PAYKII'S Information Security Program

Overview: This document summarizes PAYKII's (the "***Company's***") information security program (the "***Program***"), and in particular describes the Program elements pursuant to which PAYKII will:

(i) protect the security and confidentiality of nonpublic financial information,
(ii) protect against any anticipated threats or hazards to the security of such nonpublic financial information,
(iii) protect against the unauthorized access or use of such nonpublic financial information or information in ways that could result in substantial harm or inconvenience to consumers, and
(iv) comply with the requirements of the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("***GLBA***").

The Program incorporates PAYKII's policies and procedures enumerated below and is in addition to any internal policies and procedures that may be required pursuant to other federal and state laws and regulations.

Designation of Representatives: The Company's Chief Technology Officer shall be designated as the "*Program Officer*" and is responsible for coordinating and overseeing the Program. The Program Officer may designate other representatives of PAYKII to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his or her designees.

Scope of Program: The Program applies to any record containing nonpublic financial information about a third party who has a relationship with the Company, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the Company or its affiliates. For these purposes, the term "*nonpublic financial information*" shall mean any information (i) a consumer/end user or other third party provides in order to obtain a financial service from PAYKII or PAYKII Partners, (ii) about a consumer/end user or other third party resulting from any transaction with PAYKII involving a financial service, or (iii) otherwise obtained about a third party in connection with providing services to that person. "*PAYKII Partners*" shall mean the vendors retained by PAYKII who have a direct relationship with utility service providers in each jurisdiction where PAYKII offers its services and through which PAYKII processes the consumer payment transactions.

Elements of the Program:

1. Risk Identification and Assessment. The Company intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Program, the Program Officer will establish procedures for identifying and assessing such risks in each relevant area of the Company's operations, including:

- *Employee training and management*. The Program Officer will coordinate with representatives in the Company's management department to evaluate the effectiveness

of the Company's procedures and practices relating to access to, use and records pertaining to the consumer, service, product, or transaction. This evaluation will include assessing the effectiveness of the Company's current policies and procedures in this area, including current procedures.

- *Information Systems and Information Processing and Disposal.* The Program Officer will coordinate with representatives of the Company's IT Department to assess the risks to nonpublic financial information associated with the Company's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Company's current polices and procedures relating to the use of the Company's network and network security, document retention and destruction. The Program Officer will also coordinate with the Company's IT Department to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- *Detecting, Preventing and Responding to Attacks*. The Program Officer will coordinate with the Company's IT Department to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer may elect to delegate to a representative of the IT Department the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Company.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. Overseeing Service Providers. The Program Officer shall coordinate with those responsible for the third party service procurement activities and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of consumersand other third parties to which they will have access. In addition, the Program Officer will work with its legal counsel to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards.

4. Adjustments to Program. The Program Officer is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Company's operations or other circumstances that may have a material impact on the Program.