section 509 of the Gramm-Leach-Bliley Act (P.L. 106-102) (15 U.S.C. § 6809) and implementing regulations thereof. The provisions contained in this Addendum shall survive the termination or expiration of the Agreement, by the expiration of time, by operation of law, or otherwise.

IN WITNESS HEREOF, and intending to be bound by the terms and conditions hereof, each of the parties has caused this Addendum to be executed by its duly authorized representative as of the respective dates set forth below.

Service Provider:_____
Its:_____
By:_____
Date: _____

Company:_____
By:_____
Its:_____
Date:_____