First National Bank of Hartford Security Schedule

Capitalized terms not defined herein have the meanings ascribed to them in the applicable Base Agreement for FNB ez Business Banking Treasury Management Products and Services and the First National Bank of Hartford Online Banking Agreement. Any reference to "we," "us," the "Bank" and "our" shall refer to First National Bank of Hartford, and any reference to "you" and "your" means the owner of any accounts covered by this Security Schedule, any delegate, any authorized representative, the Administrator, and any person using our online banking, bill payment, remote deposit capture, stop payment, ACH services, mobile banking, and any other online services provided to you by us (the "Services").

The security procedures set forth herein shall apply to all Services used by you, and the terms and conditions hereof shall supplement and be incorporated into all other agreements and schedules between you and us.

1. **GENERAL.** Many of the Services require the use of hardware, software and the Internet. Further, many of the Services allow you to access and transmit information without direct contact with a Bank employee. Accordingly, the Services involve a heightened risk of fraud, unauthorized activity, abuse, disruption, etc. 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 your continued use of the Services, you agree that these procedures are commercially reasonable 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. No security procedure for the detection of any such errors has been agreed upon between you and us.

2. **BANK'S OBLIGATIONS.** We have done or will do the following:

(a) Offer customer education and awareness programs and/or materials dealing with identity theft, phishing, and malware.

(b) Identify customers when logging on through the use of multi-factor authentication. Multi-factor authentication will utilize user IDs and passwords, plus, for high-risk transactions involving access to customer information or the movement of funds to other parties, at least one other method of security such as a 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.

(c) Install, update, maintain and properly use industry standard security procedures for firewalls, anti-virus, anti-spyware and patches.

3. **YOUR OBLIGATIONS.** You agree to do the following, as applicable:

(a) **All Accounts:** Adequate security controls should be in place to protect the online banking computers and confidential customer information. Among other things, you agree:

(i) To follow these best practice guidelines:

(1) Never leave your computer or other access device (e.g. mobile phone) unattended while logged on to this Service.

(2) Memorize your user ID and password.

(3) With regards to passwords:

a. *Prohibit the use of "shared" usernames and passwords.*

b. Always use strong passwords which are composed of at least THREE of FOUR following characteristics (using all four is encouraged):

i. At least one numeric character (0-9)

ii. At least one lower case character (a-z)

iii. At least one upper case character (A-Z)

iv. At least one non-alphanumeric character* (!, @, #, $, *, =)

c. Use a minimum of 10 characters and a maximum of 16 characters

d. Passwords should meet or exceed complexity requirements based on the risk.

e. Passwords should be changed frequently based on risk.

f. Do not use passwords that are easy to guess or include personal information such as names (relatives, pets, etc.), or dates such as birthdays or anniversaries.

g. Do not use the same password for multiple accounts.

(4) Do not save passwords on your computer or any other access device (e.g., mobile phone), unless in an encrypted password vault.

(5) Use a locking screensaver that requires a password to be entered after a period of inactivity.

(ii) To ensure that passwords are protected from exposure. Never disclose your passwords to any other person even a bank employee. Your passwords are for your use and should be kept confidential by you. Under no circumstances will we contact you and ask for your user ID, passwords or security pins. We will only request your verification of your identity when you initiate a call.

(iii) To check your statements and review your banking transactions promptly, thoroughly and regularly. Report any suspicious activity, errors or problems immediately to us.

(iv) Should you receive a suspicious e-mail or telephone request for information that purports to be from us, you must immediately notify your banker or call 262-670-3878.

(v) That from time to time we may update this Security Schedule or provide other correspondence and educational information, articles or "tips" regarding security issues and ways to protect your account. You agree to watch for, read, and, where applicable, comply with the steps identified in such materials.

(b) **Business Accounts.** In addition to the steps above, customers maintaining business deposit accounts will do the following, as applicable:

(i) Use multiple passwords and multiple computers for the transmission of data.

(ii) Install, update, maintain and properly use industry standard security products that are appropriate for you, including without limitation:

(1) Desktop firewall used to prevent unauthorized access to your network.

(2) Updated anti-virus protection used to prevent your computer from being victimized by the latest viruses and Trojans.

(3) Updated anti-spyware protection used to prevent spyware from providing potential tracking information about your website activities.

(4) Operating system and desktop applications updated with the latest patches when they are available, particularly when and if they apply to a known exploitable vulnerability.

(iii) When initiating Automated Clearing House (ACH) transactions and wire payments, use dual controls with a transaction initiator and a transaction authorizer.

(iv) Persons authorized to access online banking by the Administrator ("Authorized Person") must use a separate user ID and password to originate payment file and/or transmission of data.

(v) Where required, a separate Authorized Person (independent from the originator) verifies and transmits the payment file and/or transmission of data.

(vi) If you have multiple users, it is your responsibility to notify us of any changes in their authority.

(vii) All computer equipment used for RDC processing or initiating ACH transactions should be located in a secure area and only be used for such transactions.

(c) **Remote Deposit Capture ("RDC") Processing.** In addition to all other steps described herein, the following apply if you engage in RDC:

(i) Ensure all checks scanned through RDC are original items, properly payable and properly endorsed to the account in which they are being deposited.

(ii) Spot check images made through RDC and review prior to transmission to ensure quality.

(iii) Ensure that original checks are properly secured after being scanned and are physically destroyed after being held for at least 60 days, but not more than 90 days.

4. AGREEMENT. YOU AGREE TO TAKE ALL REASONABLE PRECAUTIONS TO PREVENT UNAUTHORIZED ACCESS TO ACCOUNTS AND SYSTEMS. IF YOU SUSPECT, KNOW, BELIEVE OR HAVE REASON TO BELIEVE THAT AN UNAUTHORIZED PERSON HAS GAINED OR ATTEMPTED TO GAIN ACCESS TO YOUR ACCOUNTS, **YOU AGREE TO IMMEDIATELY NOTIFY US AT 262-670-3878.**

5. LIMITATIONS OF LIABILITY. 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 procedure 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 transaction resulting from a breach regardless of the source thereof. Without limiting the generality of the foregoing, you are responsible for a breach of security occurring on or in connection with a computer or computer network owned, controlled or used by you or your employees, contractors, service providers or agents, by any means whatsoever, such as (by way of example and not limitation) phishing, pharming, keylogging or other fraudulent activity enabled by malware. If we do bear responsibility, it will extend only to losses caused solely and directly by us, and our liability will be limited in accordance with the other terms of the applicable Base Agreement for FNB ez Business Banking Treasury Management Products and Services,

the First National Bank of Hartford Online Banking Agreement and any other agreement entered into between you and us.

If you use any method other than the procedures set forth above in connection with the Services or to communicate, deliver, or transmit any instruction to us, you reject the security procedure set forth herein and are deemed to have chosen an alternative security procedure. In such case, you agree that such alternative security procedure 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 procedure selected by you.

Should you have any questions, please contact us at 262-670-3878.

11204831.2