



Protecting your identity and financial information are top priorities at Tioga Franklin Savings Bank. Before initiating your Internet Banking, we first require that a "secure session" is established using 256 BIT Secure Socket Layer (SSL) encryption. This encrypts or scrambles information between our server and your browser so it cannot be read by unauthorized parties. Generally, a URL (web page address) with the prefix "https" (as opposed to "http") indicates a secure site.

Security refers to preventing unauthorized access to a computer system or network. Internet Banking uses several layers of technology to prevent unauthorized users from gaining access to the internal network. Our Internet Banking security professionals manage a sophisticated networking architecture that includes screening routers, filtering routers, and firewalls.

The Internet Banking section is automatically secured/encrypted, but the rest of the website can be accessed as either secure or unsecure. Internet Banking is a term for accessing your account information over the Internet. We may refer to it as Internet Account Access, Online Banking or a different name.

Secure Sign-on with Online Banking

Our state-of-the-art technology and Multi-factor Authentication (MFA) helps protect the security of your online sessions by adding an additional layer of security for your personal and financial information, to protect you while you are banking online.

What is Multi-factor Authentication (MFA)?

We make banking easy and convenient for you with online banking tools that include sophisticated security features. Your online banking experience may include a new Enhanced Login Security service to further protect you from identity theft: this extra protection is known in the online security industry as Multi-factor Authentication, or MFA.

Authentication is the process used to allow access to only the correct customer. Without effective authentication controls, it is possible for fraudulent users to access your account. We authenticate customers by issuing challenges that only the actual customer should be able to pass.

MFA means that two or more different types (or factors) of authentication must be passed. By using two different factors of authentication, we get a higher assurance that the customer is the intended user. MFA is commonly used to protect transactions at ATMs: for example, your card is a factor you have, and your PIN code is a factor you know.

For your convenience, after you successfully authenticate with your Access ID, password and Login Security (One-Time Passcode [OTP] or Challenge Questions, if available), you may enroll your computer for use in authentication. If you choose to enroll your computer, a special browser "cookie" will be present on the system, which will act in place of your phone for a factor that you have in your possession.

We recommend you ensure that your browser settings and any antivirus software you have do not delete your cookies (data files) so that you are not prompted to provide Login Security (One-Time Passcode [OTP] or Challenge Questions, if available) every time you log into Internet Banking.

Logging in from a computer you normally use?

When you choose to enroll your computer as PRIVATE, a special browser cookie will be present on the system, which will act in place of your Login Security (One-Time Passcode [OTP] or Challenge Questions, if available). You will only need your Access ID and password to access your account information.

If you are still getting prompted to provide your Login Security, then please ensure that you have the following:

You are using one of the Recommended Operating Systems for Internet Banking

You are using one of the Recommended Browsers for Internet Banking

Browser is not set to delete cookies (please follow the steps listed in the online banking HELP Section for your respective browser to determine if cookies are being deleted)

Any antivirus software is not set to delete cookies

No viruses or malware on your computer

No usage of a proxy server or “web accelerator” by your internet service provider (ISP)

If using a computer from work, verify that your office technical department is not automating deletion of cookies.

Logging in from a computer you DO NOT normally use?

When you choose to list your computer as PUBLIC, you will need to provide your Access ID, password and you will be prompted to provide your Login Security (One-Time Passcode (OTP) or Challenge Questions, if available) each time you log into your account. We recommend this setting when logging in from a library or school computer.

Password Security

To ensure security, experts recommend that you never reveal your password**.

If you have questions about what to enter in order to access Internet Banking for the first time, please call our customer service team at 215-423-8012.

Some browsers allow you to enable a function to require passwords for specific sites or certifications. In that instance, you should enter the password for the browser.

Passwords are case sensitive. Mixing uppercase and lowercase letters is permitted.

You can change your Internet Banking password under My Profile/User Options at any time. It is recommended that you change your password every six months.

We do not have access to your password. If you forget your password and/or challenge questions, contact our customer service team at 215-423-8012 to request your password reset for Internet Banking.

