MID PENN BANK
ON-LINE ACCESS AGREEMENT
(BUSINESS ACCOUNTS)

Please read this Agreement carefully. Your first use of Mid Penn Bank's online banking system is your agreement with the terms and conditions set forth hereinto.

As a business customer of this Bank, you desire and request Mid Penn Bank to permit electronic on-line access to your accounts, which you own and maintain with the Bank, via the Bank's Internet Banking System (IBS), www.midpennbank.com (Website). No person who is not a party to this Agreement will have any rights or interest in this Agreement. This Agreement may not be assigned by you without prior written consent by us.

This Agreement, including the Regulation E Disclosure (Electronic Fund Transfers Your Rights and Responsibilities), is a contract that establishes the rules which cover your electronic access to your accounts at Mid Penn Bank through our Internet Banking System (System). By use of the System or permitting any other person to access and use the System, you agree to accept all the terms and conditions of this Agreement. Please read it carefully. You have designated authorized individual access to the System by the signed enrollment forms executed by your company (whether executed directly with Mid Penn Bank or the result of Mid Penn Bank acquiring a financial institution).

The terms and conditions of the deposit agreements and disclosures for each of your Bank accounts, where you are listed as an owner or signer, as well as your other agreements with Mid Penn Bank, such as loans, continue to apply notwithstanding anything to the contrary in this Agreement. This Agreement is also subject to applicable federal laws and the laws of the Commonwealth of Pennsylvania (except to the extent this Agreement can and does vary from such rules or laws). If any provision of this Agreement is found to be unenforceable according to its terms, all remaining provisions will continue in full force and effect.

The headings in this Agreement are for convenience or reference only and will not govern the interpretation of the provisions. Any waiver (express or implied) by either party of any default or breach of this Agreement must be in writing and shall not constitute a waiver of any other or subsequent default or breach.

This Agreement is binding upon all authorized signers and users as designated by the company and the Bank's successors and assigns. Certain of the obligations of the parties pursuant to this Agreement that by their nature would continue beyond the termination, cancellation or expiration of this Agreement shall survive termination, cancellation or expiration of this Agreement. This Agreement along with the related forms and disclosures constitutes the entire agreement to initiate on-line banking services between you and Mid Penn Bank.

Definitions
As used in this Agreement, the words "we", "our", "us", "Bank", and "MPB" mean Mid Penn Bank. "Customer", "you", and "your" refer to the accountholder authorized by the Bank to use the Internet Banking System under this Agreement and anyone else authorized by that accountholder to exercise control over the accountholder's funds through the System. "Account" or "accounts" means your accounts at Mid Penn Bank. "Electronic funds transfers" means ATM withdrawals, preauthorized transactions, point-of-sale transactions, transfers to and from your Bank accounts using the Internet Banking System, including bill payments. "System Services" means the services provided pursuant to this Agreement. "Business days" means Monday through Friday, excluding Bank observed holidays. "System" and "IBS" refers to Mid Penn Bank's Internet Banking System.

Registration
We require business customers to complete an enrollment form to add the business to the system, and to assign an authorized Primary Administrator of the IBS. The enrollment form will identify everything we

need to provide the service for you. (The exception to this is if Mid Penn Bank acquired a financial institution and converted your current online banking access to our system.)

Once the business accounts are added to the System by the Bank's On-Line Banking Department, the Primary Administrator you designate will have immediate access to the accounts for which you are an authorized signer, under the parameters of the System.

Access
To use the System, you must have at least one loan or deposit account at MPB, access to Internet service, and an e-mail address. Once you have completed the enrollment form and a member of the Bank's On-Line Banking Department has added the accounts to the System (or your access has been converted to our current online banking system as the result of a bank acquisition), you will have immediate access to the accounts for which you are an authorized Primary Administrator or an authorized user, under the parameters of the System and the designation indicated on the executed enrollment form(s) or the result of a converted online banking profile. To utilize the optional Bill Payment Service, you must have a checking account. We undertake no obligation to monitor transactions through the System to determine that they are made on behalf of the business account holder.

Assignment of an Online Banking Primary Administrator – An Authorized Representative of the company (or organization), as identified in the Corporate Resolution, should assign an online banking Primary Administrator. The Primary Administrator is recommended by the Bank to be an Authorized Representative of the company as listed in the Corporate Resolution. However, the Bank realizes that due to the nature and management of some businesses, it may be preferred to appoint a Primary Administrator who is not an authorized representative listed in the Corporate Resolution. Regardless of who is appointed as the Primary Administrator, the following will apply to the Company's named Primary Administrator. By granting an individual access to your accounts as a Primary Administrator, you expressly agree to take responsibility for all activity initiated by the Primary Administrator and those established users that are set up by the Primary Administrator. In effect, you have authorized each transaction initiated through the Service(s) to take place and the Bank will not be held liable for individual user actions.

By enrolling in online banking, you agree to be subject to a higher standard of care with respect to your accounts, transactions, and statements.

It is your responsibility to understand the capabilities built into each Service to prevent unauthorized transactions, and to decide which Account(s) and Service(s) to link to each User. When you designate a Primary Administrator, you should keep in mind the importance of separation of duties as a means of protecting yourself against losses or damages. You agree, based on the type, frequency, and amount of transactions that you will have with us, that the relevant security procedures provided are a commercially reasonable means of protection against unauthorized transactions and potential losses.

Primary Administrator's Access and Use of the Bank's Online Banking Services – With the acceptance of this Agreement, the Primary Administrator appointed shall have complete online access to all of Customer's Accounts and Services, as defined in the enrollment form, or as converted to the system as the result of a bank acquisition. This is necessary as the Primary Administrator cannot administer accounts or services to other online banking users without having the same or higher online banking access rights as other users being established

Customer shall be responsible for conveying and training the Primary Administrator in the proper use of the Bank's Online Banking Services and for supervising and auditing his or her use of the Bank's Online Banking Services.

There is no limit on the number of users a Primary Administrator can authorize. You assume sole responsibility for the actions of your Primary Administrator, the authority he or she gives others to act on your behalf, and the actions of the persons designated by the Primary Administrator to use the Service(s).

After issuance of the initial Primary Administrator credentials, it is the responsibility of the Primary Administrator to establish any additional company users and convey those credentials to the company users.

Establishment of Primary Administrator – The Bank will establish the credentials for the Primary Administrator based on written direction from an Authorized Representative of the company.

An Authorized User could be set up by the Primary Administrator to also have Administrator rights. The Primary Administrator, and any subsequently established Administrators set up by the Primary Administrator, are authorized by Customer to:

1. Designate individuals to access and use the Bank's Online Banking Services (each an "Authorized User") to receive information from the Bank concerning the operation and use of the Bank's Online Banking Services.

2. Give written instructions to the Bank or otherwise inform the Bank of any action or request for action by Customer with respect to the Bank's Online Banking Services, including but not limited to:

    a. The selection or deletion of any services provided to Customer by the Bank.
    b. The addition or removal of any Authorized Users.
    c. Establishing online limitations and access levels for each Authorized User. These limitations and access levels include which Accounts and which Services each Authorized User is authorized to access.
    d. Establishing any Second Level Approvals required for the completion of certain online banking transactions, as well as establishing Authorized Users with Approval Authority.
    e. The addition or removal of any Login Credentials.
    f. The addition or removal of any Authorized User's entitlements.
    g. The clearing or resetting of an Authorized User's password.
    h. The locking or deactivating of an Authorized User to prevent access or use of the Bank's Online Banking Services.
    i. The clearing of an Authorized User's session when the Authorized User becomes locked due to a browser malfunction or when an Authorized User incorrectly logs into the system beyond the allowed number of times.

The Primary Administrator is NOT authorized to add additional accounts or services to the Company's online banking access. Only an Authorized Representative (or Representatives) listed on the Corporate Resolution can assign new accounts and new services. Typically, these accounts and services can be assigned to the Primary Administrator unless otherwise specified by the Customer. Once assigned to the Primary Administrator, the Primary Administrator can then assign further online banking access to company users.

Customer agrees to notify the Bank of any change in the Primary Administrator. Such notice may be oral but must be confirmed in writing within three (3) business days of the oral notification

Upon receipt of notice of a change of the Primary Administrator, the Bank will disable access for the current Primary Administrator's access to Online Banking Services until written notice is received and approved naming a new Primary Administrator. A new Enrollment form will be required to establish a new Primary Administrator for the Company.

