National Exchange Bank & Trust®

Security Schedule (Consumer)

This Security Schedule ("Schedule") to the Electronic Services Agreement covering consumer online banking & eBanking products (the "Agreement") sets forth the required security procedures that shall apply to all Exchange OnLine services used by you regardless of how you access the service (including, without limitation, access by use of the mobile app).

1. Scope; Definitions. 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. 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 National Exchange Bank & Trust, and any reference to "you" or "your" shall refer to the owner of the account(s) covered by this Schedule, any delegate, or any person using Exchange OnLine, inclusive of all services provided through the Exchange OnLine portal including but not limited to bill payment, person to person payments, remote deposit services, and eDisclosures including without limitation the use of any of those services through the mobile app (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. You also acknowledge that from time to time we may update this Schedule or provide other correspondence 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.

2. Background. The Services require the use of Exchange OnLine. 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, 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 that you agree with and accept the terms and conditions set forth herein. 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. Rejection of Security Procedures. If you use any method other than the procedures set forth herein 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 (i) 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, and (ii) to the extent permitted by law, will be liable for any damages caused indirectly or directly by your use of an alternative security procedure.

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

    4.1 Provide identity authentication methods to secure access to your information on Exchange OnLine. These may include log-in IDs, passwords, and one-time passcodes (collectively "Codes"). We may require you to change or update your username and/or password at any time, including to meet any new standards we may establish. 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.

    4.2 Set up limits for bill payments, person to person transactions, funds transfers, and other money movement services, as we may deem appropriate from time to time. We may require enhanced security methods including multi-factor authentication when executing a transfer.

    4.3 Provide user and device transaction monitoring, which requires multi-factor authentication confirmations for certain abnormal or out of character activity detected by our advanced security settings.

National Exchange Bank & Trust®

4.4 Offer client education and awareness information pertaining to the prevention of security breaches of online banking at www.nebat.com.

4.5 Restrict access to Exchange OnLine if we believe your device has been compromised. We will ask for evidence of professional threat mitigation of the impacted device before reinstating access. We reserve the right to withhold access until the Bank feels comfortable the risk has been mitigated.

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

5.1 Investigate, implement, and maintain adequate online banking security practices and procedures related to access to and use of Exchange OnLine including changing your password regularly. You are responsible for keeping your password confidential. We recommend you select a unique username and password combination for use only with the Service, and memorize it rather than writing it down. Exchange OnLine offers the ability to force multi-factor authentication at login, and we encourage you to enable this for your security.

5.2 Set up, maintain and regularly review security arrangements concerning access to, and use of, Exchange OnLine and the Services. This includes, but is not limited to, a device, computer or computer network owned, controlled or used by you; the control of your Internet access services; and the control of your Codes.

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

5.3.1 Firewall to prevent unauthorized access.

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

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

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

5.4 Install, update, maintain and properly use 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.

5.4.1 Supported computing systems include all versions Microsoft Windows and Apple mac OS currently supported by the provider.

5.4.2 Supported browsers for the computing systems include the latest two versions of Google Chrome, Firefox, Microsoft Edge and Safari.

5.4.3 Supported operating systems for mobile devices include the current version and two most recent major versions of Android and iOS.

5.4.4 Supported browsers for Android and iOS systems include the current device operating system browser.

National Exchange Bank & Trust®

5.5 Follow these minimum general safety guidelines:

5.4.5 Never walk away from your computer or phone while logged on to Exchange OnLine.

5.4.6 Check your account balances and activity regularly and report any suspicious activity immediately by calling 877-921-7700.

5.4.7 Memorize your Codes, change them regularly (or upon our request), and never use any "save password" feature available on your computer or software. Use unique codes on Exchange OnLine that are not duplicated across other sites that require Codes.

5.4.8 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.

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

5.4.10 Read and stay abreast of the fraud prevention information as published on our website. From time to time, this information may be updated.

5.4.11 Call us immediately at 877-921-7700 if you know of or suspect any unauthorized access to or viewing of Exchange OnLine, or any unauthorized transaction or instruction, or you believe your Codes have been stolen or compromised.

5.6 Install, update, maintain, and properly use email and/or text message alerts offered by Exchange OnLine that alert you when there has been transaction activity on your accounts.

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

6. 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 Exchange OnLine, 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.