Use the Sign Off Icon to End an Internet Banking Session

This will securely close out your Internet Banking session and expire all the cookies that were set in your session. Do not use the Back key.

If you do not exit the browser, the browser will allow you to use the Back key to get back into your Internet Banking session should you wish to explore another site.

The amount of time you can remain inactive before being automatically logged out of Internet Banking can be set under

User Options.

For your own security, keep this time setting as short as possible.

We recommend that you balance your account at least once a month so that any discrepancies can be reported in a timely manner.

More tips to help safeguard your money and personal information:

Stay up to date: Install anti-virus software on your computer and keep it updated. Use the latest version of your web browser. Install security patches and software updates as soon as they are ready to install.

Use wireless connections with caution: Whenever possible use only your personal/private computer to access your Online Banking. Wireless networks may not provide as much security as wired Internet connections. Many wireless networks in public areas like airports, hotels and restaurants reduce their security to make it easier for individuals to access these networks.

Go paperless: When available, enroll to receive electronic statements, it's safer, convenient, and it saves trees!

Mobile Banking

Tioga Franklin Savings Bank's built-in security features ensure your account information is protected. These security features include authentication checks via strong passwords before access to account information is granted. Mobile Banking requires "128-bit" encryption technology for all communications. Personal or financial information is retrieved only when requested and is not stored on your phone, so your information is not at risk if your phone is ever lost or stolen.

Tioga Franklin Savings Bank will NEVER contact you by telephone, send you an email or text message, or written communication on an unsolicited basis requesting that you validate or provide your online banking credentials including your Access ID, password, social security number, account number, or date of birth. If you receive any type of unsolicited requests supposedly from Tioga Franklin Bank asking for your personal information, or if you suspect you have become a victim of Identity Theft or fraud, please contact us immediately at 215-423-8012.

Some points for securing your online banking:

Maintain a current browser

Avoid downloading programs from unknown sources

Select unique and complex passwords

Avoid writing down login credentials

Maintain currently-supported Operating Systems on computing devices

Install current Operating System and software application security patches

Keep anti-virus and spyware protection up-to-date

Install a firewall and intrusion prevention system

Use a trusted, secure computing device for Internet banking – avoid public computers

Avoid public WiFi usage, especially when performing banking functions

Be aware and cautious of suspicious and unsolicited emails

Contact the Bank immediately upon suspected fraudulent activity

Never provide account login information over the phone or via email

Daily review of transaction history and account balancing

Setup the transaction alert notifications

Implement dual control for high-risk transactions

MOBILE BANKING AGREEMENT AND DISCLOSURE

ADDENDUM TO ONLINE BANKING AGREEMENT & DISCLOSURE

THERE IS NO CHARGE FOR MOBILE BANKING.



I. Introduction

As an additional delivery channel for our Online Banking service, Tioga-Franklin Savings Bank may provide to you mobile banking services which include, by way of example and not limitation, short message service (“SMS”) text banking, mobile web browser banking, and banking initiated by means of a downloadable application, accessible via a wireless handheld device such as a cell phone, smartphone, personal digital assistant or tablet computer (“Mobile Banking” or the “Service”). By enrolling in the Service, you agree to all the terms and conditions contained in this Agreement and Disclosure (the "Agreement"). We may offer additional Mobile Banking services and features in the future. Any such added Mobile Banking services and features will be governed by this Agreement and by any terms and conditions provided to you at the time the new Mobile Banking service or feature is added and/or at the time of enrollment for the feature or service, if applicable. From time to time, we may amend these terms and modify or cancel the Mobile Banking services we offer without notice, except as may be required by law.

This Agreement is an addendum to and supplements and amends any agreements you have entered into with Tioga-Franklin Savings Bank, including without limitation the Online Banking Agreement and Bill Payment Service Terms and Conditions. Any deposit account, loan or other banking product accessed through this Service is also subject to the Depositor or Loan Account Agreements and Disclosures provided at the time of Account opening, or as the same may be subsequently amended or modified. You should review the Account disclosures carefully, as they may include transaction limitations and fees which might apply to your use of the Service. You acknowledge that any such agreements are incorporated by reference into this Agreement in their entirety and that you remain subject to all the terms and conditions of such agreements, except to the extent they conflict or are inconsistent with this Agreement, in which case the terms and conditions of this Agreement will control.