Customer agrees that it is solely the responsibility of the Customer to monitor and audit all activities performed by the Primary Administrator including, but not limited to verifying the appropriateness and accuracy of: all users given access to the Internet Banking System; the services, accounts, permissions, and entitlements provided to those users; and the transactions performed by, or the accounts accessible by, the Primary Administrator and all other users.

Customer understands and acknowledges that the Bank and its service providers have established certain security measures and procedures such as firewalls, codes and data encryption designed to prevent unauthorized access to Customer's accounts or transactions. Customer agrees to adhere to and comply with any security measures or protocols established by the Bank and/or its service providers.

Customer further understands and acknowledges that access to the Bank's Online Banking Services will not be free from delays, malfunctions or other inconveniences generally associated with using this electronic medium.

In the event the Bank's Online Banking Services are terminated for any reason, Customer shall immediately cease its use of the Bank's Online Banking Services.

Purge Rights – For security reasons, the Bank reserves it's right to purge, without prior notice, users, modules, or services that are deemed to be inactive by the Bank. Inactive is defined as having not been active/used for 12 months.

Your Password

You determine what password you will use. Through the System, all users have the ability to change their password at any time. You agree that we are authorized to act on instructions received under your password. You accept responsibility for the confidentiality and security of your password and agree to change your password regularly. The System will require you to change your password every 180 days. You will receive a warning of your password expiration 10 days before your password will need changed. Upon four unsuccessful attempts to use your password, your access to the System will be locked out. If you are locked out of your account, you will need to contact your Primary Administrator to request to have your log in unlocked or contact Mid Penn Bank's Customer Support during business hours to have your password reset. You will be required to change your temporary password once you log in.

You will be required to create a password that utilizes both upper and lower case alpha and numeric characters for purposes of security. 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. If it is necessary to write down your password, it should not be stored near your computer. Your password should not be a word found in the English dictionary. The minimum password requirements for the system are the use of one upper case letter, one lower case letter, one number and at least 8 characters, but not longer than 75 characters in length. For your security, you will be required to change your password every 180 days.

You agree that the Bank may change or enhance the process by which you and all other users gain access to the System, as such changes occur from time to time as the Bank attempts to maintain the highest level of security so as to protect your accounts, funds, and information from unauthorized access.

You agree that you will be solely responsible for liability, loss, or damage, if any, resulting from the Bank's actions, either directly or indirectly, that were made in accordance with requests or instructions received by us via the Website when access to your account is gained via said Website by use, authorized or otherwise, of your password or any subsequent password established by you. You agree to indemnify and hold harmless Mid Penn Bank from any and all such liability, loss or damage.

Internet Banking System Services

Upon granting your request for access to the System, you authorize MPB to honor and act upon all requests and instructions that we receive via the System with regard to your designated account(s). You assume full and sole responsibility for all requests and instructions made via the System with regard to your designated account(s). The individual terms and conditions of your account(s) will continue to apply in all respects.

We agree to use our best efforts to act upon all instructions received via the System with regard to your account(s) on the banking day of receipt, when such instructions are received prior to deadlines set by Bank, and to use any means and routes that the Bank, in its sole discretion, may consider suitable for the transmission of fund transfer requests. We may, at our discretion but not obligation, verify instructions by inquiry to you at the telephone number(s) specified by you in your account records with us. You agree to assign no responsibility to us beyond the duty to exercise ordinary care when the Bank follows the instructions received via the System.

You agree to release MPB for responsibility or liability for any inaccuracy, interruption, delay or failure in transmission, and to indemnify and hold harmless against claims based thereon, when the same are occasioned by any circumstance beyond our reasonable control, including but not limited to circumstances associated with the following: System availability, weather, power failure, communication line failures, and errors or the lack of responsiveness of other organizations or entities. We do not and cannot warrant that the System will operate without errors, or that any or all of the System will be available and operational at all times.

System Services

You can use the System to check the balance of your Bank accounts, view Bank account histories, transfer funds between your Bank accounts, make stop payment requests, download account information to import into financial management software and pay bills from your Bank accounts in the amounts and on the dates you request, provided you have requested the optional Bill Payment Service. Additional services and enhancements to existing services may be added from time to time by MPB without notice. Not all services offered on the site may be available to you. The Bank reserves the right to determine your eligibility for any product or service.

If you use the on-line Stop Payment service, you agree to the following terms and conditions: The stop payment order is effective for 184 days unless renewed before the end of the 184 days in writing or through Mid Penn Bank's On-Line Banking System. Each renewal is effective for 184 days. The information on the stop payment order must be correct, including the account, check number, amount, date written, written to (payee) and reason (selecting the best reason from a drop-down option). You understand that there may be claims or demands made against us as a result of your request to us. You agree that you will be responsible to us if any claim or demand is made against us as a result of us having acted as you requested. You agree to reimburse us for any costs, expenses or attorney's fees that we have incurred in defending ourselves against any such claims or demands.

Limits on Amounts and Frequency of On-Line Transactions
The number of transfers from MPB accounts and the amounts that may be transferred are limited pursuant to the terms of the applicable deposit agreement and disclosure for those accounts. If a hold has been placed on deposits made to an account from which you wish to transfer funds, you cannot transfer the portion of the funds held until the hold expires. Limits also apply to mobile deposit amounts that you are able to submit per day.

Fees and Charges
You agree to pay the fees and charges for your use of System Services, if any, as set forth in the Business On-Line Banking Fee Schedule, which is contained as part of this Agreement. You agree that all such fees and charges will be deducted from the Bank checking account designated by you as your "Primary Checking Account." If you close your Primary Checking Account, you must immediately designate another account as your Primary Checking Account. You agree to pay any additional reasonable charges for services you request, which are not covered by this Agreement. You are also responsible for telephone and Internet service fees you incur in connection with your use of the System.

Hours of Access
You can use the System seven days a week, twenty-four hours a day, although some or all System services may not be available occasionally due to emergency or scheduled system maintenance. We agree to post, if possible, notice of any extended periods of non-availability on the System website.

Equipment
Your use of the System requires a compatible personal computer (with sufficient power and memory), a modem or other Internet access device, an Internet Service Provider (ISP) and a capable browser. You recognize that the computer system which stores your account information is the property of a third party and you agree to comply with such procedures and requirements as may be established from time to time by the owner of the System or by the Bank. You agree not to disclose any proprietary information regarding the System to any third party and to comply with such security measures and recognition procedures as may be established from time to time by the Bank or by the System owner.

Security
It is your responsibility to utilize a browser that supports the required minimum encryption level so that you can access Mid Penn Bank's On-Line Banking System. Your use of any browser may be subject to the license agreements of the browser manufacturer, in addition to the terms and conditions of this Agreement. We are not responsible for notifying you of any upgrades, fixes or enhancements to, or for providing technical or other support for any browser or for any compromise or loss of data transmitted across computer networks or telecommunications facilities, including, but not limited to, the Internet.

You acknowledge and agree that you are responsible for obtaining Internet access through an Internet service provider of your choice and that you may be subject to fees imposed by such Internet service provider and for any associated communications service provider charges. You acknowledge and agree that there are certain security, corruption, transmission error and access availability risks associated with using open networks such as the Internet and you hereby expressly assume such risks (to the extent the

law allows you to do so). You acknowledge that you have requested Mid Penn Bank 's On-Line Banking service, have made your own independent assessment of the adequacy of the Internet as a delivery mechanism for accessing information and initiating transactions and other instructions and that you have determined to proceed with use of Mid Penn Bank's On-Line Banking service based on your independent assessment.

The System utilizes a comprehensive security strategy to protect accounts and transactions conducted over the Internet. Please refer to Mid Penn Bank's On-Line Security Policy for more details.

You understand the importance of your role in preventing misuse of your accounts through the System and you agree to promptly examine your account statement(s) as soon as you receive it (them). You agree to protect the confidentiality of your account(s) and account number(s), and your personal identification information, such as your driver's license number and social security number. You understand that personal identification information by itself, or together with information related to your account(s), may allow unauthorized access to your account(s). Your Client ID, User ID and password/PIN are intended to provide security against unauthorized entry and access to your account(s). Data transferred via the System is encrypted (scrambled) in an effort to provide transmission security and System utilizes identification technology to verify that the sender and receiver of System transmissions can be appropriately identified by each other. Notwithstanding our efforts to ensure that the System is secure, you acknowledge that the Internet is inherently insecure and that all data transfers, including electronic mail, occur openly on the Internet and potentially can be monitored and read by others. We cannot and do not warrant that all data transfers utilizing this System, or e-mail transmitted to and from us, will not be monitored or read by others. Customers should NOT send account information or items of a confidential nature via unsecure e-mail. When sending information of a confidential nature, Mid Penn Bank does provide access to a secure e-mail link from our website. Please be sure that if you are including confidential information in an e-mail to us, that you are using the secure e-mail/contact us link.

