HORICON BANK
The Natural Choice

Security Schedule

This Security Schedule ("Schedule") to the Horicon Bank Master Treasury Management and Online Banking Agreement (the "Agreement") sets forth the required security procedures that shall apply to all Services (as defined in the Agreement) used by you.

1. Scope, Definitions. By signing below and through your use of the Services, you agree to be bound by the terms and conditions hereof. It is understood and agreed that this Schedule shall supplement and is hereby incorporated into the Agreement and any related Schedules. Unless otherwise defined herein, capitalized terms have the meanings ascribed to them in the Agreement. Any reference to "we", "us", or the "Bank" shall refer to Horicon Bank, and any reference to "you" or the "Company" shall refer to the company countersigning this Schedule below.

2. Background. The Services require the use of our Online Banking platform. In order to mitigate the risks to you and us, and to clearly establish each party's expectations, liability, and responsibilities regarding the Services, we have developed this Security Schedule. By using the Services, you agree that these procedures are commercially reasonable and that you agree with and accept the terms and conditions set forth below. You understand that the security procedures are for verification of authenticity of any transaction or access request and are not intended to detect errors in the transmission or content of any entries. You and we have not agreed upon any security procedures for the detection of any such errors.

3. Commercially Reasonable. **YOU HEREBY AGREE TO THE SECURITY PROCEDURES HEREIN AND ACKNOWLEDGE THAT SUCH SECURITY PROCEDURES ARE A COMMERCIALLY REASONABLE METHOD OF PROVIDING SECURITY AGAINST UNAUTHORIZED TRANSFER OF FUNDS, PAYMENT INSTRUCTIONS AND OTHER TRANSACTIONS.** You confirm that you have assessed the security procedures for Online Banking and have determined that these features, in combination with your own security measures, are adequate for your Account(s). If you use any method other than the security procedures set forth herein in connection with Online Banking or to communicate, deliver, or transmit any instruction to us, you reject the security procedures set forth herein and are deemed to have chosen an alternative security procedure. In such case, you agree that such alternative security procedures may not be found to be commercially reasonable, and agree to be bound by any instruction or any other transaction, whether or not authorized, that was issued in your name, or otherwise, and accepted by us using the alternative security procedures selected by you.

4. Designation of Authorized Users. From time to time, you will designate users to be Authorized Users of any given service. The Bank may rely on instructions reasonably believed to be received from Authorized Users. Until the Bank receives a new designation adding or removing Authorized Users from any given Service, the Bank may continue to act pursuant to the designations on file.

5. Bank Duties. We will do the following, as applicable:

5.1 Provide multi-factor authentication that utilizes user IDs and passwords ("Codes"), to identify clients when logging into Online Banking, plus, for high-risk transactions involving access to client information or the movement of funds to other parties, at least one other method of security such as a security device ("Token"), callback, or some other "out-of-band"

control. We reserve the right to modify the identification process from time to time to implement new measures that are recommended in the industry to combat new or increased threats.

5.2 Set up limits for bill payment, funds transfer, wires, ACH, and other cash management services, as we may deem appropriate from time to time.

5.3 Provide user and device transaction monitoring, which requires "out-of-band" confirmations for certain abnormal transaction activity detected by our advanced login service.

5.4 Publish minimum best practices for online banking security on our website at www.horiconbank.com. We will also offer client education and awareness information pertaining to the prevention of security breaches of online banking.

6. Customer Duties. You will do the following, as applicable:

6.1 Investigate, implement, and maintain adequate online banking security practices and procedures related to access to and use of Online Banking.

6.2 Set up, maintain and regularly review security arrangements concerning access to, and use of, Online Banking and the Services. This includes, but is not limited to, a device, computer or computer network owned, controlled or used by you or your employees, contractors, service providers or agents; the control of your Internet access services; and the control of your Codes and Tokens.

6.3 Install, update, maintain and properly use industry standard security products that are appropriate for you, such as the following, without limitation:

6.3.1 Firewall to prevent unauthorized access.

6.3.2 Anti-virus protection to prevent your personal computers from being victimized by the latest viruses and other destructive or disruptive components.

6.3.3 Anti-spyware protection to prevent spyware from providing potential tracking information about your Web activities.

6.3.4 A product that indicates the Web site you are on, or an Internet browser that indicates the site name.

6.4 Install, update, maintain and properly use industry standard operating systems and desktop applications with the latest patches when they are available, particularly when and if they apply to a known exploitable vulnerability. We require your browser to be, at a minimum, a fully SSL-compliant, 128 bit encrypted browser.

