| Port # | Account Name | Date Activated | Employee Responsibility | Primary Account # |
|---|---|---|---|---|
| | | | | |

# *e*CHIEF Internet Banking with eStatements

Clear All Fields

## APPLICATION AND FUNDS TRANSFER AUTHORIZATION

Yes! I/we want the ease and convenience of eCHIEF Internet Banking. Please sign me up for eCHIEF. I/we have received and read a copy of the eCHIEF agreement and disclosure and I/we agree to the terms contained therein.

Business Name (if applicable)

Address

City State Zip

EIN Phone

Refer to the eStatement section of the eCHIEF agreement and disclosure for details on eStatements. I/We would like to receive eStatements (check one)

☐ For all accounts

☐ For some accounts. (detail below)

| | | |
|---|---|---|
| | | |
| | | |

### Applicant Information

Applicant Name:

Social Security #:

Birthdate:

E-Mail Address:

Primary Phone #:

**Username:** Your temporary Username will be the first 3 letters of your first name + the first 3 letters of your last name. (ex. John Doe's username will be "johdoe")

**Signature:**

### Business Use Only Complete for each Applicant

☐ Allow Option of Bill Pay Enrollment

By checking "Allow Option of Bill Pay Enrollment" above, authorized signers agree to allow Bill Pay on the eCHIEF account without two signatures required for making payments.

☐ View Only Access

Applicant Name:

Social Security #:

Birthdate:

E-Mail Address:

Primary Phone #:

**Username:** Your temporary Username will be the first 3 letters of your first name + the first 3 letters of your last name. (ex. John Doe's username will be "johdoe")

**Signature:**

☐ Allow Option of Bill Pay Enrollment

By checking "Allow Option of Bill Pay Enrollment" above, authorized signers agree to allow Bill Pay on the eCHIEF account without two signatures required for making payments.

☐ View Only Access

## Business Use Only

**BUSINESS ACCOUNTS:** By signing below, authorized signers defined in the business resolution agree to grant eCHIEF access to all above applicants. By checking "Allow Option of Bill Pay Enrollment" above next to one or more applicants, authorized signers agree to allow Bill Pay on the eCHIEF account without two signatures required for making payments.

**Authorized Signature:** **Authorized Signature:**

**Date:** **Date:**

# eCHIEF Online (Internet) Banking Agreement

1. The service. In consideration of the eCHIEF Online (Internet) Banking Service ("Service") to be provided by Blackhawk Bank & Trust ("BANK"), as described from time to time in information distributed by BANK to its customers. In the agreement, "Customer" refers to the person(s) [or person(s) authorized by the corporate entity] subscribing to or using the service. The Customer agrees as follows: The Customer may use a Personal Computer ("PC") or mobile device through an Internet connection to obtain account balances transaction information and to transfer money between accounts. The Customer may also use a PC to obtain account statements. Transfers from Money Market accounts are considered pre-authorized transfers, and pre-authorized transfers are limited to six (6) per monthly statement cycle by federal regulations.

   PLEASE READ THIS AGREEMENT CAREFULLY & KEEP A COPY FOR YOUR RECORDS.

2. Your Unique Username & Password. Each Customer who has access to the Service, including each individual named on joint accounts or authorized by the corporate entity subscribing to use the Service, must designate a Username and Password. Your Password must be between eight (8) and twelve (12) characters long with at least four of those characters being letters and at least two of those characters being numbers. Letters are case sensitive and can be in either uppercase, lowercase, or a combination of the two. (For example: MyBank1243 would be acceptable. Bank4 would not be acceptable.) Your Username must be between six (6) and nineteen (19) characters. Letters are case sensitive and can be in either uppercase, lowercase, or a combination of the two.

3. Fees. Fees associated with specific features within the Service shall be payable in accordance with a schedule of charges as established and amended by BANK from time to time. Applicable charges shall be automatically deducted from Customer's account, and BANK shall provide Customer with a monthly notice of such debit(s) on said account.