You agree that you will promptly notify us of any security compromise, or potential security compromise, of your initial password/PIN or any subsequent password/PIN established by you.

MPB cannot, and does not, guarantee that downloads from the System will not contain a virus or other destructive device.

Third Party Software; Virus Protection
The Bank makes no representations or warranties regarding the accuracy, functionality, or performance of any third-party software that may be used in connection with the System (e.g. Quicken®, QuickBooks®). The Bank is not responsible for any electronic virus or viruses that you may encounter. We encourage you to routinely scan your computer, disks, and software using a reliable virus detection product to detect and remove any viruses found. Undetected or unrepaired viruses may alter, corrupt, damage, or destroy your programs, files, and even your computer. Additionally, you may unintentionally transmit the virus to other computers, disks and software.

Posting of Transfers
Transfers initiated through System before 6:30 PM (Eastern Standard Time) on a business day are posted to your account the same day. Transfers completed after 6:30 PM. (Eastern Standard Time) on a business day may not be posted until the next business day. Transfer requests on Saturday, Sunday or a banking holiday will be posted on the next business day. Transfers are posted to your account(s) according to the rules and regulations of the account(s) and the Bank's Funds Availability Policy. Electronic Fund Transfers generally have immediate availability. The System identifies transfers based upon the User ID of the user who made the electronic transfer.

Change in Terms
We may change any term to this Agreement at any time. If the change would result in increased fees for any System service, increased liability for you, fewer types of available electronic fund transfers, or stricter limitations on the frequency or dollar amount of transfers, we agree to give you notice at least 30 calendar days before the effective date of any such change, unless an immediate change is necessary to maintain the security of the account or our electronic fund transfer system. We will post any required notice of the change in terms on the System's Website or forward it to you by e-mail or postal mail. If advance notice of the change is not required, and disclosure does not jeopardize the security of the account or our electronic fund transfer system, we will notify you of the change in terms within 30 calendar days after the change becomes effective. Your continued use of any or all the System services indicates your acceptance of the change in terms. We reserve the right to waive, reduce or reverse

charges or fees in individual situations. You acknowledge and agree that changes to fees applicable to specific accounts are governed by the applicable deposit agreements and disclosures and agree to accept notification of any and all changes to these accounts by e-mail.

Disclaimer of Warranty and Limitation of Liability
We make no warranty of any kind, express or implied, including any implied warranty of merchantability or fitness for a particular purpose, in connection with the System services provided to you under this Agreement. We do not and cannot warrant that the System will operate without errors, or that any or all System services will be available and operational at all times. Except as specifically provided in this Agreement, or otherwise required by law, you agree that our officers, directors, employees, agents or contractors are not liable for any indirect, incidental, special or consequential damages under or by reason of any services or products provided under this Agreement or by reason of your use of or access to System, including loss of profits, revenue, data or use by you or any third party, whether in an action in contract or tort or based on a warranty. Further, in no event shall the liability of the Bank or its affiliates exceed the amounts paid by you for the services provided to you through the System.

Third Party Network Disclaimer
You may not resell or redistribute any services you receive through the System, or our other services, or from our suppliers. You acknowledge and agree that neither MPB nor its suppliers are responsible for the content of your transmissions, which may pass through any Internet Service Provider or over the Internet. You agree to take reasonable steps to ensure that you will NOT use the services provided to you or the Internet for illegal purposes, for transmission of threatening, obscene, or harassing materials, or to interfere with or disrupt other users, services or equipment. Disruptions include, but are not limited to, distributing chain letters or mass mailings of unsolicited e-mail ("spamming"), propagating computer worms and viruses, or using the services and the Internet to make unauthorized entry to any other machine. Violation of the foregoing may result in termination of access rights to the offending party or parties. We do not warrant that our services, the Internet or our suppliers will be available on a specified date or time or that our services and the Internet will have the capacity to meet your demand during specific hours. Neither MPB nor its suppliers will be liable for any damage that you may suffer arising out of use, or inability to use, the services or products provided hereunder. Neither MPB nor its suppliers will be liable for unauthorized access to MPB's transmission facilities or premise equipment or for unauthorized access to or alteration, theft or destruction of your data files, programs, procedures or information through accident, fraudulent means or devices, or any other method, regardless of whether such damage occurs as a result of MPB or its supplier's negligence.

In no event will MPB or its suppliers be liable for any other damages, including but not limited to loss of data, loss of revenue or profits, or for any other special, incidental, indirect or consequential damages, arising out of or in connection with the use of the services or the Internet. Access to the services and the Internet cannot be guaranteed. You may be unable to access any Internet Service Provider or the Internet at any given time, and disconnections may occur from time to time. For security reasons, during your MPB On-Line session, you will be automatically timed-out upon being logged in for twenty minutes (20) minutes with no activity (no clicks). You will be able to sign-on again, if desired.

Your Right to Terminate
You may cancel your System service at any time by providing us with written notice by secure e-mail, postal mail or fax. Please include all User ID's assigned to your business in your correspondence. Your access to the System will be suspended within 2 business days of our receipt of your instructions to cancel the service. You will remain responsible for all outstanding fees and charges incurred prior to the date of cancellation.

Our Right to Terminate
You agree that we can terminate or limit your access to System services for any of the following reasons:

1. You or any authorized user of the System breaches this or any other agreement with us.
2. We have reason to believe that there has been unauthorized use of your accounts on the System, or your User ID or Password/PIN.
3. Without prior notice, if you have insufficient funds in any one of your Bank accounts. System service may be reinstated, in our sole discretion, once sufficient funds are available to cover any fees, pending transfers and debits.

4. If you do not sign on or have any transactions scheduled through the Service within a one-year period. After one year of non-use, we may convert your Service to an

inactive status or terminate your Service. **If your account is deemed inactive and/or MPB terminates your access to the Service, your on-line bill payment information will be lost. Please refer to the CheckFree® Terms and Conditions for further Information about termination of the Bill Payer Service.**

5. Upon reasonable notice, for any other reason at our sole discretion, we can cancel your online banking service. We will notify you or any other party to your account that we have cancelled or will cancel this Agreement. Termination of this Agreement will not affect the rights and responsibilities of the parties under this Agreement for transactions initiated before termination.

OPTIONAL BILL PAYMENT SERVICES
(BUSINESS ACCOUNTS)

On-Line Bill Payment Services are provided to you for your convenience, at your request. The actual payment of such bills is handled by an independent third party and the Bank cannot and will not guarantee or be held responsible for the completion and accuracy of such transactions. You must agree to the Terms and Conditions of the Bill Payment Service prior to being granted access to the Bill Pay function on the website.

Mid Penn Bank's On-Line Bill Payer Service (MPB Small Biz Easy Pay) is offered through CheckFree® and allows you to schedule bill payments through the Internet. Please access MPB Small Biz Easy Pay bill pay service through the "Funds Management" button within the Internet Banking System.

In addition to the Terms and Conditions of the Bill Payment Service, the following also apply to your use of MPB Small Biz Easy Pay bill pay service.

- MPB may terminate your use of MPB Small Biz Easy Pay bill pay service at any time without prior written notice, for any reason, such as inactivity.
- MPB Small Biz Easy Pay bill pay service will be terminated automatically if your Account(s) are closed.

MID PENN BANK
BUSINESS MOBILE BANKING SERVICES
TERMS & CONDITIONS

Mid Penn Bank ("Bank") offers its business, government, association and organizational customers and authorized employees or agents an ability to access information about their accounts, or to perform certain types of account transactions and authorizations via mobile devices. The Bank makes this service available through special apps, for Apple, Samsung and Android-based smartphones. These apps may be downloaded from the app repository unique to each type of smartphone. The apps allow customers to retrieve account balances and perform certain types of transactions.

The use of the term "customer" throughout this document is defined as any owner, agent, or employee of a business or organization that has been granted online access to view defined accounts, or to perform defined transactions, as stipulated by an authorized individual on behalf of the business or organization.

