Whitaker Bank Corporation's Online Banking (WeB)
Personal Enrollment Agreement

Whitaker Bank Corporation's Online Banking Enrollment Agreement ("Agreement") governs use of the Whitaker Bank Corporation ("WBC") Online Banking Service, Whitaker electronic Banking ("WeB"). As used in this document, the words "you" and "your" refer to Whitaker Bank Corporation's customer(s) and their use of WeB. The words "we" and "our" refer to WBC.

INTRODUCTION

This Agreement explains the terms and conditions governing WeB offered through WBC. By accepting below or by otherwise using WeB, you agree to the terms and conditions of this Agreement. The terms and conditions of the deposit agreements and disclosures for each of your accounts held at WBC as well as any other agreements with WBC, such as for loans, etc., continue to apply notwithstanding anything to the contrary in this Agreement. This Agreement will be governed by and interpreted in accordance with Federal laws and regulations, or to the extent there is no applicable Federal law or regulation, by the laws of the State of Kentucky. By accepting below or otherwise using WeB, you agree to use WeB only for bona fide and lawful purposes permitted under this Agreement.

INTERNET BROWSER REQUIREMENT

For your privacy and protection, WBC requires your browser to support 128-bit encryption. If you do not know how your browser is set, please contact your browser supplier and ask them for instructions on setting your browser for 128-bit encryption. You are responsible for the installation, maintenance, and operation of your computer and your browser software. The risk of error, failure, or non-performance is your personal risk and includes, but is not limited to, the risk that you do not operate your computer, WeB, or your software properly. WBC is not responsible for any problems related to electronic virus(es) that may infect your system. WBC makes no warranty to you regarding your computer or your software.

ACCESS

To use WeB, you must have a WBC checking (DDA) or savings account and access to Internet services. Once you have accepted this Agreement, we will send you, either by e-mail or by postal service, confirmation of your enrollment and that you may access WeB using the User ID and Password you created during enrollment. For banking transactions, you must use the appropriate functions within WeB or visit your local WBC branch office.

YOUR PASSWORD

Your new WeB password will be determined by you and will not be accessible by WBC. You are responsible for keeping your passwords, account number(s) and other account information confidential. WBC strongly recommends you do not authorize any other person to use your passwords. If you do authorize any other person to use your passwords, such authorization will be at your own risk and shall be deemed to be without limitation. WBC and each biller shall be entitled to rely on any payment orders or other entries or instructions made by or on behalf of such person using your passwords until you have met all of the following requirements: (1) you have revoked such authorization; (2) you have changed your passwords; (3) you have provided us with written notice of such revocation; and (4) WBC has had a reasonable opportunity to act on such notice. Upon three unsuccessful attempts to use your WeB login and/or password, access to WeB will be revoked. To re-establish your password to use WeB, to report that your WeB password may have been lost or stolen, or to report that someone has transferred or may transfer money from your account without your permission, immediately notify Customer Service at your local WBC office.

SECURITY

Your role in preventing misuse of your account(s) is extremely important. Examine your statement promptly upon receipt. If you find that your records and WBC's disagree, immediately call Customer Service at any WBC branch. In addition to protecting your account information, you agree to take precautions to protect your personal identification information, such as your driver's license, social security number, etc. This information by itself or together with information on your account(s) may allow unauthorized access to your account(s). You agree to notify WBC immediately if you believe another person has improperly obtained your WeB password(s). You also agree to notify WBC if someone has transferred or you suspect someone may transfer money from your account(s) without your permission, or if you suspect any type of fraudulent activity on your account(s). Only reveal your account number(s) to a legitimate entity for a purpose you authorize (such as your insurance company for automatic payments). You could lose all the money in your bank account(s), plus your maximum overdraft allowance and/or line-of-credit, if applicable. WBC will not be responsible for losses that may occur.

CONSUMER LIABILITY FOR UNAUTHORIZED USE

Your account is a consumer account if it is used primarily for personal, family or household purposes. The following three paragraphs apply to consumer accounts. If your statement shows transfers that you did not make, you agree to notify WBC immediately. If you do not notify us within sixty (60) days following the date of the first bank statement on which the problem first occurred, you may not receive any reimbursement for money lost after the said sixty (60) days. If you believe your password has been lost or stolen, and you inform us within two (2) business days after you learn of the loss or theft, your maximum loss is $50

if someone used your password without your permission. If you do NOT tell us within two (2) business days after you learn of the loss or theft, and WBC could have stopped someone from using your password without your permission if you had told us, your maximum loss is $500.

