CAPITAL EXPRESS ONLINE BANKING AND CHECKFREE BILL PAY
POLICY AND AGREEMENT FOR BUSINESS ACCOUNTS

THE CAPITAL EXPRESS SERVICE

In consideration of the use of the Capital Express Internet Banking 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 you may use your PC for Bill Payments ("Bill Payments") from your account to third parties ("Payees") that you designate. You may make payments through the use of the Bill Payment service to any business, professional, merchant, family member, or friend. The "Account" or "Billing Account" means your designated Bill Payment account at Capital Bank from which Bill Payments or transfers on your behalf pursuant to this Agreement.

SERVICE DEFINITIONS

"Agreement" means these Terms and Conditions of the Online Banking, Bill Delivery and Payment Service. "Bill Payment" is a payment that is initiated by you through the Service to a Payee. "Billing Account" is the checking account from which all Service fees will be automatically debited. "Business Day" is every Monday through Friday, excluding Federal Reserve holidays. "Due Date" is the date reflected on your Payee statement for which the Bill Payment is due; it is not the late date or grace period. "Payee" is the entity to which you wish a payment to be directed through the Service. "Payment Account" is the checking account or credit card account from which payments will be debited. "Payment Instruction" is the information provided by you to the Service for a payment to be made to the Payee (such as, but not limited to, Payee name, Payee account number, and Scheduled Payment Date). "Scheduled Payment" is a Bill Payment that has been scheduled through the Service but has not begun processing. "Scheduled Payment Date" is the day you want your Payee to receive your Bill Payment and is also the day your Payment Account will be debited (except for credit card payments, which are charged to your Payment Account two (2) Business Days prior to the Scheduled Payment Date); if the Scheduled Payment Date falls on a non-Business Day, the Scheduled Payment Date will be considered to be the previous Business Day. "Service" means the Bill Delivery and Payment Service offered by or through CHECKFREE CORPORATION and its subsidiaries ("CHECKFREE"). "We," "us," and "our" refer to the Service. "You" and "your" refer to the individual that is accepting the payment service from the Service. An "Authorized User" is any individual which you allow to use the Service or your password or other means to access your account.

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 AND PROFILE 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 personally identifying 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.

ONLINE BILL PAY PROFILE INFORMATION

Information included in your Service profile, as identified in the application, including, but not limited to, your user name, password, and Payment Account data, is used as part of the Service with participating billers that offer their own biller direct sites through CHECKFREE. You will be able to use your same profile data (such as user name and password) to sign-in to such participating biller direct sites. Your Payment Account information will also be available to make payments to such participating billers.

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

b) The Bank limits employee access to confidential customer financial information to those who have a business reason for knowing the information

c) Bank employees are trained to understand the importance of customer financial privacy and to properly handle confidential information

d) The Bank endeavors to maintain the most accurate and up-to-date customer records possible

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, FiServ., who employs state of the art Internet firewall and network security technologies.

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

- **Access IDs and Passwords**
  Access to the Capital Express system and your accounts requires your valid User Code/Access ID and separate Password that you may change any time.
- **Strong Passwords**
  Your password is case sensitive. It must be at least 8 characters long and no more than 17 characters. There must be at least 1 number (1,2,3, etc.) , 1 letter (a,b,c, etc.) and one symbol (!,@,#,$, etc.).
- **Automatic Time Out**
  Capital Express system will automatically log you out of your session after 6 minutes of non-use (in case you forgot) and to prevent unauthorized access.
- **Security Enhancements**
  The Capital Express system is constantly monitored and evaluated. The system is tested regularly to detect any potential problems that might compromise security or privacy. Security technologies are always being evaluated, and the system 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 Factor Authentication ("MFA")**
  Multi Factor Authentication or MFA is a security feature which functions through several methods to authenticate the rightful account user before access to account-sensitive information is achieved. Three major factors include verification by something a user knows (such as a password), something the user has (such as a smart card or a security token), and something the user is (such as the use of biometrics or security questions). Due to their increased complexity, authentication systems using a multi-factor configuration are harder to compromise than ones using a single factors.

