

THE BANK OF PRINCETON ONLINE BANKING AGREEMENT AND DISCLOSURE

This Online Banking Agreement and Disclosure (the "Agreement") is between you and The Bank of Princeton. It governs your use of certain electronic banking services offered by The Bank of Princeton through an Internet banking system known as "Online Banking." By using Online Banking or by permitting another person to use Online Banking, you agree to the terms and conditions of this Agreement.

Definitions

"We," "our," "us," and "the Bank" mean The Bank of Princeton. "You" and "your" mean a depositor of the Bank who either (a) uses Online Banking pursuant to this Agreement and/or (b) authorizes any other person to use Online Banking in connection with the depositor's account(s) at the Bank. "Account" or "Accounts" means your deposit account(s) at the Bank. "Electronic funds transfer" means an ATM withdrawal, a preauthorized transaction, a point of sale (POS) transaction or a transfer of funds between your Accounts using Online Banking. "Online Banking Services" means the services provided pursuant to this Agreement. "Business days" are Monday through Friday, excluding federal bank holidays.

Online Banking Services

You may use Online Banking to check the balance of your Account, view the transaction history of your Account, transfer funds between internal accounts, place stop payment orders on checks and view images of paid checks. Balance and activity information is generally available as of the current business day. Customer may request access to certain Funds Transfer Services as described below. If the Customer requests the ability to use the Funds Transfer Services, the following shall apply:

- a. Bill Payments - The Bill Payment feature of Online Banking is not available for your use unless you have first agreed to the terms of a separate Bill Payment Agreement between you and the Bank.
- b. ACH Transfer - Customer acknowledges that the ACH feature of the Service is an alternate entry system for issuing funds transfer requests to the Automated Clearing House network. A separate ACH Agreement between Customer and the Bank is required. This ACH Agreement shall govern the acceptance and liability for all ACH transfer requests.
- c. Wire Transfers - Customer acknowledges that the Wire Transfer feature of the Service is an alternate entry system for issuing wire transfer orders between the Customer and the Bank. A separate Wire Transfer Agreement between Customer and the Bank is required. The Wire Transfer Agreement shall govern the acceptance and liability for all Wire Transfer Requests.

Exclusion of Warranties

THE ONLINE BANKING SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Account Eligibility and Transaction Limits

Multiple Signature Accounts – An account that requires more than one signature on a check or more than one signature to make a withdrawal may not be used in connection with Online Banking Services. If you designate an Account that requires more than one signature for a check or a withdrawal for use in connection with Online Banking Services, then you irrevocably waive the requirement for more than one signature for any check or withdrawal from that Account.

Account Transaction Limits - If any of your Accounts are money market accounts or statement savings accounts, you are permitted to make no more than six transfers and withdrawals, or a combination of such transfers and withdrawals, per calendar month or statement cycle (or similar period) of at least four weeks, to another of your accounts at the Bank or to a third party by means of a preauthorized or automatic transfer. If you exceed these limits on more than an occasional basis, we will close the account.

The following are eligible accounts to access in Business Online Banking:

Checking, Savings, Money Market, Certificates of Deposit, IRAs and Loans.

Computer Requirements

To use the Online Banking Services, you must have a computer with Internet access and a supported web browser with 128-bit encryption. It is your responsibility to maintain and upgrade your computer equipment as needed for your use of Online Banking. We are not responsible for any failure or malfunction on your computer, any computer virus that may affect your computer or other problems that may occur, directly or indirectly, from your use of Online Banking.

Hours of Access

You may use Online Banking at any time, seven days a week, twenty-four hours a day. From time to time, however, the Online Banking Services may be temporarily unavailable due to system maintenance or technical difficulties. We will post a notice of any extended periods of system outages on the The Bank of Princeton website.

Password and Access ID

You will determine what Access ID and password you will use. Your access ID and password should be kept confidential and not shared with anyone, including employees of the Bank. You must change your password on a regular basis. Your password should not be associated with any commonly known personal identification, such as social security numbers, address, date of birth, names of children, and should be memorized rather than written down.

SECURITY

In order to maintain secure communications and reduce fraud, Customer agrees to protect the security of all Access IDs, Passwords, codes, marks, signs, public keys, Security Tokens or other means of identification under their authority. The Bank reserves the right to block access to Business Online Banking in order to maintain the security of the site and its systems if we reasonably believe your access codes have been or may be obtained or are being used or may

be used by an unauthorized person(s). All uses of Business Online Banking using Customer's credentials will be presumed to be uses authorized by the Customer and binding upon the Customer.