IMPORTANT: READ THE TERMS OF THIS AGREEMENT CAREFULLY BEFORE USING THE SERVICE. THIS AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU AND TIOGA-FRANKLIN SAVINGS BANK CONCERNING THE SERVICE. BY SELECTING THE “I ACCEPT THESE TERMS AND CONDITIONS” CHECK BOX OR USING THE SERVICE, EACH AN ACCEPTANCE OF THIS AGREEMENT, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT.

II. Definitions

As used in this Agreement, the following words have the meanings given below:

"Account(s)" means your eligible Tioga-Franklin Savings Bank Checking, Savings, Certificate of Deposit, or Loan account that can be accessed through Mobile Banking.

“Deposit Account Agreement” means that by providing a written or electronic signature on a signature card or other agreement or contract, or by opening or continuing to hold an account with us, you agree to the current and subsequent terms and conditions on your account.

“Device” means a supportable mobile device including a cellular phone or other mobile device that is web-enabled and allows secure SSL traffic which is also capable of receiving text messages. **Your wireless carrier may assess you fees for data or text messaging services. Please consult your wireless plan or provider for details.**

“Disclosures” means information that we are required by law to provide or make available to you in writing - for example, Electronic Funds Transfers Disclosure, Funds Availability Disclosure, Truth in Savings Disclosures, privacy notice, adverse action notice, etc.

“Licensor” shall have the meaning as ascribed in Section VI.

“Licensor Software” shall have the meaning as ascribed in Section VI.

“Mobile Banking Software” shall have the meaning as ascribed in Section III.B.

“Software” means collectively or individually as the context may require, the Mobile Banking Software and the Licensor Software.

“Touch Banking” shall have the meaning as ascribed in Section VI.

“User Information” shall have the meaning as ascribed in Section VII.

“We,” “Us,” “Our” and “Bank” means Tioga-Franklin Savings Bank.

“You” and “Your(s),” mean each person with authorized access to your Account(s) who applies and uses the Service.

III. The Service

A. Description of Service. Mobile Banking is offered as a convenience to you and as a supplemental service to our Online Banking services. It is not intended to replace access to Online Banking from your personal computer or other methods you use for managing your Accounts and services with us. Mobile Banking allows you to access your Account information, make payments to existing payees, transfer funds and conduct other banking transactions.

B. Use of Service. In order to properly use Mobile Banking, you should review and follow the instructions provided on our website. You agree to accept responsibility for learning how to use

Mobile Banking in accordance with the online instructions and agree that you will contact us directly if you have any problems with Mobile Banking. We may modify the Service from time to time at our sole discretion. In the event of any modifications, you are responsible for making sure you understand how to use Mobile Banking as modified. Any use of the Service after the Bank provides you notice of such modification will constitute your agreement to such change(s). You must obtain and maintain, at your own expense, compatible hardware and software. We are not responsible for

the functionality or maintenance of any such hardware or software you may need to use the Service. You also accept responsibility for making sure that you know how to properly use your Device and we will not be liable to you for any losses caused by your failure to properly use the Service or your Device.

To enroll: To utilize the Service, you must be enrolled in Tioga-Franklin Savings Bank's Online Banking service and logon to request mobile banking, select mobile services, and activate your Device within the Online Banking system. Once your Account is activated you may log on to your Account from your Device using one of the Services provided. We reserve the right to limit the types and number of Accounts eligible and the right to refuse to make any transaction you request through Mobile Banking. We may also reserve the right to modify the scope of the Service at any time.

Mobile Banking may not be accessible or may have limited utility over some network carriers. In addition, the Service may not be supportable for all Devices. The Bank cannot guarantee and is not responsible for the availability of data services provided by your mobile carrier, such as data outages or "out of range" issues. Mobile Banking and any software you may obtain from Mobile Banking ("Mobile Banking Software") may not be available for reasons outside of the reasonable control of the Bank or any service provider. We do not assume responsibility or liability for any technical or other difficulties or any resulting damages that you may incur. We reserve the right to change, suspend, or terminate the Service or revoke your right of access to the Service immediately at any time and without notice to you.

