CAPITAL EXPRESS ONLINE BANKING POLICY AND AGREEMENT

FOR BUSINESS

THE CAPITAL EXPRESS SERVICE

In consideration of the use of the Capital Express Internet Banking Service ("Service") to be provided to you by Capital Bank, ("Bank") as described herein and as amended from time to time in information distributed by The Bank to its customers, you agree to the terms of this Agreement. In this Agreement, "Customer" or "you" refers to the person(s) subscribing to or using Capital Express. You may use a Personal Computer ("PC") through an Internet connection to obtain account balances and transaction information. You may also use your PC to obtain statements on your accounts and to transfer money between your accounts. However, transfers from your savings and Money Market accounts are considered pre-authorized transfers, and pre-authorized transfers are limited to six (6) per monthly statement cycle by federal regulations. In addition when the Service becomes available, you may use your PC to electronically direct us to make Bill Payments ("Bill Payments") from your account to third parties ("Payees") that you have selected to receive payment through the Service. You may make payments through the use of the Bill Payment service to any business, professional, merchant, family member, or friend. The "Account" means your designated Bill Payment account at The Bank from which we make Bill Payments or transfers on your behalf pursuant to this Agreement.

ELECTRONIC DISCLOSURE

For you to continue enrollment for this Service, you need to agree to the following electronic disclosure, permitting us to send you important information electronically. You give your consent to the terms of this Agreement by continuing with the enrollment process for Capital Express and using the Service. You acknowledge you have received and read the error resolution provisions of this Agreement and your liabilities for errors by proceeding with use of the Capital Express Service.

PERSONAL INFORMATION COLLECTION

Certain personal information about visitors to this Web site is being collected by the Bank. Personal information is collected from you at the time an application for a loan or deposit account is submitted to us, at the time transactions are conducted through the online banking Service, and at the time information is provided by you via e-mail (including the name, e-mail address, and any other information on the e-mail header). The Bank does not use "cookies" to collect and track information about you.

At this time, the Bank does not collect information for loans or deposit accounts over the Internet, these types of accounts must be opened by contacting the branch office directly. Please refer to Capital Bank's Privacy Statement, for additional information about customer information collected and disclosed by the Bank.

DISCLOSURE OF ACCOUNT INFORMATION TO THIRD PARTIES

We may disclose information to third parties about your Account or the transactions you make:

a. where it is necessary for completing transactions or resolving errors involving the Services; or
b. in order to verify the existence and condition of your Account for a third party, such as a credit bureau or a merchant; or
c. in order to comply with government agency rules, court or administrative agency orders, or other applicable law or regulation; or
d. to our employees, service providers, auditors, collection agents, affiliated companies, or attorneys in the course of their duties and to the extent allowed by law; or
e. if you give us your permission.

PROTECTION OF INFORMATION

We are taking the following steps to ensure the privacy and accuracy of the information collected from or about you:

a. Ensuring your financial privacy is of vital importance to the Bank and its employees. and
b. The Bank limits employee access to confidential customer financial information who have a business reason for knowing the information. and
c. Bank employees are trained to understand the importance of customer financial privacy and to properly handle confidential information. and
d. The Bank endeavors to maintain the most accurate and up-to-date customer records possible. and
e. If you find that your account information is not correct, current, or complete, please call or write to us at the telephone number or address on listed below under errors and complaints Appropriate corrections will be made as soon as possible.

SYSTEM SECURITY

The Bank continually updates and improves its security standards and procedures to help protect against anyone gaining unauthorized access to your confidential information and to prevent fraud. We maintain physical, electronic, and procedures safeguards that comply with federal standards.

The Bank has taken every precaution to ensure a secure environment for our Internet banking customers. To accomplish our goal of secure Internet banking, we have contracted with one of the best service providers in the business, ITI Fidelity., who employs state of the art Internet firewall and network security technologies.