SERVICES

With WeB, you can manage your personal, sole-proprietor, or business account(s) from your home or office on your personal computer. You can use WeB to view account balances and transaction histories, pay bills, and transfer money between your accounts (as noted in the applicable account deposit agreement and disclosure statement.)

FEES & CHARGES

There are currently no additional fees for accessing your account(s) through WeB

ACCOUNT TERMINATION

If you close all WBC accounts, you must notify WBC Customer Service to cancel WeB. You agree to be responsible for any telephone charges or other out-of-pocket expenses incurred or related to the use of WeB.

OVERDRAFTS

If your account has insufficient funds to cover all the transactions requested for a given business day, certain electronic funds transfers involving currency disbursement, such as ATM withdrawals or pre-authorized transactions, will have priority. Other transactions, such as electronic funds transfers initiated through WeB, may result in overdrawing your account and/or may, at WBC's discretion and without prior notification to you, be canceled. In addition, all overdraft charges that apply will be debited from your account. You also authorize WBC to charge any or all of your accounts to cover uncollected funds or overdrafts in your designated account(s). Refer to our Checking Account Truth in Savings Disclosures for further information.

DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY

WBC makes no warranty of any kind, expressed or implied, including any implied warranty of merchantability or fitness for a particular purpose, in connection with WeB as provided to you under this Agreement. We do not and cannot warrant that WeB will operate without errors or that any or all WeB services will be available and operational at all times. Except as specifically provided in this Agreement or where the law requires a different standard, you agree that neither we, nor the service providers, shall be responsible for and you hereby release and discharge WBC and all such service providers from any loss, property damage, or bodily injury whether caused by the equipment, software, WBC, Internet browser providers, Internet access providers, online service providers, or by an agent or subcontractor of any of the foregoing. Nor shall we or the service providers be responsible for any direct, indirect, special, consequential, economic or other damages arising in any way out of the installation, use or maintenance of the equipment, software, online financial services, or Internet browser or access software.

HOURS OF ACCESS

You can access your WBC account(s) through WeB seven days a week, 24 hours a day. However, at certain times, WeB may not be available due to system updates, planned maintenance or other maintenance.

POSTING OF TRANSFERS

A transfer initiated through WeB before 8:00 PM Eastern Standard Time on a business day is posted to your account the same day and will be available to you the next business day. All transfers completed after 8:00 PM Eastern Standard Time on a business day or on a Saturday, Sunday or banking holiday, will be posted on the next business day and be available the following business day

TRANSFERRING FUNDS

Transfers may be subject to limitations based on individual account types. If a hold has been placed on a deposit(s) made to an account from which you wish to transfer funds, you cannot transfer the portion of the funds being held until the hold expires.

OBTAINING ACCOUNT BALANCES AND TRANSACTION HISTORIES

You can obtain balances and transaction histories on all eligible accounts. Current balance and activity information is available the morning following the previous day's business.

BILL PAY

Allows you to schedule bill payments through WBC's Bill Pay service. You may schedule payments for your current, future and recurring bills from your WBC checking account(s). By signing up for Bill Pay you will agree to the terms and conditions that must be acknowledged during signup.

BILL PAY SERVICE FEES

If a payment is not scheduled and paid within a 90 day period, bill payment service will be suspended.

Additional Charges for Customer requested Services and Other Items. These charges will only be assessed if you request one or more of the services listed below:

Same Day Bill Pay Fee: $9.95

Stop Payment Fee: $20.00

Current NSF/OD fees will be charged if your account does not contain sufficient available funds to complete the transaction, or the transaction would exceed the credit limit of your overdraft protection account. This also includes cases where the funds in your account are subject to legal processes, an uncollected funds hold or other cases where the funds are not available for withdrawal.