Customer is responsible for maintaining the security of their device (PC, mobile device, etc.) and all transactions performed within Business Online Banking. Customer agrees to continuously update all devices used for accessing Business Online Banking applications with current patches, antivirus signatures, and security updates as released. Customer agrees not to leave their device unattended while logged into Business Online Banking and to log off immediately at the completion of banking session. Customer is highly recommended to use a segregated PC for Business Online Banking activity; i.e., a PC that is not used for other activities including email, internet surfing, etc. Passwords and user credentials should not be saved to the user's PC or browser.

Customer is responsible for the security of the network they connect to - to access Business Online Banking. The Bank recommends using network firewalls and blocking unnecessary ports, as well as filtering internet traffic to prevent viruses. Users of Business Online Banking should attend Bank-provided training to ensure they understand how to protect their privacy and accounts online.

Customer is responsible for monitoring their account(s) and access to their account(s). Suspicious activity or suspected fraud must be reported to the Bank immediately.

Additionally, under no circumstances, will a Bank employee request Customer's Password via the Internet. Customer should not send confidential information via the Internet or email.

Upon approval for select Business Online Banking services, Customer may be issued a Soft Security Token.

Authority to Make Transactions

You understand and agree that anyone who has your password and access ID will have the ability to transfer funds and conduct other transactions in your Accounts. Authority to initiate transactions will be conclusively presumed by us if the person initiating the transaction uses the password regardless of whether or not the person is in fact authorized to make the transaction. We will not monitor or evaluate transactions made through Online Banking to determine if they are made on your behalf or for your benefit.

Hacking and Malware Risks

You acknowledge that criminals may attempt to hack into or otherwise plant computer viruses or malicious software (collectively "malware") in your computer to gain access to your passwords and user ids. This malware is then used to take control of your computer and initiate transfer instructions to us using your computer and/or your passwords and user ids. To reduce the risk of this happening, you agree to install and maintain state-of-the-art anti-virus and malware detection software on your computer before using Online Banking. You also agree that we have no duty or obligation whatsoever to protect you from such criminal activities and no duty or obligation to ascertain whether any transfer of funds or other transaction is legitimate

when the instruction to transfer funds or make a payment is accompanied by the correct password and access ID. You acknowledge that we cannot determine whether or not the security of your computer has been compromised by the actions of a third party.

Data Encryption

Data transferred via Online Banking is encrypted in an effort to provide transmission security. Online Banking utilizes identification technology to verify that the sender and receiver of Online Banking transmissions can be appropriately identified by each other. Notwithstanding our efforts to protect the security of the Online Banking system, you acknowledge that the Internet is inherently insecure and that all data transfers, including electronic mail, occur openly on the Internet and can potentially be monitored and read by others. We cannot and do not warrant that all data transfers utilizing Online Banking, or e-mail transmitted to and from us, will not be monitored or read by others.

Fees and Charges

Online Banking services are offered at no cost to you unless you place a stop payment request. You agree to pay the stop payment fee as set forth in the current fee schedule. Payment for fees and charges will be debited directly from your Account on a monthly basis.

New Services

The Bank may, from time to time, offer and introduce new Internet products and services. We will notify you of these new services and products. By using these services when they become available, you agree to be bound by the rules, which have been communicated to you, concerning these services.

Inactive Accounts

If during a consecutive 180 day period you do not access the Bank's Business Online Banking, the Bank reserves the right to terminate your access privileges. If you wish to reactivate your Business Online Banking service, new agreements and applications need to be completed and executed.

Duty to Examine Bank Statements

You will not receive a separate Online Banking statement. All of the transfers and transactions made through Online Banking will appear on your monthly account statement. In order to preserve all of your rights, you must examine the statement and the transactions appearing on it and notify us in writing of any error; irregularity or discrepancy appearing on the statement within sixty (60) calendar days after the statement is made available to you. If written notice is not received by us within the 60-day period, then the statement will conclusively be deemed to be correct and you shall thereafter be precluded from asserting such error, irregularity or discrepancy against us.

Balance Reporting

We will provide the current balance, available balance and previous statement balance and transaction information on your Account(s).

Transfers between Accounts

You are responsible for the input and accuracy of all of the information you input into the Online Banking system. We will not verify the accuracy of the information you input. Should there be any conflict between an account number and an account name; the transaction will be processed based on the account number.

You must have sufficient available funds in your Account to cover the transfer amount. We may complete transfers that exceed your available balance, but we are not obligated to do so. If we complete the transfer, you agree to immediately pay any resulting overdraft in your Account. We will not notify you if we do not complete a transfer due to insufficient or unavailable funds in your Account.