Additionally, the Capital Express Internet banking Service uses several different methods to secure and protect your personal information:

- **Access IDs and Passwords**
  Access to the Capital Express Service and your accounts requires your valid Access ID and separate Password that you change as often as you like. At a minimum, the Bank requires that your password be changed every 90 days.
- **Strong Passwords**
  Your password is case sensitive. It must be at least 8 characters long and no more than 15 characters. There must be at least 3 numbers (1,2,3, etc.) , 4 letters (a,b,c, etc.) and one symbol (!,@,#,$, etc.).
- **Automatic Time Out**
  Capital Express Service will automatically log you out of your session after 15 minutes of non use (in case you forgot) and to prevent unauthorized access.
- **Security Enhancements**
  The Capital Express Service is constantly monitored and evaluated. The Service is tested regularly to detect any potential problems that might compromise security or privacy. Security technologies are always being evaluated, and the Service is upgraded whenever relevant improvements are identified. We also endeavor to keep you informed of any security upgrades available for your system through messages and links to software provider sites. Multi Factored Authentication is also a security feature which functions through a multi-layered approach to authenticate the rightful account user before access to account-sensitive information is achieved.

YOUR RESPONSIBILITY TO SECURITY

The security of your accounts and personal information accessible through the Capital Express Service is a joint responsibility of the Bank and you, the customer user and any authorized user(s) assigned by you.. We will keep our security pledge to you, and in return, you are asked to fulfill certain responsibilities in our partnership to protect you and the Service. Among the precautions you should take to help protect your accounts and information on the Capital Express Service are:

ACCOUNT CONTROLS FOR ONLINE BANKING

1. Understand the bank's account agreement and customer liability for fraud under the agreement and the Uniform Commercial Code
2. Institute check cashing limits and automated payment filters
3. Reconcile or at least view online all banking transactions on a daily basis early in the day (to enable you to spot unauthorized activity immediately)
4. Consider using the Bank's latest transaction monitoring program, *"Positive Pay"* to ensure transactions that will post to your account are authorized.
5. Initiate ACH and wire transfer payments only under dual control (one person sets up the payment information, 2nd person authorizes and sends to the Bank)
6. Delete the web browser cache, temporary internet files, cookies & history so if your PC is compromised the hacker or malware cannot steal this data.

7. Do not alter anti-virus programs installed on your PC

COMPUTER SECURITY PRACTICES

1. Consider IMMEDIATE installation of PC software security updates & patches from the vendor. These often fix zero day exploits and vulnerabilities.
2. Always use a firewall, anti-virus & anti-spyware software. Keep it up to date. Install it on your home PC if you use your home PC for your business.
3. Never use default passwords that come with your PC, firewall system, wireless devices/access point or other programs. Use hard to guess, complex passwords using a combination of letters, numbers & special characters. Don't reveal your password in emails or talk about how you choose your password in front of others or on social networking sites.
4. Consider removing "Local Admin" rights to your user's PC log-ons. Many (but not all) malicious programs need Admin PC user rights to install.
5. DO NOT click on pop-up windows that purport to update your anti-virus software. These are likely tricks that will install malicious software.
6. DO NOT use a public Wi-Fi "hot spot" to conduct internet banking transactions.
7. Never share computer credentials with third-party providers or allow employees to share user account ID's and passwords.
8. Be aware that your company's/customer's information may be as valuable as your bank account balances. Protect this information as well.
9. We recommend that you place and enforce limits on the use of your computing resources for non-work purposes. Use of third party email (Yahoo, Hotmail, Google, others of this type) and social networking sites increases risks significantly; ideally access should be banned. (You can maintain separate "guest" networks in break rooms and visitor offices that allow this access, but block on the production/business network.)
10. Learn how to spot spear phishing email messages and avoid them, don't even click on them or the links within the message. The Bank does not send customers emails with links embedded in them to "verify" transactions or account information. Call us if you are not certain.
11. Make a regular back up of your important data onto a device not normally connected to your PC; keep it in a secure location.
12. Adopt strong PC security policies and procedures and train your employees on the expectations. Set up "rules of behavior" to protect your systems.

When you enroll for Capital Express with Capital Bank and first use the Service, you agree to the terms and conditions explained in this Agreement & Disclosures provided to you. Although the Bank has taken every reasonable precaution to assure account security, you agree that the Bank is not liable for security breaches that occur for reasons outside of our control or for any fraud, negligence, misconduct conducted by anyone who gains access to your accounts or otherwise by an authorized user who was assigned by you. The Bank cannot be responsible for customer errors or negligent use of the Service, and will not cover losses due to:

- Customer input errors or misuse of any aspect of the Internet banking Service.
- Negligent handling or sharing of Access IDs or Passwords leading to unauthorized access to accounts.
- Leaving a computer unattended during a Capital Express session that result in disclosure of personal information or unauthorized transactions on accounts.
- Failure to promptly report known incidents of unauthorized account access.
- Liability Limitations as described below.