Changes to your mobile number or device: If you purchase a new phone or device, but are using the same phone number and wireless mobile service provider you may have to reinstall previously downloaded applications. If you switch wireless mobile providers and/or phone numbers, you must log in to your Online Banking account on your personal computer and update your information by clicking on the Mobile Enrollment request link on the Requests page. You will not receive SMS Text messages regarding Mobile Banking transactions if your phone number is not correct.

Deactivate Service: If you no longer wish to have access to the Service you may deactivate the Service by logging on to your Online Banking account on your personal computer and updating your information by clicking on the Mobile Enrollment request link on the Requests page and deselecting "Mobile Access." You may also contact us directly in writing to request deactivation of the Service. Requests should be directed to: Tioga-Franklin Savings Bank, Online

Banking Department, 76 Engle Street, Englewood, NJ 07631.

C. Other Agreements. You agree that, when you use Mobile Banking, you remain subject to the terms and conditions of your existing agreements with any unaffiliated service providers, including, but not limited to, your mobile service provider and that this Agreement does not amend or supersede any of those agreements. You understand that those agreements may provide for fees, limitations and restrictions which might impact your use of Mobile Banking (such as data usage or text messaging charges imposed on you by your mobile service provider for your use of or interaction with Mobile Banking), and you agree to be solely responsible for all such fees, limitations and restrictions. You agree that only your mobile service provider is responsible for its products and services. Accordingly, you agree to resolve any problems with your provider directly without involving us.

D. Fees. There may be fees from the Bank for using Mobile Banking or any other service that can be accessed through Mobile Banking via Online Banking and Bill Pay. You agree that you are aware of the fees to use these services and you agree to pay for any fees generated by your use of these services. Fees may be automatically debited from your Account. The Service is separate and apart from any other charges that may be assessed by your wireless carrier for text messages sent to or received from the Bank. You are responsible for any fees or other charges that your wireless carrier may charge for any related data or message services, including without limitation for SMS.

IV. Permitted Mobile Banking Transfers.

You may use the Service to access your Accounts and conduct transfers that you agreed to in the Online Banking Agreement and Bill Payment Service Terms and Conditions. You must have sufficient funds available in the selected Account at the time the transfer request is received.

Federal regulations require financial institutions to limit the way withdrawals may be made from a savings or money market account. Each transfer from a savings or money market account using

Mobile Banking is counted as one of the six (6) limited transactions permitted each monthly statement cycle period, as described in the Deposit Account Agreement and Disclosures. You may be subject to fees or Account closure if you exceed the transaction limits of your Account using Mobile Banking or any other methods outlined in your Deposit Account Agreement and Disclosures.

You agree to confirm the completion of each transfer in your Account balance and transaction history before withdrawing transferred funds.

We may establish transaction limitations from time to time.

V. Your Responsibilities

You represent and agree to the following by enrolling in or using the Service:

A. Account Ownership/Accurate Information. You represent that you are the legal owner of the Accounts and other financial information which may be accessed via Mobile Banking. You represent and agree that all information you provide to us in connection with Mobile Banking is accurate, current and complete, and that you have the right to provide such information to us for the purpose of using Mobile Banking. You agree not to misrepresent your identity or your Account information. You agree to keep your Account information up to date and accurate. You represent that you are an authorized user of the Device you will use to access Mobile Banking.