We may also reject a transfer request if (1) we in good faith, believe that the transaction was not be authorized by you; (2) it contains incorrect, incomplete or ambiguous information; or (3) it involves funds subject to a lien, hold, dispute or legal process which prevents their withdrawal. We shall incur no liability to you or to any third person occasioned by our refusal to make such transfer.

Transfers between your Accounts initiated prior to 7:00 p.m. Eastern Time on any business day will be effective as of the close of business on that day. Transfers initiated after 7:00 p.m.

Eastern Time on any business day, or on a day which is not a business day, will be effective as of the close of business on the next business day.

Cancellation of Internal Transfers

Express transfers cannot be canceled or changed once accepted by Online Banking. To correct a transfer accepted by Online Banking, you must first enter an opposite entry, which will reverse the original transfer. Next, re-enter the transfer correctly. Scheduled transfers can be canceled or changed up until the day before the scheduled date.

Stop Payment Orders

You may use Online Banking to: (1) place a stop payment order; (2) view an existing stop payment order; or (3) determine whether a check or other debit item has been paid. Any stop payment placed via the Online Banking system will automatically expire six (6) months from date you place the stop payment order.

You may initiate stop payment orders via Online Banking only for paper checks you have written (non-electronically) on your Account. Before placing a stop payment order, you must first verify that the check has not been paid by the Bank. We use a computer system to stop payment. Accordingly, the stop payment order must exactly identify the correct account number, the correct check number and the dollar amount of the check (to the penny). Other information about the check to be stopped must be

reasonably accurate.

We may also require you to put your stop payment order in the form of paper writing and send that paper writing to us within 14 calendar days of your placing the stop payment order.

There is a fee for placing a stop payment order.

Account Information Disclosure

We will disclose information to third parties about your Account or the transfers you make:

- Where it is necessary for completing transfers, or
- In order to verify the existence and condition of your Account for a third party, such as a credit bureau or merchant, or
- In order to comply with government agency or court orders, or
- If you give us your written permission.

Error Resolution Notice

In Case of Errors or Questions about Your Electronic Transfers, telephone us at (609) 921-1700 or write us at The Bank of Princeton, 183 Bayard Lane Princeton NJ 08540, as soon as you can, if you think your statement or receipt is wrong or if you need more information about a transfer listed on the statement or receipt. We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error appeared.

- Tell us your name and account number (if any).
- Describe the error or the transfer you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information.
- Tell us the dollar amount of the suspected error

If you tell us orally, we may require that you send us your complaint or question in writing within 10 business days.

We will determine whether an error occurred within 10 business days after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days to investigate your complaint or question. If we decide to do this, we will credit your account within 10 business days for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not credit your account.

For errors involving new accounts, we may take up to 90 days to investigate your complaint or question. For new accounts, we may take up to 20 business days to credit your account for the amount you think is in error.

We will tell you the results within three business days after completing our investigation. If we decide that there was no error, we will send you a written explanation. You may ask for copies of the documents that we used in our investigation.

No Signature Required

When using the Bank's Business Online Banking to conduct banking transactions, you agree that we may debit your account to complete the banking transactions requested without your signature.

Your Liability for Unauthorized Transactions

Tell us AT ONCE if you believe your password has been lost or stolen, or if you believe that an electronic fund transfer has been made without your permission. Telephoning is the best way of keeping your possible losses down. You could lose all the money in your account (plus your maximum overdraft line of credit). If you tell us within 2 business days after you learn of the loss or theft of your password, you can lose no more than \$50 if someone used your password without your permission.

If you do NOT tell us within 2 business days after you learn of the loss or theft of your password, and we can prove we could have stopped someone from using your password without your permission if you had told us, you could lose as much as \$500.

Also, if your statement shows transfers that you did not make, tell us at once. If you do not tell us within 60 days after the statement was sent to you, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time. If a good reason (such as a long trip or a hospital stay) kept you from telling us, we will extend the time periods.

The Bank's Liability

If we do not complete a transfer to or from your account on time or in the correct amount, we will be liable for your losses or damages. However, there are some exceptions. We will not be liable, for instance:

- (1) If, through no fault of ours, you do not have enough money in your Account to make the transfer.
- (2) If the transfer would go over the credit limit on your overdraft line.
- (3) If the Online Banking system was not working properly and you knew about the breakdown when you started the transfer.
- (4) If circumstances beyond our control (such as fire or flood) prevent the transfer, despite reasonable precautions that we have taken.
- (5) There may be other exceptions stated in this and our other agreements with you.

Exclusion of Consequential, Indirect or Punitive Damages; Mitigation

In no event will we be liable for any present or future consequential, indirect, special or punitive damages, even if we have first been advised of the possibility of such damages. You agree to take all reasonable actions to mitigate any loss or damages.