Each time you make a transfer or payment with a Service, you warrant that our security procedures are commercially reasonable (based on the normal size, type, and frequency of your transactions). Some of our Services allow you or your Administrator to set transaction limitations and establish internal controls. Your failure to set such limitations and implement such controls increases your exposure to, and responsibility for, unauthorized transactions. You agree to be bound by any transfer, instruction or payment order we receive through the Services, even if it is not authorized by you, if it includes or was generated with your Access Credentials or is otherwise processed by us in accordance with our security procedures.

You bear sole responsibility for establishing, maintaining, implementing and updating policies, procedures, equipment and software ("Internal Security Controls") that ensure the security and integrity of your computer systems and information, protect them from any unauthorized use, intrusion, takeover or theft, and prevent your Access Credentials from any unauthorized discovery or use (collectively "Internal Security Breaches"). You bear all risk of fraudulent transfers and other losses or disclosures arising from your Internal Security Breaches or from the interception of your communications prior to their receipt by us (collectively "Internal Security Losses"). We will not reimburse your Internal Security Losses. You agree that we are authorized to execute, and it is commercially reasonable for us to execute, any instruction received by us with your Access Credentials, even if it is not authorized by you. You are encouraged to consider purchasing insurance to cover your Internal Security Losses.

To protect your system from Internal Security Breaches, your Internal Security Controls should include:

- Limiting and controlling who has access to your computer systems;
- Protecting and frequently changing your passcodes and other Access Credentials;
- Adopting dual authorization and/or transaction-based authentication procedures for financial transfers;
- Employing up-to-date security software such as anti-virus, anti-malware and anti-spyware programs, as well as up-to-date software patches for all your software programs, internet browsers, e-mail programs, and the like;
- Using effective, up-to-date firewalls;
- Procedures to avoid infection by malicious software, such as controlling what websites are visited by your computers; controlling the connection of other devices to your computers; controlling what documents, e-mail attachments, programs and other files are opened or installed on your computers;
- Limiting which of your computers are used for online banking;
- Reconciling all accounts on a daily basis, and immediately reporting any discrepancies;
- Prohibiting your authorized users from leaving a computer unattended while connected to our Service, or from communicating or accessing sensitive information from insecure locations (e.g., terminals or networks at Internet cafes or airports);
- Allowing Services to be accessed only from a secure location on your premises;
- Prohibiting your Access Credentials or account information to be sent through any public or general email system; and
- Adopting such other recommendations that we may make from time to time to help ensure your safe use of our Services.

This is not a complete listing of the Internal Security Controls that you may need. You are solely responsible for determining and implementing all of the Internal Security Controls necessary to prevent Internal Security Breaches and Internal Security Losses. We have no duty to review your Internal Security Controls, identify deficiencies or make recommendations. We do not represent or warrant that any or all of the above recommendations or any future recommendations are adequate for your needs or will prevent Security Losses.

We may at any time limit access to any online banking function to only those customers who have adopted specific Internal Security Controls required by us (e.g., this may include the use of tokens or other authentication devices). Our specification of any required Internal Security Controls shall not constitute a representation or warranty by us that they will (a) prevent any Internal Security Breach or Internal Security Losses, or (b) be compatible with any computer system or other Internal Security Controls.

You remain at all times solely responsible for your Internal Security Controls, Internal Security Breaches and Internal Security Losses. Although we may employ various systems and procedures from time to time to prevent losses to us, we assume no obligation for your Internal Security Losses.

HOW OUR SYSTEM SECURITY WORKS

Data is in transit both when it is being acquired by the Service (from The Bank) and when it is being queried by you, the customer end user. To provide a safe means of getting the data from the Bank to the Service Data Server the following method is used: The Bank initiates an encrypted logon to the firewall. The firewall authenticates the request and sets up an encrypted file transmission session with the Data Server located on the private internal network (inside the firewall). Thus, when the Bank begins transmitting the data, it is encrypted and thus, protected from snooping attacks. To prevent snooping the customer end user during account queries, we're using Secure Socket Layer (SSL), a powerful encryption and server authentication protocol, based on the RSA encryption technology. The Internet Information Server supports 128-bit encryption keys, which provides the highest level of encryption capability available for SSL.