YOUR RESPONSIBILITY TO SECURITY

- The security of your accounts and personal information accessible through the Capital Express system 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 your interest and the interests of the system at large. Among the precautions you should take to help protect your accounts and information on the Capital Express system are:
- Do not share your Access ID or Password with anyone.
- You can change your Password as often as you like online, and we encourage you to do so regularly.
- Do not use birthdays, phone numbers or names that others can guess.
- No Capital Bank employee will ever need to know your Password for any reason. Do not disclose your password to any Bank employee or otherwise.
- You should log off from Capital Express as soon as you finish your Internet banking transactions.
- Never walk away from your computer with account information still visible on the screen.
- It is best to close your browser after signing off to clear account information from your browser's memory.
- Promptly notify the Bank if you suspect that unauthorized access or transactions have taken place on your accounts.

When you enroll for Capital Express with Capital Bank and use the system, you agree to the terms and conditions explained in all the Agreements & 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 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.

CHECKFREE ONLINE BILL PAY RESPONSIBILITIES

You are responsible for all payments you authorize using the Service. If you permit Authorized Users or other persons to use the Service or your password or other means to access your account, you are responsible for any transactions they authorize. If you believe that your password or other means to access your account has been lost or stolen or that someone may attempt to use the Service without your consent or has transferred money without your permission, you must notify the Bank immediately.

HOW OUR SYSTEM SECURITY WORKS

To understand how the system protects your customer data, you must first understand how a hacker will try to steal it. A thief will try to fraudulently access data in many ways. Two of the most frequent are:

- Illicit access to data in transit.
- Illicit access to stored data.

Data in transit protection. Data is in transit both when it is being acquired by the system (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 system Data Server 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). Then, when the Bank transmits the data, it is encrypted and protected from unauthorized access. To prevent unauthorized access during customer end user account queries, we use a Secure Socket Layer (SSL). SSL is 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.

Stored data protection. 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, FiServ, 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 system goes through the firewall.

Internet Banking System: FiServ 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 a User Code/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-Factor Authentication which prompts for your answers to security phrases established by you. Your entry into the system may also require a token. Tokens are provided to account holders 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.

Funds 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.

Audit Trail: 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 onFiServ servers, operated and monitored by FiServ 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.

Redundancy: Full redundancy is provided for housing of data and the transmission and communication of data.

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: FiServ maintains 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: Capital Bank and Fiserv 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 and applications such as HTTP (the Web protocol), FTP, Gopher, etc. The SSL protocol establishes an encryption key between the client (the web browser) and the server (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 areaall data transmitted and received is protected.

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 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 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.

ERRORS AND COMPLAINTS

You should 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.

You must contact us if you believe information in your statement or on your receipt is incorrect, 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); and

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.

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

Capital Bank,
Operations Department
2275 Research Blvd., Suite 600
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. You may also use the Bank's secure email service, a link to this can be found on the Bank's website.

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 Consumer Complaints Policy. Breaches of customer privacy are considered serious employee misconduct and may result in termination of the employee.

CHECKFREE ONLINE BILL PAYMENT: FAILED OR RETURNED TRANSACTIONS/SCHEDULING/CANCELLATION AND STOP PAYMENT/ DELIVERY AND PRESENTMENT

PLEASE REFER TO THE TERMS AND CONDITIONS OF THE BILL PAYMENT SERVICE FOR THESE AND OTHER DETAILS RELATED TO CHECKFREE ONLINE BILL PAYMENT

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.

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 Web site 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.

LIMITATION OF LIABILITY

Except as otherwise provided in this Agreement or by law, we are not liable for any loss, injury, or damage, whether direct, indirect, special, incidental or consequential, caused by Capital Express or the use thereof or arising in any way out of the use of Capital Express, including but not limited to any damage to your equipment.

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 system 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 system 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.

INDEMNIFICATION

In consideration of being allowed access to Capital Express, you agree to indemnify and hold the Bank harmless for any losses or damages to the Bank resulting from your use or any user authorized by you of the Capital Express product, to the fullest extent allowed by applicable law.