By accessing and utilizing any of these services, customers agree that;

1. The mobile banking services made available by the Bank are extensions of the Bank's On Line Banking service. Customers accessing and utilizing these services are subject to the Bank's Online Access Agreement, as it exists at the time of the customer's use of any mobile banking service.
2. The downloading and use of the Bank's Business Mobile app is an extension of the customer's previously defined permissions within the Bank's online banking service, and the use of the mobile app does not convey or permit any additional authority or capability.
3. To the extent a mobile banking service offers services, capabilities, features, or procedures not expressly provided in the governing On Line Banking service agreement, this Business Mobile Banking Service Terms & Conditions document provides further guidance, rules, procedures, covenants, obligations, and warranties to which a customer agrees to be bound as a result of using any of the Bank's Business Mobile Banking Services.
4. The accounts accessed by the Bank's Business Mobile Banking Services continue to be governed by the relevant account agreements: contracts and disclosures provided to the account owners. Nothing in these Business Mobile Banking Terms & Conditions may be construed to supersede or supplant those account agreements and disclosures.

By participating in Business Mobile Banking, you are agreeing to the terms and conditions presented here.

Our participating carriers include (but are not limited to) AT&T, SprintPCS, T-Mobile®, U.S. Cellular®, Verizon Wireless (subject to change).

Mobile Banking and any software you may obtain from Mobile Banking ("Software") may not be available at any time for any reason outside of the reasonable control of Mid Penn Bank or any service provider.

Privacy and User Information. You acknowledge that in connection with your use of Business Mobile Banking, Mid Penn Bank and its affiliates and service providers, including Fiserv, Inc. and its affiliates, may receive 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"). Mid Penn 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. Mid Penn 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.

Restrictions on Use. You agree not to use Mobile Banking or the Software in or for any illegal, fraudulent, unauthorized or improper manner or purpose and 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 Mid Penn 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 Mid Penn 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 Mid Penn 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 (Mid Penn Bank's mobile banking provider) 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 the Software; or (d) otherwise abuse Mobile Banking or the Software.

MOBILE DEPOSIT

This section defines the terms and conditions specific to the Bank's Business Mobile Deposit Service, offered through the Bank's downloaded app supporting business mobile banking. Customers acknowledge they are not granted immediate access to the Business Mobile Deposit Service and must instead request mobile deposit on a Primary Administrator enrollment form or be granted mobile deposit access by the Company's established Primary Administrator.

Once a customer is granted access to the Business Mobile Deposit Service, and by using that service, you agree to be legally bound by these terms and conditions. You also agree that these terms and conditions may change from time to time, and the terms and conditions in place at the time of your transaction will be the rules against which your transaction is processed. Customers acknowledge that the Bank may change, terminate, add or remove features from its Business Mobile Banking Service. Customers will be informed, upon signing into their Business Mobile Banking App, that a new definition of terms and conditions has been applied. Customers acknowledge that they shall be bound by the new terms and conditions, whether the customer chooses to read, or not to read, those new terms and conditions. Customers may reject the Bank's new terms and conditions by immediately discontinuing use of the Business Mobile Banking service.

The Bank's Mobile Deposit Service (also referred herein as "MDS") is a service by which a mobile banking customer can upload a legal image of a check for deposit to the customer's qualified Bank account. To use MDS, a customer must provide, at their expense, a supported mobile device, such as a smartphone, tablet, etc. The device must also contain a supported camera and operate on an operating system compatible with the Bank's systems. The device must be capable of communicating with and through the Internet, either by establishing a Wi-Fi connection or by using a cellphone-based communications channel. The cost of maintaining and using such Internet-based communications (typically known as a "Data Plan") is at the customer's expense. The customer further agrees that the responsibility for obtaining, operating, updating and securing their mobile device is entirely the customer's responsibility. The customer also acknowledges that the Bank cannot guarantee that the customer's particular device or operating system will be compatible with the Bank's MDS.

Customers may scan and transmit checks for deposit to their qualified account the Bank. Checks transmitted through this MDS must comply with how that term ("check" or "item") is defined by the Federal Reserve Regulation CC and Regulation J, the Check 21 Act, and Article 4 of the Uniform Commercial Code. Customers agree that the Bank, using its sole discretion, determines whether a

scanned/transmitted item is an acceptable item for deposit with respect to how the Bank interprets these regulations and codes.

Customers also agree not to scan and transmit the following types of items or checks:

1. Checks or items already previously converted to a substitute check, as defined by Reg CC.
2. Checks or items already previously deposited to an account at Mid Penn Bank or any other type of financial institution.
3. Checks or items that have already been negotiated.
4. Checks or items made payable to any person or entity other than the customer submitting the item for deposit.
5. Checks or items made payable to the customer AND another party not named as an account owner of the account into which the item is being deposited.
6. Checks or items that have any type of alteration of any information on the check, including information contained within the MICR line.
7. Checks or items which a customer knows or suspects, or should know or suspect, of being fraudulent or unauthorized.
8. Checks or items drawn against a financial institution outside the United States.
9. Checks or items that have already been returned as unpaid.
10. Any check image taken from a computer screen or device.
11. Cash.
12. Traveler's Checks.
13. Money Orders.
14. Savings Bonds.
15. Checks or items not payable in U.S. currency.
16. Checks or items for which stop payment orders have been issued.
17. Checks or items for which the issuer does not have sufficient funds to cover that check or item.
18. Checks or items with an issue date older than 6 months from the date of deposit.
19. Checks or items that are contrary to the Deposit Agreement governing the account into which the deposit is being attempted.
20. Checks that are created without the signature of the maker, often referred to as remotely created checks (RCC).

Customers agree that the Bank is not required to accept any check or item for deposit through its MDS. If, in its sole discretion, Bank decides not to accept a particular check or deposit, the customer agrees to not attempt to deposit that item again through the MDS, and to bring that check or item to a branch office of the Bank for assistance in reviewing its collectability.

Checks or items scanned and transmitted using the Bank's MDS must have an image quality that is clear, legible, and in compliance with the standards of the American National Standards Institute and any other regulatory entity or operational processor involved in the handling of such checks or items. Customers agree that Bank shall not be liable for any damages resulting from image quality, or a perception of poor image quality, or from any inaccurate information you may supply pertaining to a check or item.

Prior to scanning and transmitting a check or item through the Bank's MDS, customers must restrictively endorse that check or item as "**For Mobile Deposit Only at Mid Penn Bank**." Customers acknowledge that failure to endorse a check or item in this manner will result in the Bank rejecting that check or item.

Customers acknowledge that, although a check or item may have been successfully scanned and delivered to the Bank using its MDS, the Bank has the right to reject that deposit for any reason, including those outlined within these terms and conditions. Customers further acknowledge that checks and items will be accepted for deposit subject to all of the limitations and terms set forth in the deposit agreement governing the account into which the deposit is being directed.

Accepted deposits made using the Bank's MDS will not be available for immediate withdrawal. The Bank will generally apply its published "Funds Availability Schedule" to deposits made through the MDS, with exceptions for certain situations. This usually means that funds from ACCEPTED checks or items are made available to customers on the first business day following the business day a check or item was considered deposited. A "business day" refers to any non-weekend or non-Federal-Holiday on which the Bank is open and accepting customer transactions. Furthermore, deposits made through the MDS must be received and accepted by the Bank no later than 4 PM (Eastern Standard Time) of a Business Day. For instance, a deposit made on a Saturday, Sunday, or on a Federal

Holiday, will not be considered as deposited until the first business day on which the Bank is open. In another example, an ACCEPTED deposit made at 4:01 PM (Eastern Standard Time) or later may not be processed until the next Business Day on which the Bank is open.

The Bank may, at its sole discretion, delay availability on checks or items deposited through the MDS, for reasons such as:

1. The check or item is being deposited into a new account at Mid Penn Bank, or;
2. The account owner has a history of improper account management, or;
3. The Bank has reason to doubt the collectability of any particular check or item.

The Bank will provide written notice to the customer when the availability of funds for a particular check or item are delayed, by sending the notice to the address on file for the account into which the check or item was deposited.

Customers acknowledge that, for security reasons, the Bank will impose limits on the amount(s) of checks or items a customer may deposit using the Mobile Deposit Service. In most circumstances, customers will be limited to a maximum of $7,501 in deposits per business day, although the Bank may, without notice and in its sole discretion, change that limit for any customer for any reason. Customers agree that the Bank has no responsibility to accept any deposit through the MDS, and that the Bank has no liability for any of the consequences resulting from deposit limits that it imposes on customer activity.

Upon making a deposit using MDS, and upon that deposit's status reflecting "ACCEPTED," customers agree to write "DEPOSITED" across the face of the check or item so as to prevent accidental re-deposit. Customers also agree to safely store that check or item for a period of 30 days. During this time, customers agree to provide the original check or item, or additional information about that check or item, to the Bank, upon the Bank's request. Following the 30-day retention period, customers agree to securely destroy the check in a manner making it impossible to recover, reconstruct, or obtain information from. This is typically done by methods such as shredding or incineration.