4. Equipment/Minimum System Requirements. Customer is solely responsible for the equipment (including your personal computer, laptop, or mobile device and software) used to access the Service. BANK is not responsible for errors or delays or Customer's inability to access the Service caused by Customers' equipment or lack thereof. BANK is not responsible for the cost of upgrading Customer's equipment to stay current with the Service nor is BANK responsible, under any circumstances, for any damage to Customer's equipment or the data resident thereon as a result of accessing or utilizing the Service.
   To use eCHIEF, you will need to have access to a PC or tablet with Internet browser access. The computer operating systems and web browsers certified to access and navigate the Service are continually changing as operating system and web browser updates are introduced. While BANK recommends a Windows Vista, Windows 7, Windows 8, Windows 10, MAC OSX 10.4 or MAC OSX 10.5 operating system, understand that over time, new operating systems will become certified and old systems may no longer be certified. This same idea applies to web browsers. BANK recommends using Internet Explorer 9 or higher with at least the latest industry standard encryption. Internet Explorer 8 is no longer supported. You may also choose to use Safari, Firefox, or Chrome browsers. BANK recommends using the latest versions of these browsers and which support the latest industry standard encryption. Over time certified browsers may change. New browsers will become certified and old browsers may no longer be certified.

   ***How to check what version of browser is being used:***

   1) Microsoft Internet Explorer: on toolbar, click "Help" then "About Internet Explorer". Note: if there is not a toolbar across the top, you may have to press the "Alt" key.

   2) Mozilla Firefox: Select "Help" then "About Mozilla Firefox". *Cookies:* While cookies are not required to use Internet Banking, if cookies are not enabled on the browser, challenge questions may be asked every time you log in to Internet Banking from that computer.

   Enabling Cookies: You may prefer to keep your cookies disabled for privacy reasons. Internet Explorer and Firefox allow you to explicitly define websites for which cookies are allowed.

   ***PassMark Authentication and Cookies:***

   1) For Personal/Home Computers: if cookies are enabled, security questions may be asked if it is the first time logging in with that PC /Browser or if cookies were recently cleared. Select "Don't challenge me again on this device." This will store a cookie on the computer then you will not be asked a challenge question next time you log in from that computer.

   2) For Public (non personal) Computers: Do not select, "Don't challenge me again on this device." This method will not store a cookie on the computer, then you will be asked a challenge question each time you log in from that computer.

   Mobile Banking: Mobile Text does not require a smartphone, however, a phone with SMS text messaging capabilities is needed. The Mobile Web and Mobile App do require a smartphone for use of the service(s). When using the Mobile Banking service, please note that there is no charge from Blackhawk Bank & Trust, but message and data rates may apply. Such charges include those from your mobile service provider. Any time you review your balance, keep in mind it may not reflect all transactions such as checks you have written but have not yet been posted to your account. Adobe Acrobat Reader must be installed to view eStatements online. Customer agrees that BANK is not responsible for any electronic virus that he/she may encounter using the Service. It is recommended that you routinely scan your PC and software using any reliable virus protection product to detect and remove any electronic virus.

5. Business Days/Hours of Operation. For determining the availability of your deposits, every day is a business day, except for Saturdays, Sundays, and federal holidays. Our business hours are Monday through Thursday 8:00 a.m. to 4:00 p.m. (CDT), Friday 8:00 a.m. to 5:30 p.m. (CDT) and Saturday 8:00 a.m. to 12:00 p.m. (CDT). eCHIEF Internet Banking transactions or transfers including loan payments performed after 6:00 p.m. (CDT) will be processed effective the following business day. Again, all transactions and transfers must be scheduled by 6:00 p.m. (CDT) on any business day in order for the transaction or transfer to be completed on that business day. The Service is available 24 hours a day, seven days a week, except during maintenance periods, for transactions and the scheduling of transfers.

6. Our Liability for Failure to Complete Transactions. If BANK does not complete a transfer to or from a Customer's account on time or in the correct amount according to our account agreement, BANK will be held liable for Customer's losses or damages. However, there are some exceptions. BANK will not be liable, for instance:

   - if, through no fault of BANK, Customer does not have enough money in his/her/their account to make the transfer;
   - if the money in Customer's account is subject to legal process or other encumbrances restricting transfer;
   - if the transfer would exceed the credit limit on Customer's overdraft line (if any);
   - if the Service was not working properly when Customer started the transfer;
   - if circumstances beyond our control (such as fire or flood) prevent the transfer, despite reasonable precautions that BANK has taken.