Several layers of security protect the Data Server, SQL Server for Windows NT. The Data Server is located inside the firewall, on a private internal network. All requests to this Data Server must come through the firewall that only allows legitimate requests from the Web Server. In other words, the only machine that the Data Server is talking to is the Internet Server and the only way it will do that is from safely behind the firewall. Combined with the filtering router on the perimeter, this means no one can access the data directly from the Internet. The data is in effect "hidden" from the Internet. The

Data Server contains a "mirrored" drive arrangement that prevents any loss of data or denial or Service even if one of the drives crashes. The Data Server is also attached to an Uninterruptible Power Supply (UPS), which will keep the server on-line, even during a power outage.

Furthermore, the Windows network on which the Internet banking applications run have been tightly secured at the operations system level and at the application level of the Internet Information Server and SQL Server. In addition to these precautions, the network is monitored extensively. Every logon, successful and failed, is reviewed to pinpoint any intrusion attempts (accounts are locked out after three failed logon attempts). If necessary, these logon attempts may be traced back to the source by the user's IP address, request time, etc.

In summary, a secure environment is provided for Internet banking by protecting customer data both in transit and on the Data Server. The combination of the filtering router, the tightly secured Web Server, the firewall and the hidden Data Server make this secure environment work. Finally, all network activity is monitored and recorded to prevent intrusion.

SECURITY HIGHLIGHTS

Security is more than just preventing unauthorized computer access. Security means minimizing the risk of interrupted Service too. In addition to providing protection against unauthorized access, we reduce the risk of equipment failures, power failures, computer viruses, and disasters.

ICSA Certification: The Bank's Internet banking service provider, ITI Fidelity, is ICSA Certified. This certification involves an extensive ICSA onsite and external security audit including ongoing external "intrusion testing".

Encryption: We use the Secure Socket Layer (SSL) protocol, based on RSA encryption methods, to ensure that data passing through the Internet is kept secure. This includes support for "strong" or 128 bit key encryption. Encryption protects data from being monitored while it is being transmitted.

Firewall: The firewall protects our servers against unauthorized access from the Internet. All access from outside the Internet banking Service goes through the firewall.

Internet Banking System: The Bank's core processor's servers are secured at the operating system level, at the database level, at the Web server level, and at the Internet banking application level through user login and passwords.

Server Authentication: We obtain a Digital ID (also known as a Digital Certificate) from a Certificate Authority. Our Certificate Authority is VeriSign, Inc. This Digital ID ensures that a customer looking at a page on our server is actually using our server. If you are looking at a fraudulent page, your browser will warn you that the Digital Certificate does not match.

Password Security: The Bank's personnel logins for performing customer and Bank level maintenance requires an eight character alphanumeric password. Customer logins require an Access ID (assigned by the Bank) and Password. Although the Bank sets the initial Password, you will be prompted to change the password and you cannot gain access to the accounts until the password is first changed by you. The Bank's personnel cannot see a private Password that has been set by the customer. The Bank has set security options to specify the minimum password length, require passwords to be a mixture of alphabetic, numeric and symbol characters, and to control how many failed login attempts "lock" a customer out and for how long. All failed login attempts are reported to the Bank through standard reports. In addition to your password, the Bank's platform utilizes Multi-Factored Authentication which prompts for your answers to security phrases established by you. Your entry into the Service may also require a token. Tokens are provided to account holders upon request who have multiple accounts established on the site and with multiple account functions such as funds transfers, ACH credit and debit activity. You have the option of a token method of authentication or a security phrase method of authentication.

Monetary Transfers: The Bank, at the individual account level, enables this feature. The customer can only transfer funds between accounts that have been pre-authorized and set up by the Bank. The Bank may set an individual dollar transfer limit per day for each account or use the account balance as a limit. Refer to the account sign up form to determine the types of money transfers you may require for each account.

Audit Trail: Every "hit" on any Web page is recorded, even anonymous browsing. Every maintenance login is logged. Every customer login is logged in the Internet Banking application. All the Bank and customer activity is logged.

Direct Hosting: Our service provider does not outsource the hosting of Internet banking. The data is running on our core processor's servers, by their personnel and the Bank. Communication lines and access to the Internet are provided directly by the telephone company. There is no other intermediate Internet Service Provider (ISP) or local communications company involved.