B. User Security. You agree to take every precaution to ensure the safety, security and integrity of your Account and transactions when using Mobile Banking, including, if and when applicable, accepting all mobile application upgrades in a timely manner. You agree not to use any personally identifiable information when creating shortcuts to your Account. You agree not to leave your Device unattended while logged into Mobile Banking and to log off immediately at the completion of each access by you. You agree not to provide your username, password or other access information

to any unauthorized person, including anyone claiming to represent us. If you permit other persons to use your Device, login information, or other means to access Mobile Banking, you are responsible for closely and regularly monitoring their activities and any transactions they authorize, notifying the Bank immediately if you have any reason to believe the security or confidentiality required by this provision has been or may be breached, and immediately changing your password if you know or suspect the confidentiality of the password has been compromised in any way. We will not be liable for any damages resulting from these activities. We make no representation that any content or use of Mobile Banking is available for use in locations outside of the United States. Accessing Mobile Banking from locations outside of the United States is at your own risk. We reserve the right at all times to take actions to protect our systems and information, including denial of access to users of the Service.

C. User Conduct. You agree not to use Mobile Banking or the content or information delivered through Mobile Banking in any way that would: (a) infringe any third-party copyright, patent, trademark, trade secret or other proprietary rights or rights of privacy, including any rights in the

Software; (b) be fraudulent or involve the sale of counterfeit or stolen items, including, but not limited to, use of Mobile Banking to impersonate another person or entity; (c) violate any law, statute, ordinance or regulation (including, but not limited to, those governing export control, consumer protection, unfair competition, anti-discrimination or false advertising); (d) be false, misleading or inaccurate; (e) create liability for us or our affiliates or service providers, or cause us to lose (in whole or in part) the services of any of our service providers; (f) be defamatory, trade libelous, unlawfully threatening or unlawfully harassing; (g) potentially be perceived as illegal, offensive or objectionable; (h) interfere with or disrupt computer networks connected to Mobile Banking; (i) interfere with or disrupt any other user's use of Mobile Banking; or (j) use Mobile Banking in such a manner as to gain unauthorized entry or access to the computer systems of others.

D. No Commercial Use or Re-Sale. You agree that the Service is only for your personal use, or the use of individuals authorized to access your Account information. You agree not to make any commercial use of Mobile Banking or resell, lease, rent or distribute access to Mobile Banking.

E. Indemnification. You agree to indemnify, defend and hold harmless the Bank, its affiliates and our providers of services and their respective affiliates, and each of our and their respective officers, directors, employees, consultants, agents, shareholders, service providers and licensors from any and all third party claims, actions, losses, liability,

damages, expenses and costs (including, but not limited to, reasonable attorneys' fees) caused by or arising from (a) a third party claim, dispute, action, or allegation of infringement, misuse, or misappropriation based on information, data, files, or otherwise in connection with the Service; (b) your violation of any law or rights of a third party; (c) your violation of your responsibilities as described in this Agreement; or (d) your use, or a third party's use, of Mobile Banking.

VI. License and Use of the Downloadable Application (Touch Banking)

the Bank offers their customers mobile access to their Account information (e.g., for checking balances and last transactions) via a downloadable application, Touch Banking – Fiserv, Inc. (“Touch Banking”).

Ownership. You acknowledge and agree that a third party provider or licensor to the Bank ("Licensor") is the owner of all right, title and interest in and to the downloaded software used to

access the Service from the Bank and the computer programs contained therein in machine readable object code form as well as any accompanying user documentation along with all subsequent copies, updates or versions thereof which are made available to you (if any), regardless of the media or form in which they may exist (collectively, the "Licensor Software").

License. You must agree to, and you are subject to, the Touch Banking End User License Agreements in order to use the application.

Restrictions. You shall not: (i) modify, revise or create any derivative works of the Software; (ii) decompile, reverse engineer or otherwise attempt to derive the source code for the Software; (iii) redistribute, sell, rent, lease, sublicense, or otherwise transfer rights to the Software; or (iv) remove or alter any proprietary notices, legends, symbols or labels in the Software, including, but not limited to, any trademark, logo or copyright.