6.5 Follow these minimum general safety guidelines:

6.5.1 Never walk away from your computer while logged on to Online Banking.

6.5.2 Check your Account balances and activity daily and report any suspicious activity immediately by calling at (888) 343-3040.

6.5.3 Memorize your Codes, change them regularly (or upon our request), and never use any "save password" feature available on your computer or software.

6.5.4 Never disclose your Codes to any other person, and take all reasonable actions to maintain their confidentiality. If someone identifies himself as one of our employees and asks for your Codes, that person is an imposter.

6.5.5 Choose Codes that are not easy to guess. Passwords must comply with our minimum requirements.

6.5.6 Read and stay abreast of the best practices for online banking security as published on our website. From time to time, these best practices may be updated.

6.5.7 Call us immediately at (888) 343-3040 if you know of or suspect any unauthorized access to Online Banking or any unauthorized transaction or instruction, or you believe your Codes or Tokens have been stolen or compromised.

6.6 Enable, update, maintain, and properly use email and/or text message alerts offered in Online Banking that alert you when there has been transaction activity on your Accounts.

6.7 Notify us immediately if your phone number, mailing address, or email address that we use to contact you changes.

7. Breaches of Security Procedures. You assume full responsibility for any transaction conducted through the Services that we accept in good faith, if we complied with the applicable security procedure or if you did not comply with it. Except for a breach of security in our internal systems, and except in a case where you comply with the applicable security procedures and either we do not so comply or we do not act in good faith, we shall have no responsibility for, and you assume full responsibility for, any transfer of funds, payment instructions or other transactions resulting from a breach of security regardless of the source or cause thereof. Without limiting the generality of the previous sentence, you are responsible for a breach of security occurring on or in connection with your systems or use of Online Banking, by whatsoever means, such as (by way of example and not limitation), viruses, Trojans, worms, phishing, pharming, keylogging or other fraudulent activity enabled by malware or other destructive or disruptive components. If we do bear responsibility, it will extend only to losses caused solely and directly by us, and our liability will in any event be limited as provided in the "Limitation of Liability" section of the Agreement.

8. Security Enhancements. The following security measures are available to you and may be subject to a fee. Each is designed and intended to further mitigate the risks associated with certain of the Services. In addition, new security measures are constantly being developed and introduced and current measures evolve quickly. From time to time we will make you aware of new security measures that we offer. If you continue to use the Services without subscribing for the enhanced security measures that we may offer now and in the future, you understand and agree that you assume all liability resulting from any losses or damages that could otherwise have been prevented with such measures.

8.1 **ACH Blocks**. We offer an ACH Blocks product that provides complete "pay" or "no pay" control of exception items by allowing you to compare authorized debtor information to ACH debits.

8.2 **Positive Pay**. We offer a Positive Pay product that provides complete "pay" or "no pay" control of exception items by comparing check issue information to checks presented for payment.

8.3 **Confirmation Call Back.** You may authorize individuals to receive call-backs from the Bank for verification of authenticity of payment orders. The Bank may rely on the verbal verification of the payment orders.

8.4 **Dual Control**. Certain products, such as wire transfers and ACH transactions, offer the ability to require dual authorization before we will honor a payment request. If you have elected to forgo the use of dual control where allowed, you agree to assume any liability that may arise from unauthorized transactions that may have been detected and/or prevented with the use of dual control security procedures.

8.5 **Trusteer Rapport**. We offer Trusteer Rapport, which is a security software application that provides online transaction protection. Trusteer Rapport protects your web browser sessions with any website that contains private or personal information, and is specifically designed to protect against keylogging, malicious browser add-ons, malicious programs, screen shooting, session hijacking, phishing, and pharming or DNS spoofing. You will be required to consent to an agreement with Trusteer for this service if you choose to use it. Trusteer is not affiliated with us, and we will have no liability whatsoever for any claims, damages, or losses caused by Trusteer Rapport. We are not responsible for the use, maintenance, effectiveness or performance of Trusteer Rapport and do not incur any additional liability whatsoever as a result of your use of Trusteer Rapport. The provisions of this paragraph shall apply to a substantially similar service offered by a different vendor, should Financial Institution change vendors. If you decline to employ one or more of these enhanced measures, you agree to assume any liability for losses or other damages that may arise from doing so.