When using the Mobile Banking Service, and/or the MDS, customers may encounter technical problems or other factors preventing the successful access to information or transaction execution. Customers acknowledge that Bank has no responsibility for any consequence of a customer's inability to successfully use the Mobile Banking Service, including the MDS.

Customers acknowledge that the Bank applies certain criteria in determining who may have access to its Mobile Banking Services, and for security reasons, may choose to deny, withhold, change, suspend or terminate access to some or all of the services available through the Bank's Business Mobile Banking App. Customers also acknowledge that a customer may terminate their use of the Business Mobile Banking App, or the MDS, at any time and for any reason. Such termination may be affected by, 1) cease using the Business Mobile Banking App immediately, and 2) calling Mid Penn Bank at 1-866-642-7736 to inform us of your desire to remove the service from your account(s). Customers further acknowledge that transactions they performed prior to terminating their use of the service will still be bound by the terms and conditions in effect at the time of the transaction, regardless whether that transaction was completed, rejected, or is still in the process of completion or rejection.

ELECTRONIC FUND TRANSFERS
YOUR RIGHTS AND RESPONSIBILITIES
(CONSUMER ACCOUNTS ONLY)

Indicated below are types of Electronic Fund Transfers (EFT) we are capable of handling, some of which may not apply to your account. Please read this disclosure carefully because it tells you your rights and obligations for the transactions listed. You should keep this notice for future reference.

Electronic Fund Transfers Initiated by Third Parties. You may authorize a third party to initiate electronic funds transfers between your account and the third party's account. These transfers to make or receive payment may be one-time occurrences or may recur as directed by you. These transfers may use the Automated Clearinghouse (ACH) or other payments network. Your authorization to the third party to make these transfers can occur in a number of ways. For example, your authorization to convert a check to an electronic fund transfer or to electronically pay a returned check charge can occur when a merchant provides you with notice and you go forward with the transaction (typically, at the point of purchase, a merchant will post a sign and print the notice on a receipt). In all cases, these third-party transfers will require you to provide the third party with your account number and bank information. This information can be found on your check as well as on a deposit or withdrawal slip. Thus, you should only provide your bank and account information (whether over the phone, the Internet, or via some other method) to trusted third parties whom you have authorized to initiate these electronic fund transfers. Examples of these transfers include, but are not limited to:

- **Preauthorized Credits.** You may make arrangements for certain direct deposits (such as Social Security, Armed Services Retirement, Railroad Retirement, or Veterans Administration Payments) to be accepted into your checking or savings account(s). If you have arranged to have direct deposits made to your account at least once every 60 calendar days from the same person or company, you can call us at 1-866-642-7736 to find out whether or not the deposit has been made.
- **Preauthorized Payments.** You may make arrangements to pay certain recurring bills from your checking account(s).
- **Electronic Check Conversion.** You may authorize a merchant or other payee to make a one-time electronic payment from your checking account using information from your check to pay for purchases or pay bills.
- **Electronic Returned Check Charge.** You may authorize a merchant or other payee to make a one-time electronic funds transfer to collect a charge in the event a check is returned for insufficient funds.

On-Line Electronic Fund Transfers. Once your on-line service is established, you can access your account information on-line to:

(1) Transfer funds between your MPB accounts, including checking, savings, money market and/or loan accounts.
(2) Get information about the account balance of your MPB checking, savings, money market and/or loan accounts.

Transfer Limits. There are no limits to the number of on-line transfers or the amounts that may be transferred except for those imposed by Federal regulations, which limit the number of electronic transfers for savings and money market accounts. Transfers from a savings account or money market account to another account or to third parties by preauthorized, automatic, telephone, or computer transfer or by check, draft, or similar order to third parties are limited to six (6) per month.

If a hold has been placed on deposits made to an account from which you wish to transfer funds, you cannot transfer the portion of the funds held until the hold expires.

FEES
We do not charge for on-line electronic internal fund transfers, except for bill payment services listed on our Fee Schedule.

DOCUMENTATION

Periodic Statements
You will get a monthly account statement from us for your checking accounts. You will get a monthly account statement from us for your statement savings account, starter savings or simple savings account,

unless there are no transfers in a particular month. In any case, you will get a statement at least quarterly. Your statements may be delivered to you as a paper statement or an electronic statement.

PREAUTHORIZED PAYMENTS

Right To Stop Payment And Procedure For Doing So
If you have told us in advance to make regular payments out of your account, you can stop any of these payments. Here is how: Call or write us at the telephone number or address listed in this agreement in time for us to receive your request 3 business days or more before the payment is scheduled to be made. If you call, we may also require you to put your request in writing and get it to us within 14 calendar days after you call. If your written request is not received within this time frame, the stop payment will be nullified.

Notice Of Varying Amounts. If these regular payments may vary in amount, the person you are going to pay will tell you 10 calendar days before each payment, when it will be made and how much it will be. (You may choose instead to get this notice only when the payment would differ by more than a certain amount from the previous payment, or when the amount would fall outside certain limits that you set.)

Please refer to our separate fee schedule for the amount we will charge you for each stop payment order you give. We reserve the right to change our fee schedule and to charge your account in accordance with the current fee schedule in effect at the time of your stop payment request.

FINANCIAL INSTITUTION'S LIABILITY

Financial Institution's Liability For Failure To Stop Payment Of Preauthorized Transfer
If you order us to stop one of these payments 3 business days or more before the transfer is scheduled, and we do not do so, we will be liable for your losses or damages.

Financial Institution's Liability For Failure To Make Transfers
If we do not complete a transfer to or from your account on time or in the correct amount according to our agreement with you when you have properly instructed us to do so, we will be liable for your losses or damages caused as a result. 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 money in your account is subject to legal process or other claim restricting such transfer.
3. If you have an overdraft line and the transfer would go over the credit limit.
4. If circumstances beyond our control (such as fire or flood) prevent the transfer, despite reasonable precautions that we have taken.
5. If any electronic terminal, telecommunication device, or any part of the IBS electronic funds transfer system is not working properly and you knew about the problem when you started the transfer.
6. If you have not properly followed the on-screen instructions for using IBS.
7. If you pay a bill too late to arrive at the Payee's place of business on a timely basis.

Other exceptions established by us:

1. If we have terminated our Agreement with you.
2. If the funds in your account are not available.
3. If your account is closed, or if it has been frozen.
4. If we have reason to believe that the transaction requested is unauthorized.
5. If your password/PIN has been reported lost or stolen and you are using the reported password/PIN or we have reason to believe that something is wrong with the transaction.
6. In the case of preauthorized transfers, we will not be liable where there is a breakdown of the system that would normally handle the transfer.
7. If you, or anyone authorized by you, commits any fraud or violates any law or regulation.
8. There may be other exceptions stated in this Agreement and in other agreements with you.

BUSINESS LIABILITY
You agree to contact us immediately if money is missing from your account or if your User ID or On-Line Banking PIN has been lost or stolen, or if you believe they may be used without your authorization. Telephoning immediately is the best way to minimize your losses. You agree to cooperate with us in the

investigation of any claim or dispute and provide us with the necessary information to assist us in resolving your claim or dispute.

CONFIDENTIALITY

It is our general policy to treat your account information as confidential. However, we will disclose information to third parties about your account or the transactions you make ONLY in the following situations:

1. Where it is necessary for completing transfers; or
2. In order to verify the existence and condition of your account for a third party, such as a credit bureau or merchant; or
3. In order to comply with government agency or court orders; or
4. If you give us your written permission; or
5. As explained in our separate Privacy Policy.

UNAUTHORIZED TRANSFERS

Contact In Event Of Unauthorized Transactions, Questions or Problems.

If you believe your password/PIN has been lost, stolen or that someone has transferred or may transfer money from your account without your permission telephone us immediately at:

1-866-642-7736
While telephoning us is the fastest way to inform us,
you also have the option to write us at:
Mid Penn Bank Operations Center
Attn: Deposit Services
894 N River Road
Halifax PA 17032

Communication Between Mid Penn Bank and You

If you have questions regarding electronic fund transfers, documentation, stop payments or error resolution, you may contact us at the telephone number or address listed below. If you believe your password/PIN has been lost, stolen or compromised in any way or that someone has transferred or may transfer money from your account without your permission, you can communicate with us using the contact information below:

OUR CONTACT INFORMATION:

Mid Penn Bank Operations Center
Attn: Deposit Services
894 N River Road
Halifax PA 17032
Phone: 1-866-642-7736

Business Days: Monday through Friday, Excluding Bank Observed Holidays

MID PENN BANK
Making things happen for you.℠

MEMBER FDIC

MID PENN BANK
BUSINESS ON-LINE BANKING
FEE SCHEDULE

Our Business fees for On-Line Banking services are as follows:

View and Transfer: Free. (Includes checking your account balances, viewing account histories, transferring funds between your accounts, ordering checks, exporting history to personal finance software such as Quicken®, QuickBooks® or MS Money® or changing your address.)