CHANGES IN TERMS

We reserve the right to change any terms or conditions described in this Agreement without notice, except when notice is required by applicable Federal and/or State law. Notification will be posted or sent at least thirty (30) days in advance of the effective date of any fee increase for online banking transactions, any decrease to type of transactions allowed, any decrease to the amount or frequency of transactions allowed, or any increase in your responsibility for unauthorized transactions, unless an immediate change is necessary to maintain the security of the system. If such a change is made for security reasons and it can be disclosed without jeopardizing the on-going security of the system, we will provide you with written notice within thirty (30) days after the change. As always, you may choose to accept or decline changes by continuing or discontinuing the account(s) or service(s) to which these changes relate.

DISCLOSURE OF ACCOUNT INFORMATION AND TRANSFERS

You understand and agree that in addition to information furnished pursuant to legal process, some information about your account(s) may be disclosed to others. For example, the tax laws require disclosure to the government of the amount of interest you earn, and some transactions, such as certain large currency or foreign transactions must be reported to the government. WBC may also provide information about your account(s) to persons or companies WBC believes would use the information for reasonable purposes, such as when a prospective creditor seeks to verify information you may have given in a credit application or a merchant calls to verify a check you have written. In addition, WBC may inform a credit bureau or collection agency when accounts are closed by WBC because they were not handled properly. Disclosure of any information should be in accordance with all applicable Federal and/or State laws and regulations. WBC may also seek information about you from others, such as a credit report from a credit bureau, in connection with the opening or maintaining of your account(s), and by accepting this agreement, you give us authority to provide or obtain all the above information.

YOUR RIGHT TO TERMINATE

You may cancel WeB at any time by providing us with written notice via postal mail or fax. Within three (3) business days of receiving instructions, your access to WeB will be suspended. You will remain responsible for all outstanding fees incurred prior to WBC receiving and processing your cancellation. You may also cancel WeB by contacting Customer Service at your local WBC branch.

OUR RIGHT TO TERMINATE

Your WeB access may be canceled by WBC at any time, without prior notice and for any reason. After cancellation, WeB service may be reinstated at WBC's discretion. To reinstate your service, contact your local WBC Customer Service Representative. If you do not access your WBC account(s) through WeB for a one-year period, WBC reserves the right to disconnect your service without notice.

COMMUNICATIONS WITH WHITAKER BANK CORPORATION OF KENTUCKY

Telephone – Please call your local WBC Branch Representative
In Person – You may visit us at any of our branch locations
Secure Email Message through Online Banking

DELIVERY OF ACCOUNT STATEMENTS

By accepting below or by otherwise using WeB, you are consenting to receive from us by e-mail only notification that your account statement(s) are available to view through WeB. Your periodic online statement and accompanying legal notices and disclosures will be presented to you via WeB. An electronic notification will be sent at the end of each statement cycle alerting you that the most recent statement is available for viewing.

All statements are in a format that can be printed or saved to your computer for your future reference. If you close an account, you will no longer be able to view that account online. You may request that a copy of your current or a previous statement be mailed to you at your home address. There could be a fee associated with this request. If you currently receive duplicate statements at the same address, mailing of the duplicate copy will be discontinued; however, you can print multiple copies of your statement through the Service. If you currently have statements mailed to an interested party, i.e., a statement mailed to your accountant, mailing of the interested party statement will be discontinued; however, you can forward your statement to your interested party at your own discretion.

This electronic delivery of your account statement(s) is known as eStatements. You will receive your account statement(s) from us in this manner, unless you discontinue the use of WeB. You may request a paper copy of any account statement you have received electronically, although fees may apply. If your e-mail notification is undeliverable, we will make a reasonable effort to notify you. It is your responsibility to notify WBC if your e-mail address has changed.

RECOMMENDED FINANCIAL AND INFORMATION SECURITY PRACTICES

Use Personal Financial Information and Financial Services Passwords Only in Secure Transactions

- Personal financial information (such as names in combination with Social Security Numbers, account numbers, and credit or debit card numbers) and passwords for financial services (such as online and mobile banking / payments, and person-to-person payments) should only be used in secure transactions using the practices described below.
- Personal financial information and passwords for financial services should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages.
- If you provide financial information and passwords for financial services in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages, you should change your passwords as quickly as possible.

Use Strong Passwords in All Systems That Require Passwords

- Passwords should use the maximum allowable number and type of characters (such as upper- and lower-case letters, numbers and symbols) and should not contain predictable terms or numbers.
- A different password should be used for each commercial and financial services website.
- Passwords that are written down or otherwise recorded should not be placed in visible or unsecured locations.