Change in Terms

We may change the terms of this Agreement from time to time. We may also change the fees and service charges, add new fees and service charges, or make other changes to our fees and charges from time to time. If a change in terms would result in increased fees for any Online Banking service, increased liability for you, fewer types of available electronic fund transfers, or stricter limitations on the frequency or dollar amount of transfers, we will give you notice at least 21 days before the effective date of any such change, unless an immediate change is necessary to maintain the security of an account or the Online Banking system. We will mail or deliver a written notice to you of the change and post a notice of the change on the Bank's website. If advance notice of the change is not required by law, and disclosure does not jeopardize the security of your Account or the Online Banking system, we will notify you of the change in terms within 30 days after the change to Online Banking is effective. Your continued use of any or the Online Banking services means that you accepted and agreed to the change in terms.

Consent to Electronic Delivery of Notices

You agree that any notice or other type of communication provided to you pursuant to the terms of this Agreement, and any future disclosures required by law, including electronic fund transfer disclosures, may be made electronically by posting the notice on the Online Banking system website, the Bank's website or sent to you by e-mail. You agree to notify us immediately of any change in your e-mail address.

Termination

You may terminate this Agreement at any time for any reason by calling us at (609) 921-1700 or by sending a written notice of termination to us at The Bank of Princeton, 183 Bayard Lane Princeton NJ 08540

We may terminate this Agreement or suspend your access to Online Banking Services at any time for any reason without notice to you.

Neither termination nor suspension will affect either party's rights or obligations under this Agreement.

Inconsistent Terms

In the event of any inconsistency between this Agreement and the terms of the deposit account agreement between you and us, then the terms of this Agreement shall control.

Entire Agreement

This Agreement constitutes the entire agreement between you and us with respect to Online Banking Services. There are no understandings or agreements relative to Online Banking services not expressed in this Agreement.

RESTRICTIONS ON USE

Customer agrees not to use Business Online Banking or its Software in or for any illegal, fraudulent, unauthorized or improper manner or purpose and will use Business Online Banking in compliance with all applicable laws, rules and regulations, including all applicable state, federal, and international internet, data, telecommunications, telemarketing, "spam," and import/export laws and regulations, including the U.S. Export Administration Regulations. Without limiting the foregoing, customer agrees that they will not use Business Online Banking or the Software to transmit or disseminate: (i) junk mail, spam, or unsolicited material to persons or entities that have not agreed to receive such material or to whom customer does not otherwise have a legal right to send such material; (ii) material that infringes or violates any third party's intellectual property rights, rights of publicity, privacy, or confidentiality, or the rights or legal obligations of any wireless service provider or any of its clients or subscribers; (iii) material or data, that is illegal, or material or data, as determined by the Bank (in its sole discretion), that is harassing, coercive, defamatory, libelous, abusive, threatening, obscene, or otherwise objectionable, materials that are harmful to minors or excessive in quantity, or materials the transmission of which could diminish or harm the reputation of the Bank or any third-party service provider involved in the provision of Business Online Banking; (iv) material or data that is alcoholic beverage- related (e.g., beer, wine, or liquor), tobacco-related (e.g., cigarettes, cigars, pipes, chewing tobacco), guns or weapons-related (e.g., firearms, bullets), illegal drugs-related (e.g., marijuana, cocaine), pornographic-related (e.g., adult themes, sexual content), crime-related (e.g., organized crime, notorious characters), violence-related (e.g., violent games), death-related (e.g., funeral homes, mortuaries), hate- related (e.g. racist organizations), gambling-related (e.g., casinos, lotteries), specifically mentions any wireless carrier or copies or parodies the products or services of any wireless carrier; (v) viruses, Trojan horses, worms, timebombs, bots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data, or Business information; (vi) any material or information that is false, misleading, or inaccurate; (vii) any material that would expose the Bank ,any third- party service provider involved in providing Business Online Banking, or any other third party to liability; or (viii) any signal or impulse that could cause electrical, magnetic, optical, or other technical harm to the equipment or facilities of any supporting third party. Customer agrees that they will not attempt to: (a) access any software or services for which their use has not been authorized; or (b) use or attempt to use a third party's account; or (c) interfere in any manner with the provision of Business Online Banking or the Software, the security of Business Online Banking or the Software, or other customers of Business Online Banking or the Software; or (d) otherwise abuse Business Online Banking or the Software.

Governing Law

This Agreement is governed by applicable federal law and the laws of the State of New Jersey (to the extent that New Jersey law is not preempted by federal law). New Jersey law will be applied without giving effect to its principles of conflicts of laws.