Bill Payment Service: Users can self-enroll in on-line bill pay provided you have at least one checking account which you are an owner. To self-enroll, click on the "Payments" tab within the System and follow the prompts to self-enroll in MPB Easy Pay bill pay. The cost for Mid Penn Bank's bill pay service is $5.75 per month for the first 15 bills, and $.50 each additional bill. Other bill payment fees may be applicable. Please refer to the bill pay vendor's Terms and Conditions regarding other fee information. (Bill pay fees may vary based on previous bill pay fees related to accounts acquired as part of a bank conversion, provided such fees are less than Mid Penn Bank's current bill pay fee scheduled.

Stop Payment Fee: Now you can complete a stop payment request, for a check issued against your account on-line. There is substantial risk to the bank in honoring your stop payment request, for which the fee is $30.00 per stop payment item.

Other Service Fees: Other service fees may be applicable, including wire transfer and ACH file transfer fees, which require additional agreements.

(Fee schedule subject to change without prior notice.)

MID PENN BANK
ONLINE PRIVACY PRACTICES

Mid Penn Bank is committed to providing the highest level of security and privacy regarding the collection and use of our customers' personal information. Our goal is to protect your confidential information when we interact with you at one of our offices, at ATM's and ITM's, on the phone and on our website.

Respecting Our Customer's Privacy: Mid Penn Bank respects your right to privacy and we will take every precaution to protect your privacy. Having the most accurate and updated information is the foundation of Mid Penn Bank's ability to provide the best possible customer service to you. Keeping your information secure and using it only to better service you is Mid Penn Bank's top priority. If you decide to close your account(s) or become an inactive customer, we will adhere to Mid Penn Bank's Privacy Policy as well as the practices as described in this online privacy practices notice.

Collection, Use and Retention of Personal Information: The collection of personal information is designed to provide access to your personal accounts and to assist the bank in providing you with the products and services you want and need. Personal information collected and stored by the bank is used for specific business purposes, to protect and administer your personal accounts and transactions, to comply with state and federal banking regulations, and to help the bank better understand your financial needs in order to design or improve our products and services.

Protection of Information: We will safeguard the information you share with us according to strict bank standards of security and confidentiality. The bank maintains physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information. We will limit the collection and use of customer information to the minimum that we require to deliver excellent customer service to customers, which includes recommending or advising customers about any products, services or other opportunities which may better service their current or anticipated needs.

Visiting Our Web Site: Visitors to Mid Penn Bank's website remain anonymous. We do not collect identifying information about visitors to our site. We may use standard software to collect non-identifying information about our visitors, such as:

- Date and time our site was accessed
- IP address (a numeric address given to servers connected to the Internet)
- Web browser used
- City, State and Country

The bank uses this information to create summary statistics and to determine the level of interest in information available on our site.

Visitors may elect to provide us with personal information via a secure contact us form available from our website. This information is used internally, as appropriate, to handle the sender's request. It is not disseminated or sold to other organizations.

Some areas of our web site may use a "cookie", which is a small file that is temporarily stored in the visitor's computer memory (RAM) on the hard drive to allow the web server to log the pages you use within the site and to determine if you have visited our site before. If you are uncomfortable with the use of cookie technology, you can set your browser to refuse cookies or to alert you when and by whom cookies are being written to your hard drive. The Bank may also use combinations of other technologies, as they are developed, to track a user's web server activity.

Links to Other Sites: Mid Penn Bank's website may contain links to third-party sites that you may find useful. These sites may have their own privacy policies. You should review the privacy policy of any website before you provide personal or confidential information.

Privacy of Children: Mid Penn Bank respects the privacy of children. Mid Penn Bank does not knowingly market to children.

Information Accuracy and Security Practices: Mid Penn Bank will attempt to keep customer information complete, up to date and accurate. We will tell our customers how and where to access their account information (except when prohibited by law) and how to notify us about errors, which will promptly be corrected.

Information specific to any of your account relationships or financial services can be updated or changed at your request. Questions regarding corrections of this nature should be directed to Mid Penn Bank, 894 N. River Road, Halifax, PA, 17032 or by calling us at 1-866-642-7736.

We will continually assess ourselves to ensure that customer privacy is respected. We will conduct business in a manner that fulfills our promise to the customers whom we serve.

You can also help safeguard your personal information by taking a few simple precautions. Protect your account number, PIN and customer access numbers. Never disclose confidential information to unknown callers. When banking On-Line, be sure to use a secure browser and current virus detection software, and never open e-mails from unknown sources.

We want to ensure that you are aware of Mid Penn Bank's online privacy practices.

ONLINE BUSINESS BANKING
FREQUENTLY ASKED QUESTIONS

Q Is my Business Banking User ID case sensitive?
A. Yes, your Business Banking User ID (Log In ID) is case sensitive and is a minimum of 5 characters long for personal users. Consumer users (and some sole proprietorship users) should log in using the Personal Online Banking from Mid Penn Bank's website.

Q. Is my User ID the same as my password?
A. No. Your User ID is the unique identifier you would have selected when you enrolled in Online Banking. Your User ID will never change unless you ask us to change it. Your password is case sensitive and must contain upper and lower case letters as well as numbers and special characters. Your password is subject to change every 180 days.

Q. Is my password case sensitive?
A. Yes, your password is case sensitive. Your password must be a minimum number of characters and must include at least 1 Upper Case letter, 1 lower case letter, 1 number and 1 special character. Your password may also have a maximum character count and should not be a word found in the English dictionary.

Q. What do I do if I have entered the wrong password too many times and am now locked out?
A. The system's security will lock your account after four incorrect password entries. We suggest that you click on "Forgot Password/PIN" if you have had three incorrect password attempts. Clicking on "Forgot Password/PIN" will generate an automated e-mail or text message to you with a temporary password (if you have enrolled to receive text messages in your online banking profile). Your password will be e-mailed to the e-mail address (or text phone number) that we have on file for you and will be required to be changed once you attempt to log in again. If the incorrect password is entered four times, your access will be locked out and you must have your online banking profile unlocked by contacting your Company's Primary Administrator or by calling our On-Line Banking Department at 1-866-642-7736.

Q. How can I change my account "nicknames" that appear in online banking?
A. A Primary Administrator can update account nicknames in online banking by choosing Admin Manager from the left-hand navigation bar and then choosing Accounts. An "Update Accounts" screen will appear with the option to change account nicknames and then those changes can then be saved. Account nicknames, when changed, will be updated for every user under the Company.

Q. Why does the log-in from the Bank's home page include a drop down of "Account Type" Choices?
A. Both personal and business on-line banking can be accessed through Mid Penn Bank's home page, as well as Trust account services. The drop-down box allows us to keep the login box for all of these different services in one easy to find location for users of multiple bank services.

Q. Can I use the same User ID if I have personal accounts and business accounts?
A. Yes. If not already in use, you can choose to use the same User ID for your personal accounts and your business accounts.

Q. Why don't I have access to all the accounts for the business?
A. When business online banking is created, it is based on the paperwork that was provided to the Bank by someone authorized per the Company's resolution on file with the Bank or per an authorized account signer. We can only add the accounts listed on the paperwork. If any changes are needed, such as adding accounts, changing access options or adding/deleting users, please complete a Form 2 online banking maintenance form available from our website and have it signed by the parties specified on the business resolution.

Q. If I need to have a co-worker do my online banking for me while I am out, can I share my User ID with another co-worker versus each of us having our own User ID and password to access the accounts?
A. Each business user must have his/her own User ID and password. This access is determined and granted by the parties on the business resolution, by an authorized account signer, or by the authorization provided to the Primary Administrator. User credentials should not be shared with

another employee. If a user is no longer with the company, or another user needs to be added, then the correct form must be completed to make any changes or the Primary Administrator can grant access to new users and delete users, as necessary. User ID's cannot be shared.