Disk Redundancy: Our Internet servers have either mirrored hard drives or RAID drives to reduce the risk of problems associated with a "disk crash".

UPS (Uninterruptible Power Supply): All Internet servers are connected to a data processing caliber UPS (battery backup) for protection against power failures. This is not to be confused with UPS systems meant to protect against momentary or transient power outages.

Disaster Recovery Capability: Both the Bank and our core processor maintain a separate disaster recovery center or "hot site". This hot site includes duplicate communication lines already programmed for a "switch over" in a disaster. This means there is a minimized risk of disruption of customer service. Daily offsite data file backups are maintained.

Virus Checking: Our servers are protected against computer viruses through automated ongoing scanning processes utilizing several commercially available anti-virus and anti-malware systems that are expertly maintained and updated.

Secure Socket Layer (SSL) Technology: The Secure Socket Layer Protocol was developed by Netscape to protect information transferred over TCP\IP-based protocols and applications such as HTTP (the Web protocol), FTP, Gopher, etc. To simplify, what the SSL protocol does is establish an encryption key between the client (your web browser) and the server (our Internet server). After this key is established, only the client and server can decode the information transmitted between them. As long as your web browser stays in a secure area, you can be assured that all data transmitted and received is protected.

ERRORS AND COMPLAINTS

You may review the information we collect about you and correct any errors in that information by reviewing account statements and any other correspondence from us and notifying us of any inaccurate or outdated information at the address or phone number on your statements within 30 days of the date of the statement.

You must contact us if you believe your statement or receipt is wrong, or if you need more information about a transaction listed on your statement or receipt. You will need to:

a. tell us your name and Account number (if any);
b. describe the error or the transaction you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information; and
c. tell us the dollar amount of the suspected error.

Notify us **IMMEDIATELY** if you believe your password has been lost or stolen or compromised in any way. If you believe your password has been lost or stolen or that someone has transferred or may transfer money from your account without your permission, call (301) 468-8848 during normal business hours listed above and or email operations@capitalbankmd.com.

We do not assume any other liability or otherwise guarantee the security of information in transit to or from our facilities. We reserve the right to (1) monitor and/or record all communications and activity related to the Service, and (2) require verification of all requested transfers in the manner we deem appropriate before making the transfer (which may include written verification by you). You agree that our records will be final and conclusive as to all questions concerning whether or not your password was used in connection with a particular transaction. If any unauthorized use of your password occurs you agree to (1) cooperate fully with us and appropriate law enforcement authorities in identifying and prosecuting the perpetrator, and (2) provide any assistance requested by us in recovering any unauthorized transfer of funds.

If you have questions about your personal information or would like to inform us about the potential misuse of your personal information, you may do so by notifying us at:

Capital Bank,
Operations Department
One Church Street, Suite 300
Rockville, MD 20850 or
Send a telefacsimile to operations at 240/283-0419 or
Contact us at (301) 468-8848, or 877/568-4262

e-mail us at operations@capitalbankmd.com.

Since e-mail transmissions may be subject to interception by an unauthorized person, if your correspondence contains sensitive information (e.g., your account number or social security number) please do not send us an email, please send a letter or telefacsimile to us instead. Or use the Bank's secure email transmission system available at www.capitalbankmd.com.

If you feel we have not met our obligations in the protection or use of your personal information, you may submit a complaint to the Bank. Any complaint will be handled in compliance with the Bank's Complaints Policy.

EXCEPT AS OTHERWISE PROVIDED IN THIS AGREEMENT, NEITHER WE NOR OUR SUPPLIERS OR VENDORS MAKE ANY WARRANTY, EXPRESS OR IMPLIED, IN LAW OR IN FACT, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE OR OF MERCHANTABILITY, WITH RESPECT TO THE SERVICES OR ANY COMPUTER PROGRAMS, EQUIPMENT OR SOFTWARE MADE AVAILABLE TO YOU.

You agree to notify us promptly if any equipment or software we provide to you becomes defective. Our sole responsibility (if any) in such instances will be to replace or repair such defective equipment or software. We do not warrant that any equipment or software provided to you will be error free or that the Services will be uninterrupted.