   **Stop Payment.** If Customer requests BANK to stop payment on any item, BANK must be furnished with the items exact amount, date, number, name of payee, plus any other information BANK may request. Failure to provide BANK with the same shall relieve BANK of any liability in the transaction. Customer agrees to reimburse BANK for any expense or losses that might occur therein. There may be other exceptions stated in our account agreement with Customer.

7. Statements. All transactions and/or transfers made with the Service will appear on Customer's monthly account statement.

8. Notice of Customer Rights & Liabilities. Security of Customer transactions and transfers is important to BANK. Therefore, use of the Service will require a Username and Password for access. If Customer loses or forgets his/her/their Username or Password, please call (309) 787-9575 during the normal business hours listed above, leave a voice mail message after hours,

or reset your password online at www.ChoosetheChief.com. If Customer loses a mobile device used to access the Service, please notify BANK immediately so that mobile access can be turned off. Customer may also disable mobile device access by logging into the Service and disabling mobile banking under "Profile". BANK may accept as authentic any instructions given to it through the use of Customer's Username or Password. Customer agrees to keep his/her/their Username and Password secret and will notify BANK immediately if said Username or Password is lost, stolen, or if Customer believes that someone else has discovered said Username or Password. Customer agrees that if his/her/their Username or Password is given to someone else, Customer is authorizing that individual or entity to act on Customer's behalf, and BANK may accept any instructions given to it to make transactions, transfers or otherwise use the Service. The Service enables Customer the ability to change his/her/their Password; BANK requires that Customer perform this task regularly, at least once per calendar year. BANK may be liable for certain security breaches to the extent required by applicable law and regulation. BANK will not assume any other liability or otherwise guarantee the security of the information in transit to or from our facilities and/or equipment. Please note that BANK reserves the right to (1) monitor and/or record all communications and activity related to the service and (2) requires verification of all requested transfers in the manner BANK deems appropriate before making the transfer (which may include written verification by the Customer). Customer agrees that BANK records will be final and conclusive as to any and all questions concerning whether or not Customer's Username and Password was used in connection with a particular transaction or transfer. If any unauthorized use of Customer's Username or Password occurs, Customer agrees to (1) cooperate with BANK and the appropriate law enforcement authorities in identifying and prosecuting the perpetrator; and (2) provide reasonable assistance requested by BANK in recovering any unauthorized transaction and/or transfer. Customer agrees to tell BANK at once if Customer believes his/her/their Username or Password has been lost, stolen or otherwise compromised. Telephoning is the best way of keeping your exposure and potential losses down. If Customer fails to communicate to BANK that his/her/their Username or Password has been lost, stolen or otherwise compromised, Customer could lose all the money in his/her/their account plus Customer's maximum line of credit. If Customer notifies BANK within two (2) business days, Customer can lose no more than $50. If Customer DOES NOT tell BANK within two (2) business days after Customer learns of the loss, theft or compromise of said Username or Password, and BANK can prove that it could have stopped someone from using Customer's Username or Password without Customer's permission if he/she/they had told BANK, Customer could lose as much as $500. Also, if Customer's monthly account statement shows transactions and/or transfers that Customer did not make, Customer should tell BANK at once. If Customer does not tell BANK within sixty (60) days after the FIRST monthly account statement on which the problem or error appeared was mailed to Customer, Customer may not get back any money he/she/they lost after the sixty (60) days if BANK can prove that BANK could have prevented someone from taking the money from Customer if Customer had told BANK in time. If Customer believes that his/her/their Username or Password has been lost, stolen or otherwise compromised, or that someone has transferred or may transfer money from Customer's account without Customer's permission, call (309) 787-9575 during the normal business hours listed below in section 9. BANK CANNOT AND WILL NOT ACCEPT NOTIFICATION OF LOST OR STOLEN USERNAMES, PASSWORDS OR UNAUTHORIZED TRANSFERS VIA EMAIL.

9. Errors & Questions. In case of errors and/or questions about Customer's electronic transactions, telephone BANK at (309) 787-9575 Monday through Thursday 8:00 a.m. to 4:00 p.m. (CDT), Friday 8:00 a.m. to 5:30 p.m. (CDT) and Saturday 8:00 a.m. to 12:00 p.m. (CDT). Customer may also contact BANK by mail at the following address:

**Blackhawk Bank & Trust**
**ATTN: eBanking Department**
**P.O. Box 1100, Milan, IL 61264-1100**

If Customer thinks his/her/their statement or receipt is wrong or if Customer needs more information about a transaction listed on his/her/their statement or a receipt, contact BANK immediately. BANK must hear from Customer no later than sixty (60) days after BANK sent Customer the FIRST statement on which the problem or error appeared. Customer will need to provide BANK with the following information:

- Customer Name and Account Number (if any);
- Describe the error or transaction in question, and explain as clearly as possible why Customer believes it is an error or Customer needs more information;
- The dollar amount of the suspected error.