Approach Applications and Links on All Devices and Delivery Channels with Caution

- Approach all applications and links on all devices (such as personal computers, tablets and cell phones) and delivery channels (such as email, text messages and social media sites) with caution, as cybercriminals often use applications and links as the first step in installing malicious software on devices with which fraudulent acts can be enabled.
- Take steps to verify that applications and links posted on social media sites correspond to legitimate websites, and that they have been posted by individuals who are known and trusted.

Use Computers and Online Banking, Bill Payment and Shopping Securely

- Antivirus protection and scanning software that has been reviewed and rated as satisfactory by independent analysts should be installed, updated and utilized as recommended. In addition:
    - If the security software can update automatically, set it to do so.
    - If the security software cannot update automatically, update it after each login.
    - If viruses (also referred to as “malicious software” or “malware”) are detected, the recommendations provided by the antivirus program should be followed promptly.
- Operating system software updates (also referred to as “patches”) should be accepted, downloaded, installed and run promptly, and as recommended.
- Personal financial information should never be sent by email in an unencrypted state.
- Financial transactions that are conducted on websites should be conducted on secure websites only. An indicator of a secure website is a URL that begins with “https” in the address, the “s” standing for “secure.” The “https” prefix should be on every page of websites used to conduct transactions, in addition to the sign-in page.
- Privacy policies should be easily found and understood. If the privacy policy is not easily found and understood, then consider conducting business elsewhere. Privacy policies provided by financial institutions in connection with financial services are required to offer consumers a clear method to “opt out” of certain types of information sharing if the institution engages in them.
- Most Wi-Fi networks do not encrypt information and are not secure. Some use encryption and are more secure. However, if any Wi-Fi network is to be used, a virtual private network (VPN) should be established and used to encrypt communications. VPN encryption applies all the way from the user’s PC to the host computer, regardless of the type of network used. The encryption methods used by VPN are stronger than those used by Wi-Fi networks.

- Unfamiliar or suspicious emails, text messages, instant messages, phone calls, websites and social media solicitations that request personal financial information should be deleted immediately. They should not be replied to or forwarded, and any links that they contain should not be opened.
- Options to "Remember me" on websites where transactions are conducted should not be used.
- Computer workstations and laptops should be logged off, and preferably not left on, when the user steps away.
- Computer workstations and laptops should be set to logoff automatically after no more than two minutes of non-use, with a password required to log back in.
- Computer workstations, laptops and external storage devices such as USB drives and storage discs should be physically secured with locks (such as with a cable lock or in a locked drawer) when not in use.
- Computers that are no longer in use should have hard drives removed and shredded, or a software program that wipes and eliminates all data from their hard drives should be used, following DoD 5220.22M standards for data sanitization.

Use Mobile Phones, Mobile Banking and Mobile Payments Securely

- Mobile phone applications, text messages, instant messages and calls from unfamiliar or suspicious sources that request personal financial information and passwords should be declined and, when appropriate, promptly deleted, and not replied to or forwarded. Any links they contain should not be opened.
- Each mobile phone and mobile phone application should be assigned a different password with the maximum allowable number and type of characters.
- Mobile phones should be set to log off automatically after no more than two minutes of non-use, with a password required to log back into the phone.
- Mobile phones should be locked up when not in use and not left in visible, unsecured locations.
- Lost or stolen phones should be reported to the carrier promptly.

Use ATM, Credit, Debit and Prepaid Cards Securely

- Cards should be signed as soon as they arrive.
- Card numbers should only be used in secure transactions and should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages.
- If conducted on websites, card transactions should be conducted only on secure websites. An indicator of a secure website is a URL that begins with "https" in the address, the "s" standing for "secure." The "https" prefix should be on every page of websites used to conduct transactions, in addition to the sign-in page.
- Options to "Remember my card number" on websites where transactions are conducted should not be used.
- Cards should not be left in visible or unsecured locations.
- Lost or stolen cards should be promptly reported to the card issuer.
- Cards that are unused, have been canceled or have been replaced by a new card should be securely eliminated, for example by cutting them into small pieces so they cannot be read.