Disclaimer of Warranty. YOU ACKNOWLEDGE THAT YOUR USE OF THE SERVICE AND SOFTWARE IS AT YOUR OWN RISK AND DISCRETION AND ANY INFORMATION, CONTENT, MATERIALS THEREIN OR FUNCTIONS MADE ACCESSIBLE BY THE SERVICE OR SOFTWARE IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. NO WARRANTY IS PROVIDED THAT THE SERVICE OR SOFTWARE WILL BE FREE FROM DEFECTS OR VIRUSES OR THAT OPERATION OF THE SERVICE OR SOFTWARE WILL BE UNINTERRUPTED. YOU ARE SOLELY RESPONSIBLE FOR ANY DAMAGE RESULTING FROM THE USE OF THE SERVICE AND SOFTWARE AND ANY OTHER MATERIAL OR SERVICES DOWNLOADED OR MADE AVAILABLE TO YOU THROUGH THE SERVICE AND SOFTWARE.

Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR, THE BANK, OR ANY OF OUR OR THEIR RESPECTIVE OFFICERS, DIRECTORS,

EMPLOYEES, AGENTS, CONTRACTORS OR PROVIDERS OR ANY OF OUR OR THEIR AFFILIATES BE LIABLE FOR ANY DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE SERVICE OR SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY THEREOF, AND REGARDLESS OF THE LEGAL OR EQUITABLE THEORY (CONTRACT, TORT OR OTHERWISE) UPON WHICH ANY CLAIM IS BASED. IN ANY CASE, LIABILITY OF LICENSOR, THE BANK, OR ANY OF THE OTHER PERSONS OR ENTITIES DESCRIBED IN THE PRECEDING SENTENCE ARISING OUT OF THE USE OR INABILITY TO USE THE SERVICE OR SOFTWARE SHALL NOT EXCEED IN THE AGGREGATE THE LESSER OF \$10.00 OR THE SUM OF THE FEES PAID BY YOU FOR THIS LICENSE.

VII. Privacy and User Information.

You acknowledge that in connection with your use of Mobile Banking, the Bank and its affiliates and service providers, including Fiserv, Inc. and its affiliates, may receive and may share with one another names, domain names, addresses, passwords, telephone and device numbers, the content of messages, data files and other data and information provided by you or from other sources in connection with Mobile Banking or the Software (collectively "User Information").

The Bank and its affiliates and service providers will maintain reasonable safeguards to protect the information from unauthorized disclosure or use, but reserve the right to use and disclose this information as reasonably necessary to deliver Mobile Banking and as otherwise permitted by law, including compliance with court orders or lawful instructions from a government agency, to protect the personal safety of subscribers or the public, to defend claims, and as otherwise authorized by you.

The Bank and its affiliates and service providers also reserve the right to monitor use of Mobile Banking and the Software for purposes of verifying compliance with the law, these terms and conditions and any applicable license, but disclaim any obligation to monitor, filter, or edit any content.

VIII. Restrictions on Use.

You agree not to use Mobile Banking or the Software in connection with any illegal, fraudulent, unauthorized or improper manner or purpose. The Service and Software will only be used 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, you agree that you will not use Mobile 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 you do 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 Mobile 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, time bombs, cancelbots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data, or personal 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 Mobile 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 Fiserv or any third party. You agree that you will not attempt to: (a) access any software or services for which your 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 Mobile Banking or the Software, the security of Mobile Banking or the Software, or other customers of Mobile Banking; or (d) otherwise abuse Mobile Banking or the Software.

Miscellaneous. This Agreement constitutes the entire agreement between the parties concerning the subject matter hereof. This Agreement will be governed by and construed in accordance with the laws of the state of Pennsylvania, excluding that body of laws pertaining to conflict of laws. If any provision of this Agreement is determined by a court of law to be illegal or unenforceable, such provision will be enforced to the maximum extent possible and the other provisions will remain effective and enforceable. All disputes relating to this Agreement are subject to the exclusive jurisdiction of the courts of Pennsylvania and the parties expressly consent to jurisdiction and venue thereof and therein. The parties confirm that this Agreement and all related documentation is and will be in the English language. The application of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly waived and excluded.

Agreement and Acknowledgement. You expressly agree that you have carefully read this Agreement and will carefully read all materials provided by the Bank in connection with this Agreement and agree that these terms and conditions will control the obligations of the parties for the Service.

If you have any questions regarding the above disclaimers or need additional information regarding the Service, please contact us at 215-423-8012.