If Customer chooses to tell BANK verbally, BANK may require Customer to send Customer's complaint or question in writing within ten (10) business days. This notification period will be extended to twenty (20) business days if the notice or error involves an electronic funds transfer to or from the account within thirty (30) days after the first deposit to the account was made. BANK will correct any error promptly.
However, if BANK needs more time to investigate the matter, BANK may take up to forty-five (45) days to investigate your complaint or question. If we decide to do this, BANK will credit Customer's account within ten (10) business days (twenty (20) business days if the notice or error involves an electronic funds transfer to or from the account within thirty (30) days after the first deposit to the account was made) for the entire amount Customer thinks is in error, so that Customer may have use of the money during the time it takes BANK to complete its investigation. If BANK asks Customer to put his/her/their complaint or question in writing and BANK does not receive it within ten (10) business days, BANK may not credit Customer's account. If BANK determines there was no error, BANK will reverse the previously credited amount, if any, and BANK will send Customer a written explanation within three (3) business days after BANK finishes its investigation. Customer may ask for copies of the documents BANK used in its investigation.

10. Disclosure of Account Information to Third Parties - Privacy Disclosure. BANK collects information Customer might consider to be private, such as account number(s), social security number, assets, income, and debt (non-public personal information) about Customer from the following sources: Information BANK receives from Customer on applications or other forms; Information about Customer transactions with BANK, our affiliates or others; and Information BANK receives from a consumer reporting agency. BANK may disclose all of the information it collects, as described above, to companies that perform marketing services on BANK's behalf or to other financial institutions with whom BANK has joint marketing agreements. Since BANK values its relationship with Customer, BANK will not disclose Customer's personal and account information to any third parties, except as permitted by law such as to report credit bureaus, IRS Reporting, responses to subpoenas, search warrants, or summons. BANK restricts access to Customer's personal and account information to those employees who need to know that information to provide products or services to Customer. BANK maintains physical, electronic and procedural safeguards that comply with federal standards to guard Customer's non-public personal information. Maintaining the security and confidentiality of information BANK maintains about Customer is a top priority for BANK. BANK carefully manages Customer's information within BANK in order to give Customer better service, greater convenience, and additional benefits consistent with the nature of Customer's overall business with BANK. If Customer decides to close his/her/their account(s) or become an inactive Customer, BANK will follow the privacy policies and practices as described in this notice. BANK may also disclose information to third parties about Customer's account or the transactions Customer makes:

- where it is necessary for completing transactions or resolving errors involving the Service;
- in order to verify the existence and condition of Customer's account for a third party, such as a credit bureau or a merchant; or
- in order to comply with government agency rules, court orders, or other applicable law; or
- to our employees, service providers/vendors, auditors, collection agents, affiliated companies, or attorneys in the course of their duties and to the extent allowed by law; or
- if Customer give us his/her/their permission.

11. Authorization to Obtain Information. Customer agrees that BANK may obtain and review Customer's credit report from a credit bureau or similar agency. If applicable, Customer also agrees that BANK may obtain information regarding Customer's Payee Accounts in order to facilitate proper handling and crediting of Customer's payments. BANK reserves the right to periodically monitor Customer's account(s) and online activity for legitimacy and accuracy.