Use Checks Securely

- Checks should not have Social Security Numbers or driver's license numbers printed or written on them.
- Checks should not be left visible in unsecured locations.
- Checks that are to be discarded should be eliminated securely, for example by shredding, and should not be discarded in a readable form.
- Checks that are tamper resistant are available at certain financial institutions. These checks include security features such as chemically sensitive paper to deter alterations.

Use Statements and E-Statements, Bills and E-Bills, and Transaction Receipts Securely

- Statements, e-statements, bills and e-bills should be reviewed promptly upon receipt to verify that all transactions were made by authorized parties; any transactions made by unauthorized parties should be reported to the appropriate financial institution, card issuer or biller.
- Transaction receipts should be saved and compared to statements to ensure that unauthorized charges have not been added. Any transactions made by unauthorized parties should be reported to the appropriate financial institution, card issuer or biller.
- Incorrect transaction receipts should be voided.
- Blank transaction receipts should not be signed. Draw a line through any blank spaces above the total on any transaction receipt that is to be signed.
- Statements, bills and transaction receipts that are to be discarded should be eliminated securely, for example by shredding, and should not be discarded in a readable form.
- Financial institutions, card issuers and billers should be notified in advance of a change of address.

Use Social Media Securely

- The highest available level of privacy and security settings should be selected and activated on any social media site.
- No information that can be used to compromise information security should be viewable on any social media site. Such information includes the names of financial institutions, card companies, commerce websites, Internet service providers, utilities and wireless carriers with which you have accounts. This also includes personal financial information, passwords, phone numbers, email addresses, addresses and dates of significance (for example, birth dates and anniversaries).
- Accept only known and trusted individuals into your social network.
- Do not allow social media sites to scan your address book.

Monitor Credit Accounts

- Credit accounts and reports should be monitored regularly. Any unauthorized or suspicious activity should be reported promptly to the appropriate financial institution, card issuer, local law enforcement agency and the Federal Trade Commission (877-438-4338, or online at www.consumer.gov).
- As a precaution, you may choose to place a fraud alert on your credit file. A fraud alert will notify you before unauthorized third parties open new accounts in your name or charge existing accounts in your name. This can be done at no charge to you. To receive fraud alerts, contact Equifax® (800-525-6285), Experian® (888-397-3742) or TransUnion® (800-680-7289).

ELECTRONIC DELIVERY OF NOTICES

By accepting below or by otherwise using WeB, you also agree that any and all disclosures and communications regarding WeB between you and WBC, including this Agreement, may be made electronically by posting to the WBC web site in accordance with applicable law. Any electronic disclosure or communication we make will be considered made when transmitted by WBC, and any disclosure or communication we make by posting to our web site will be considered made when posted by WBC.

EXCEPT AS SPECIFIED ABOVE, OR AS MAY OTHERWISE BE PROVIDED BY LAW, WBC SHALL HAVE NO LIABILITY FOR ANY ACT OR OMISSION IN CONNECTION WITH WeB. WBC'S CUMULATIVE LIABILITY IN ANY ONE CALENDAR YEAR, SHOULD IT BE FOUND TO EXIST NOTWITHSTANDING THIS PROVISION, SHALL NOT EXCEED THE FEES YOU HAVE PAID FOR WeB IN THAT CALENDAR YEAR. WBC HEREBY DISCLAIMS, FOR ITSELF AND/OR ANY OTHER ENTITY INVOLVED IN THE PROVIDING OF WeB, ALL WARRANTIES, EITHER EXPRESSED, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR LACK OF VIRUSES. IN NO EVENT SHALL WBC OR ANY OTHER ENTITY INVOLVED IN THE PROVIDING OF WeB BE LIABLE FOR (1) DAMAGES CAUSED OTHER THAN BY ITS OWN GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT, OR (2) INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES.

BY CLICKING "I AGREE" YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. YOU ALSO AUTHORIZE WBC TO SEEK INFORMATION ABOUT YOU FROM OTHERS, FOR EXAMPLE A CREDIT REPORT FROM ANY CREDIT BUREAU(S) SELECTED BY WBC, IN CONNECTION WITH THE OPENING AND MAINTAINING OF YOUR ACCOUNT(S).

Revised: April 2024