You agree to comply with the terms of any software license provided to you in connection with the Services. You may not transfer, distribute, copy, reverse compile, modify or alter such software. Unless otherwise agreed by us in writing, any equipment, Service guides, security procedures, and systems provided to you in connection with a Service represent our proprietary property and must be returned to us upon request. We and/or our suppliers retain all right, title and interest in and to the intellectual property rights associated with the Services and the equipment and software provided to you. Your license to use equipment and/or software provided to you will end with the termination of this Agreement or upon our earlier notice to you. You may only use such equipment and software in connection with your use of the Services. You may not use or move such equipment or software outside the United States without our written consent.

LIMITATION OF LIABILITY.

Except as otherwise stated in this Agreement, we will be liable to you only for damages arising directly from our intentional misconduct or gross negligence in the performance of the Services. We will not be responsible for any loss, delay, cost or liability to the extent that it arises, directly or indirectly, in whole or in part, from: (a) your actions or omissions, or those of third parties which are not within our immediate and reasonable control (including, but not limited to, your Internal Security Breaches or the interception, corruption and/or modification of instructions that you send to us); (b) your negligence, misconduct or breach of any agreement with us; (c) any ambiguity, inaccuracy or omission in any instruction or information provided to us; (d) any error, failure or delay in the transmission or delivery of data, records or items due to a breakdown or transmission error in any third party computer or communications facility; (e) accidents, strikes, labor disputes, civil unrest, fire, flood, water damage (e.g., from fire suppression systems), or acts of God; (f) causes beyond our reasonable control; (g) the application of any government or funds-transfer system rule, guideline, policy or regulation; (h) the lack of available funds in your account to complete a transaction; (i) the funds in your account being subject to legal process or other encumbrance restricting a transaction; (j) our inability to confirm to our satisfaction the authority of any person to act on your behalf; (k) losses for which we are not liable by law, NACHA rules or other clearinghouse rules, or for which you have agreed to indemnify or release us; (l) losses for which you fail to give us timely notice; or (m) your failure to follow any applicable equipment or software manufacturer's recommendations or our Service instructions. There may be other exceptions to those noted above in other sections of this Agreement or as stated in your Deposit Account Agreement.

We will not be responsible under any circumstances for special, indirect, or consequential damages which you incur as a result of our actions or omissions, even if we have been informed or are aware of the possibility for such damages. Our liability and your remedy for actual costs and losses resulting from our failure to transmit funds in the correct amount or to the correct beneficiary listed in your funds transfer orders shall not exceed the direct money damages that you incur as a result of the failure (e.g., the amount of a wire transfer that is sent to the wrong party, or the amount by which a transfer exceeds the amount you authorized, plus interest as permitted by law). In all other cases, our liability and your remedy for actual costs and losses resulting from our actions and/or omissions, whether the claim is in contract or tort, will not exceed the lesser of (i) six times the average monthly charge for the Service(s) in question for the three months immediately preceding the cost or loss, or (ii) $20,000. We shall not be liable for any punitive damages.

Any claim, action or proceeding by you to enforce the terms of this Agreement or to recover for any Service-related loss must be commenced within one year from the date that the event giving rise to the claim, action or proceeding first occurs. You agree to cooperate with us in any loss recovery efforts we undertake to reduce any loss or liability that arises in connection with your Services. You acknowledge that our Service fees have been established in contemplation of: (a) these limitations on our liability; (b) your agreement to review statements, confirmations, and notices promptly and to notify us immediately of any discrepancies or problems; and (c) your agreement to assist us in any loss recovery effort.

INDEMNIFICATION.

In addition to the other indemnity provisions set forth in this Agreement, you agree to release and indemnify, defend and hold harmless us, our parent company, affiliates, and subsidiaries, and our respective directors, officers, employees and agents, from and against any and all Losses which result directly or indirectly, in whole or in part, from: (a) our actions or omissions, if they are in accordance with your instructions, the terms of this Agreement, or instructions purporting to come from you that are accompanied by your Access Credentials; (b) the actions or omissions of you, your agents or employees; (c) any warranty that we are required or deemed to make to a third party in connection with your transactions, provided we act in compliance with this Agreement; (d) your use or distribution of any equipment or software made available to you through a Service that is inconsistent with the license or sublicense that you receive; (e) your failure to comply with applicable law, NACHA rules or the rules of any clearing house or payment organization that processes your transactions; or (f) your Internal Security Breaches or Internal Security Losses. You agree that this indemnification shall survive the termination of this Agreement.