Q. If I transfer funds between my Mid Penn Bank accounts will the transfer occur immediately?
A. This is the quickest and easiest way to move transfer funds between accounts and the balance in your accounts is affected immediately, provided the transfer is completed before 6:30 PM Eastern Time. Any transfer scheduled after 6:30 PM will become effective on the next business day. You can also schedule transfers to be recurring or to occur on a future date by using the "Repeat Transfer" option.

Q. How can I pay my Mid Penn Bank loan payment?
A. Provided you have the ability to transfer to your loan (credit) and you have another Mid Penn Bank account that you wish to transfer the payment from (debit), then you can complete an internal bank transfer to your loan, which will complete the loan payment. You can choose to make a Principal Only Payment, an Interest Only Payment or a Regular Payment (Regular P & I), which will apply the funds to your current payment due, applying the funds to your principal and interest due.

Q. How do I enroll for eStatements?
A. To enroll your business account(s) for eStatements, please go to our website and click on Business link, then choose Business Online & Mobile. Scroll to the bottom of the page to the section labeled "Business Banking Enrollment Forms." Look for the "Business Account eStatement Enrollment Form" and click on the form name. This will open as a PDF and can be printed off after completing the information. Complete the form with all the accounts for your business and have it signed per your company resolution or an authorized account signer. Once completed, drop it off at the nearest branch or mail/fax it to the Bank using the information listed on the bottom of the form.

Q. What is the benefits of eStatements when I can already see my account statements online?
A. While you can view and download your bank statements online, when you enroll for eStatements, your online statement will also include copies of your check images at the end of your statement. Plus, we will turn off paper statements so that you don't need to worry about the paper statement being lost or stolen in the mail or having to shred your paper statement at a later date. Online statements can be saved to your PC, printed and retained or obtained electronically for a period of 18 consecutive months from our online banking portal.

Q. Can I cancel eStatements at any time?
A. Yes, should you or another authorized account signer want to cancel eStatements at any time, please contact our Customer Support Team at 1-866-642-7736.

Q. If I have questions or trouble logging in, who do I contact?
A. You can call 1-866-642-7736 Monday – Friday 8:00 A.M. to Midnight and Saturday & Sunday 8:30 to 5:00 P.M. Additional educational videos and user guides are also available on our website or you can use the "Contact Us" link from our website to obtain information during regular business hours.

Q. Do you offer Mobile Banking?
A. Mobile Banking is available. We recommend customers have a data plan with their cell phone prior to enrolling in mobile banking. Mobile Banking is free for all on-line banking users.

Q. How do I sign up for Mobile Banking?
A. Business customers would need to select this option when enrolling for online banking. If you are an existing Primary Administrator and would like to enroll for mobile banking, please contact the online banking department at 1-866-642-7736 or contact your local Mid Penn Bank Financial Center for more information on how to enroll. This will require additional paperwork be completed to add mobile banking services to your User ID.

Q. What can I do with Mobile Banking?

A. Mobile Banking will provide you with the capability to transfer funds between accounts, view account transactions, deposit checks to your account using the camera on your phone and uploading the check image(s) to the Bank, pay existing bill payments, etc.

Q. I have enrolled for Mobile Banking and Downloaded the App. Where can I find my Activation Code that is required to activate the Mobile App ?

A. Your software activation code can be found by logging into your online banking, choosing your "Profile" from the top right and then searching on the left-hand side for our software activation code. Enter your code into the app where required. The activation code is not case sensitive when entered.

Q. With the Bill Pay provider, when are funds debited from my account?

A. Funds for bill payments are either debited when the item clears your account, such as for a paper draft check, or if the payment is sent as an electronic payment, the amount of the payment will be debited from your account at the time the transaction is created. There are certain transactions that may be debited at the time the payment is sent, such as for large dollar payments. These are called single check payments.

Q. How do I add additional checking accounts to my list of bill pay accounts?

A. Existing bill pay customers can request to add additional accounts to bill pay by completing an enrollment form available from our website. You will receive an e-mail confirmation from our On-Line Banking Department when your additional account or accounts have been verified and added to your bill pay option. You must be an owner of an account to request to link it to your bill pay access. Contact our Customer Support Team with any questions by calling 1-866-642-7736.

Q. How do I download to Quicken® or QuickBooks®?

A. Currently, Mid Penn Bank **c**ustomers can download your bank account transactions and then import the saved file to your Quicken or QuickBooks. Once logged into Mid Penn Bank's on-line banking, click the "Accounts" option from the left-hand navigation menu. Select the account you wish to download into Quicken or QuickBooks. Under the Recent Transactions section, choose the Actions link on the right-hand side and then choose "History." Complete the "Transaction Date From" and "Transaction Date To" dates, then select the "Actions" link and choose the type of file you wish to download such as .csv, QuickBooks, Quicken (Windows), Quicken (Mac) or if you choose, you can simply print the report of transactions. If downloading, you should be prompted to Save your transaction report in the format you chose. Save the file somewhere on our PC/Network/Desktop so that you can easily find it. Then open your Financial Management software (Quicken/QuickBooks) and import the transaction file per the software instructions. You will need to know where you saved your file to import it to your software. Our system also supports Express Web Connect. You may need to request a separate log-in ID from the Bank just for use with QuickBooks.

MID PENN BANK

BUSINESS ACCOUNT GUIDANCE: PROTECTING YOUR ONLINE BUSINESS TRANSACTIONS

The FFIEC (Federal Financial Institutions Examination Council) is a formal interagency body of the United States government empowered to set uniform principles, standards and report forms for the federal examination of financial institutions by the major financial industry regulators and examiners, as well as to make recommendations to promote uniformity in the supervision of financial institutions. The FFIEC has issued new guidance to help banks assure your business accounts are properly secured during online transfers of any kind. By identifying the risks, learning to control them, and guidance from the FFIEC, we can achieve a much safer online experience.

WHAT RISKS ARE INVOLVED WITH ONLINE BANKING

Many organized criminal groups of fraudsters have evolved in their criminal activities, deploying more sophisticated methods to compromise authentication methods and gain unauthorized access to online account information. Online account takeovers and unauthorized fund transfers are real threats to users and banks. The techniques used by these criminals are being developed routinely in order to compromise sensitive data. The methods which are used by these organized groups have become complex and are now available for many to use by downloading from the internet. This has resulted in a significant increase of fraud; particularly electronic transactions.

BANK CONTROLS

Not every online transaction poses the same level of risk, therefore, banks are encouraged to implement more layered security controls for higher risk transactions, such as ACH file origination, wire transfer capabilities and remote deposit capture services. Transactions that present greater risk allow for the easier movement of funds and allow for faster fund settlement. Due to the fact that these transactions are simple to originate and move money across accounts, the greater the level of controls that are needed. Mid Penn Bank has a variety of controls that are set in place in order to provide the use of electronic banking services in a secure environment. The controls are not always identical. Enhanced controls are designed to exceed the controls provided to routine customer users. Mid Penn Bank uses multi-factor authentication, as well as additional “layered security” measures for higher risk transactions. Authentication is simply the process used to confirm that it is you, and not someone who has stolen your identity. Authentication typically involves one or more basic factors, including: something the user knows (password, PIN), something the user has, (ATM card), something the user is (fingerprint). Single factor authentication uses one of these methods and multi-factor authentication uses more than one method combined, which of course, is considered a stronger fraud deterrent.

Layered security is simply a practice of combining multiple security controls to protect resources and data. The use of different controls at different points in a transaction process means that a weakness in one control could be generally compensated for by the strength or requirement of another control. Layered security can substantially strengthen the overall security of online transactions. Examples of layered security controls for your business accounts include: Verification that all online enrollments and online changes are requested by an authorized representative of your company, dual customer authorization of transactions is available, limiting access times to online banking is available, transaction value thresholds (including per day, per file and per user dollar values) can be assigned, account maintenance controls limiting activities performed by users, alerting you to new bill payments established, account alerts, and the issuance of tokens that generate one-time passwords for online access. We can also limit user logins to certain restricted IPs and highly encourage this as another security option. Taking advantage of a variety of services from your financial institution will help in providing ways of monitoring account activity. All of these security measures are available to you, in addition to anti-virus and anti-malware software, firewalls, data encryption, granting network permissions on an as needed basis, etc.

BUSINESS/USER CONTROLS

Risks are different for each business. In order to reduce the risk of account fraud, an assessment of the risks that may impact your company should be conducted. Your business should design and develop methods to combat fraud and implement the security measures into the business practices. Layered security allows for prevention of your data being compromised. Layered security involves having multiple

methods of prevention for one point of access.

Some examples are installing anti-virus and anti-malware software, installing or choosing automatic operating system patches and updates, firewalls on your computer, data encryption, using secure sites (verify url address starts with https:// prior to entering any confidential information such as passwords or account information), and never opening attachments to e-mails that you are not expecting. Other methods may include account reconcilement, dual control, and granting network permissions on an as needed basis. These controls assist the checks and balances process within your business. Taking advantage of a variety of services available from your financial institution will help in providing ways of monitoring account activity. This includes requiring dual customer authorization of transactions, limiting access times to online banking for users, setting transaction value thresholds (including per day, per file and per user dollar values), account maintenance controls limiting activities performed by users, securing access devices such as passwords and tokens and never sharing this information with others.

REGUATION E

Regulation E is an outline of rules that have been placed in order to provide a guideline for Electronic Funds Transfers (EFT). If you have any questions regarding Regulation E and your business services with us, you may refer to the ***Electronic Fund Transfers – Your Rights and Responsibilities (Business Accounts)*** disclosure. You may also contact us by phone, email or by visiting a Mid Penn Bank Financial Center.

WHO TO CONTACT

If you believe your online banking information has been compromised, please contact us as soon as possible. We will assist you through the process of resolving the issue or answer any account security questions you may have. Contacting us by phone is the fastest way to reach us and is the preferred contact method. You can also call our Fraud Hotline at 1-866-372-8433.

- **By phone: 1-866-642-7736**
- **By email: online@midpennbank.com**
- **By mail: Mid Penn Bank**
  Electronic Banking Dept
  894 North River Rd
  Halifax PA 17032

ADDITIONAL RESOURCES

Additional resources are available to review regarding online safety and security. These websites include:

- **www.staysafeonline.com**
- **www.idtheft.gov**
- **www.ftc.gov**

MID PENN BANK

Business On-Line Banking Security Tips

Mid Penn Bank is pleased to offer the convenience of On-Line Banking. We are always concerned about your security no matter how you access your accounts. The following suggested security tips will help you keep your PC and your on-line banking secure.

- **Protect Your Password.** You determine what password you will use, and the identity of your password should not be communicated to us. You accept responsibility for the confidentiality and security of your password and agree to change your password regularly.

- **Password Requirements.** 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. If it is necessary to write down your password, it should not be stored near your computer. Your password should not be a word found in the English dictionary. Passwords have minimum requirements, including password length, the inclusion of upper case, lower case, numbers and special characters when composing a password and use of out of band codes as well.. Password requirements are subject to change. Passwords are also required to be changed on a regular basis, the term of which may also change.
- **Internet Banking System Services.** Mid Penn Bank may, at our discretion but not obligation, verify instructions received by Bank via the Internet Banking System by inquiry to you at the telephone number(s) specified by you in your account records with us.

- **Equipment.** Your use of the System requires a compatible personal computer (with sufficient power and memory), a modem or other Internet access device, an Internet Service Provider (ISP) and a capable browser.

- **Software.** Always maintain your software updates, security patches, and service packs on **ALL** your software. You may have other software running on your device besides a Microsoft operating system (OS). Make sure you're maintaining updates on other software such as iTunes, Java, Adobe Reader, Flash and other non-OS-specific software. Every software developed has updates from time-to-time and many fix known security issues. Remember, within 24 hours of a patch being released, someone out on the Internet has already started exploiting the problem the patch fixed. Prompt updates insure you are not a victim.

- **Security.** It is your responsibility to utilize a browser that supports the minimum level of encryption so that you can access Mid Penn Bank's On-Line Banking System.

- **Security.** You acknowledge and agree that there are certain security, corruption, transmission error and access availability risks associated with using open networks such as the Internet and you hereby expressly assume such risks (to the extent the law allows you to do so).

- **Security.** You understand the importance of your role in preventing misuse of your accounts through the System and you agree to promptly examine your account statement(s) as soon as you receive it (them). You agree to protect the confidentiality of your account(s) and account number(s), and your personal identification information, such as your driver's license number and social security number.

- **Security.** You agree that you will promptly notify us of any security compromise, or potential security compromise, of your initial password/PIN or any subsequent password/PIN established by you.

- **Virus Protection.** We encourage you to routinely scan your computer, disks, and software using a reliable virus product to detect and remove any viruses found. Undetected or unrepaired viruses may

alter, corrupt, damage, or destroy your programs, files, and even your computer. Additionally, you may unintentionally transmit the virus to other computers, disks and software.

- **Wireless Security.** If using wireless technology at home, we encourage you to review the "Basic Wireless Security Tips" document for additional security practices.

NOTIFY THE BANK IMMEDIATELY IF YOU SUSPECT FRAUD

- If you suspect fraud or fraudulent attempts on any of your accounts, notify the Bank immediately. You can contact your local Mid Penn Bank Financial Center during regular banking hours or call 1-866-642-7736 Monday through Friday 8:00 A.M. – Midnight and on Saturday & Sunday from 8:30 A.M. – 5:00 P.M. If you do not reach a representative, please leave a voice mail stating that you believe there is fraud on your account and the best phone number to reach you. Please include an after-hours contact number if possible. We recommend, if you do not reach a representative, log into your online banking and change your password immediately. For further protection, we recommend you purposely enter a wrong password multiple times until you lock your account out. **This is your best protection until a bank representative can call you back to review the account with you. Under some circumstances, we also recommend you turn off the power to your computer, especially if you allowed someone to remote into your computer under the assumption to do "repairs" to your computer system.**

MID PENN BANK

Basic Wireless Security Tips

Wireless security is a hot topic these days, and different advice abounds. Here's a checklist to make sure you have the basics covered:

- **Change Default Administrator Passwords (and Usernames)**
  At the center of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Changing these settings immediately is essential to a secure Wi-Fi network. Always choose strong passwords. (Strong passwords are at least 12 characters in length and contain upper case letters, lower case letters, numbers and symbols, and are not a word found in the dictionary, etc)

- **Use Vendor-Supplied Security.** Since the capabilities of each wireless router/access point/bridge differ from brand to brand, it's best to get the vendor's recommendation on the best security options for their devices

- **Turn Off Remote Management.** Turning off remote management will prevent people from managing your router from the WAN.

- **Turn On (Compatible) WPA / WEP Encryption**. All Wi-Fi equipment supports some form of encryption. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore you may need to find a "lowest common denominator" setting.

- **Use Strong Encryption**. Industry-standard Wi-Fi Protected Access (WPA) or WPA2 is preferred if supported by many mobile devices.

- **Consult The Vendor About Antenna Positioning.** Different antennas radiate signal in different patterns. Check your vendor's documentation to verify optimal antenna positioning for your wireless network.

- **Change the Default SSID Broadcast.** Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "linksys." True, knowing the SSID does not by itself allow your neighbors to break into your network, but it is a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring wireless security on your network. Also, some vendor's may offer the option of not broadcasting this network identifier.

- **Disable SSID Broadcast.** In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. In the home, this roaming feature is unnecessary, and it increases the likelihood someone will try to log in to your home network. Fortunately, most Wi-Fi access points allow the SSID broadcast feature to be disabled by the network administrator.

- **Keep Your Wireless Router/Access Point/Bridge Firmware Up To Date.** New firmware can help resolve compatibility problems, plug security holes and provide other important fixes. Check the vendor's website for these updates regularly. (Firmware is a software program or set of

instructions programmed on a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.)

- **Use A VPN For Working At Home.** For enterprise users working at home, always check with your enterprise IT department or help desk for best practices regarding accessing the company network over your wireless home network. Often, virtual private network (VPN) software is required for this purpose.

- **Enable Firewalls On Each Computer And The Router.** Modern network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on. For extra protection, consider installing and running personal firewall software on each computer connected to the router.

- **Use A Good Antivirus And Good Firewall Protection.** Many of the security software vendors have special encryption toolbars for wireless connections. It senses when you are using wireless and automatically engages the encryption keyboard for use in your browser. Most hackers and identity thieves don't want to have to work hard, so by encrypting your information, you make it harder for them and they will move on to the next person who's giving away their information easily. A good firewall will block any suspicious incoming packet – a good thing to do when on unsecured wireless.

- **Keep Your Antivirus Software Up To Date.** Viruses, worms and Trojans are a continuous threat. Make sure your wireless network is not a haven for these problems by keeping your antivirus software up to date.

- **Do Not Auto-Connect to Open Wi-Fi Networks.** Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbor's router exposes your computer to security risks. Although not normally enabled, most computers have a setting available allowing these connections to happen automatically without notifying you (the user). This setting should not be enabled except in temporary situations.