CHILDREN'S INFORMATION

We recognize the importance of protecting children's identities and privacy online. We comply with the Children's Online Privacy Protection Act. Our website is not directed at children, and we do not knowingly collect or maintain personal information from children under the age of thirteen unless that information is provided to us by an adult authorized to do so.

SYSTEM REQUIREMENTS FOR YOUR COMPUTER

To provide you with the highest level of protection and the best visual use of Capital Express, we require 128 bit encryption. You may need to upgrade your browser to at least Explorer 5.0 or greater to meet this requirement. You can do so by downloading the latest security upgrades from Microsoft's download center at http://www.microsoft.com/downloads/search.aspx?displaylang=en

- You should have a printer so you can print a copy of this Agreement for yourself as well as any other documents you wish out of Capital Express.
- You should set your screen resolution to a minimum of 800 x 600 pixels for best viewing.
- You are solely responsible for the equipment you use to access Capital Express (including, your personal computer and any software you may need to access the Internet). We are not responsible for errors or delays or your inability to access Capital Express caused by your equipment.
- We are not responsible for the cost of upgrading your equipment to stay current with the Capital Express, nor are we responsible, under any circumstances, for any damage to your equipment or the data resident on your computer equipment.

DELIVERY OF YOUR PAYMENTS AND TRANSFERS

You may schedule payments to be initiated on the current business day, on a future date, or on the same date of each month, subject to the restrictions in the Agreement. Although you can enter payment information through Capital Express twenty-four (24) hours a day, seven (7) days a week, payments can be initiated only on business days. Funds will be deducted from your Account on the business day on which a payment is to be "initiated." This date is referred to in this Agreement as the "Transaction Date." If you direct the initiation of a payment to occur on a day other than a business day, it will be initiated on the previous business day. After funds are withdrawn from your Account, we may remit your payments by mailing your Payee a check, by electronic funds transfer, including ACH (Automated Clearing House) or by other means. ACH payments should be set up and submitted on Capital Express 3 days before the date you desire the payee to receive the funds. For bill pay due to the time it takes to send check payments to Payees, your Payees generally will not receive payment on the Transaction Date. This applies regardless of whether the payment is a next-day payment, a future payment, or a recurring payment, as described below. Therefore, in order to provide sufficient time for payments to be received by your Payees, the Transaction Date should be at least five (5) days prior to the date your payment is due, excluding any applicable grace periods (the "Due Date"). It is helpful if you allow additional time for a payment to be completed the first time you send a payment to a Payee through Capital Express. This allows the Payee to adjust to the new form of payment. Payments must be scheduled by the normal cut-off time of 4:30 p.m. (Eastern Standard Time) on any business day in order for the payment to be initiated for that business day. Transfers between your accounts must be scheduled by the normal cut-off time of 4:30 p.m. (EST) on any business day in order for the transaction to be completed on that business day.

YOUR PAYEE LIST

You may include all utility companies, merchants, financial institutions, insurance companies, individuals, etc. whom you wish to pay through the Bill Payment service. Include a complete mailing address and telephone number for each and your account number with each Payee. We reserve the right to decline to make payments to any person and entity.

RECURRING PAYMENTS

Recurring payments are those made for the same amount and are made on a weekly, bi-monthly, monthly, or other regularly scheduled basis. Once started, recurring payments will be made automatically until you tell us to cancel the payment as provided below in Canceling Transactions.

OUR LIABILITY FOR FAILURE TO COMPLETE TRANSACTIONS

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, we may be liable for some of your losses or damages. However, we will not be liable: or

a. if, through no fault of ours, you do not have enough money in your Account to make the transfer; or
b. if the money in your Account is subject to a dispute, legal process or other encumbrance restricting transfer; or
c. if the transfer would go over the credit limit on your overdraft line (if any); or
d. if the automated teller machine or the merchant where you are making the transfer does not have enough cash; or
e. if the Service was not working properly when you started the transfer; or
f. if circumstances beyond our control (such as fire, flood, systems failure or an Act of God) prevent the transfer, despite reasonable precautions that we have taken, or
g. if the Payee mishandles or delays handling payments sent by us.

CANCELING TRANSFERS & PAYMENTS

You may cancel a transfer between your accounts or a payment to a Payee up to 11:30 a.m. (EST) on the Transaction Date by calling customer service at 301-468-8848. A payment that has been sent may be recalled for a fee of $30 per item. The Bank does not guarantee the ability to recall an item even if you meet the time deadline. If you are canceling a recurring payment using the Bill Payment service, all future receiving payments to that Payee will cease unless you specifically instruct The Bank to continue future recurring payments.

STATEMENTS

All payments, transfers, and/or fees made with Capital Express will appear on your monthly Account statement. The Payee name, payment amount, and date of the payment will be shown for each payment made through Capital Express during that statement cycle.

FEES

Fees for Capital Express shall be payable in accordance with a schedule of charges as established and amended by The Bank from time to time. Charges shall be automatically deducted from your account, and The Bank shall provide you with monthly notice of such debit(s) on your statement.

BUSINESS DAYS/HOURS OF OPERATION

Our business hours are 9:00 a.m. to 5:00 p.m. (EST), Monday through Friday, except bank holidays. Our branch hours are from 9:00 a.m. to 3:00 p.m. Monday through Thursday, 9:00 a.m. to 5:00 p.m. on Friday. Although payments and transfers can be completed only on business days, Capital Express is available 24 hours a day, seven days a week, except during maintenance periods, for the scheduling of payment orders and transfers.

AUTHORIZATION TO OBTAIN INFORMATION

You agree that we may obtain and review your credit report from a credit bureau or similar entity. You also agree that we may obtain information regarding your account with any Payee in order to facilitate proper handling and crediting of your payments.

TERMINATION

If you want to terminate your access to Capital Express, call us at (301) 468-8848. After receipt of your call, we will send a written termination authorization for your signature and return to us. Upon receipt by Capital Bank of the authorization to terminate Capital Express signed by you, we will terminate Capital Express. In order to avoid imposition of the next monthly fee, we must receive your written authorization to terminate three (3) days before your service charge is scheduled to assess. RECURRING TRANSFERS BETWEEN ACCOUNTS WILL NOT NECESSARILY BE DISCONTINUED BECAUSE YOU TERMINATE ACCESS TO THE SERVICE. IF YOU WANT TO TERMINATE RECURRING TRANSFERS BETWEEN ACCOUNTS YOU MUST SPECIFICALLY STATE ON THE TERMINATION AUTHORIZATION THAT YOU WANT ALL RECURRING TRANSFERS TO CEASE.

We reserve the right to terminate Capital Express, in whole or in part, at any time with or without cause and without prior written notice. In the event that you give us a termination notice, we may (but are not obligated to) immediately discontinue making previously authorized transfers, including recurring transfers and other transfers that were previously authorized but not yet made. We also reserve the right to temporarily suspend Capital Express in situations deemed appropriate by us, in our sole and absolute discretion, including when we believe a breach of system security has occurred or is being attempted. We may consider repeated incorrect attempts to enter your password as an indication of an attempted security breach. Termination of Capital Express does not affect your obligations under this Agreement with respect to occurrences before termination.

WAIVERS

No waiver of the terms of this Agreement will be effective unless in writing and signed by an authorized officer of The Bank.

ASSIGNMENT

You may not transfer or assign your rights or duties under this Agreement.

GOVERNING LAW

The laws of the state of Maryland shall govern this Agreement and all transactions hereunder. You acknowledge that you have reviewed this Agreement, understand the terms and conditions set forth herein, and agree to be bound hereby.

AMENDMENTS

We can change a term or condition of this Agreement by mailing or delivering to you a written notice at least thirty (30) days before the effective date of any such change. We do not need to provide you with any prior notice where an immediate change in the terms or conditions of this Agreement is necessary to maintain or restore the security of our Service or an account. However, even in these cases, if the change is to be made permanent, we will provide you with a notice of the change with the next regularly scheduled periodic statement we send you if practicable, or within thirty (30) days, unless disclosure would jeopardize the security of our Service or an account. Notices mailed or delivered to you under this paragraph will be considered effective if mailed to the most recent address we show for you in the Account records, or the e-mail address which you authorized to receive such notices and/or disclosures.

PLEASE READ THIS AGREEMENT CAREFULLY AND PRINT A COPY FOR YOUR RECORDS.

YOUR USE OF THE BANK'S CAPITAL EXPRESS ONLINE BANKING SERVICES INDICATES YOUR AGREEMENT TO ALL TERMS, CONDITIONS, LIABILITIES AND WARRANTIES AS HEREIN DESCRIBED.