12. Termination. If Customer wants to terminate his/her/their access to the Service, call BANK at (309) 787-9575. After receipt of Customer's call, BANK will send a written termination authorization form for Customer's signature and ask Customer to return the form to BANK. If applicable, in order to avoid imposition of the next monthly statement fee for the Service, BANK must receive Customer's written termination authorization three (3) business days before Customer's service charge is scheduled to be assessed. RECURRING TRANSFERS WILL NOT NECESSARILY BE DISCONTINUED BECAUSE CUSTOMER TERMINATES ACCESS TO THE SERVICES. IF CUSTOMER WANTS TO MAKE CERTAIN THAT RECURRING TRANSFERS BETWEEN ACCOUNTS ARE STOPPED, CUSTOMER MUST FOLLOW THE PROCEDURES IN CANCELING HIS/HER/THEIR ACCOUNT AS INDICATED ABOVE. BANK reserves the right to terminate the Service, in whole or in part, at any time, with or without cause and without prior written notice. In that event, or in the event that Customer provides a written termination notice, BANK may (but is not obligated to) immediately discontinue making previously authorized transfers, including recurring transfers and other transfers that were previously authorized and scheduled but not yet made. BANK also reserves the right to temporarily suspend the Service in situations deemed appropriate by it, in its sole and absolute discretion, including when BANK believes a breach of system security has occurred or is being attempted. BANK may consider repeated incorrect attempts to enter Customer's Username or Password as an indication of an attempted security breach. Termination will also occur automatically when a customer does not successfully log

into the Service for 120 days. In the event that this occurs, customer will be required to re-enroll. Termination of the Service does not affect Customer's obligations under this Agreement with respect to occurrences before termination occurs.

13. Limitation of Liability. Except as otherwise provided in this Agreement or by law, BANK is not responsible for any loss, injury or damage, whether direct, indirect, special or consequential, caused by the Service or the use thereof or arising in any way out of the installation, operation or maintenance of Customer's PC equipment.

14. Waivers. No waiver of the terms of this Agreement will be effective, unless in writing and signed by an authorized officer of BANK.

15. Assignment. Customer may not transfer or assign his/her/their rights or duties under this Agreement.

16. Governing Law. The laws of the state of Illinois shall govern this Agreement and all transactions hereunder. Customer acknowledges that prior to usage, he/she/they has/have received and reviewed this Customer Agreement, understands the terms and conditions set forth herein, and agrees to be bound hereby.

17. Amendments. BANK can change a term or condition of this Agreement by mailing or delivering to Customer a written notice at least thirty (30) days before the effective date of any such change. BANK does not need to provide Customer with any prior notice where an immediate change in the terms and conditions of this Agreement is necessary to maintain or restore the security of the Service or an account. However, even in these cases, if the change is to be made permanent, BANK will provide the Customer with a notice of the change with his/her/their next regularly scheduled periodic statement, or within thirty (30) days, unless disclosure would jeopardize the security of the Service or an account. Notice mailed or delivered to Customer under this paragraph will be considered effective if mailed to Customer to the most recent address BANK shows for Customer in either our Checking or Savings Account records, or if the notice is sent to the email address Customer provided and authorized BANK to deliver such notices and/or disclosures to.

18. Indemnification. Customer, in consideration of being allowed access to the Service, agrees to indemnify and hold BANK harmless for any losses or damages to the BANK resulting from the use of the Service, to the extent allowed by applicable law.

19. Security Procedures. By accessing the Service, Customer hereby acknowledges that he/she/they will be entering a web site owned by BANK and accessing account information on a secure server owned by and located at Fiserv, Inc. Customer acknowledges that access to either of the aforementioned entities will be for authorized purposes only. BANK may periodically monitor and audit usage of the Service, and all persons are hereby notified that use of the Service constitutes consent to such monitoring and auditing. Unauthorized attempts to up-load, download, and/or change information on the aforementioned websites are strictly prohibited and are subject to criminal prosecution under the Computer Fraud and Abuse Act of 1986. If applicable, violators will be prosecuted to the fullest extent of the law. There are several levels and layers of security within the BANK framework. User levels deal with cryptology and Secure Sockets Layer (SSL) protocol and are the first line of defense used by all Customers accessing the Service from the Internet. Server Level focuses on firewalls, filtering routers and BANK's trusted operating system. Host Level deals specifically with BANK's Service and the processing of Customer's secure financial transactions and transfers. User Level deals with the Customer and his/her/their PC equipment, browser, Username, correct Security Question Response (or registered cookie), and Password used to access the Service. When a secure connection has been established between the Customer and the BANK server, Customer must provide a valid Username and Password to gain access to the Service. This information is encrypted, logged by the server forming another complete physical security layer to protect the server's information and a request to log on to the Service is processed. Although SSL utilizes proven cryptography techniques, it is important for Customer to protect his/her/their Username and Password from others. Session time-outs and a limit on the number of logon attempts are examples of other security measures BANK has in place to ensure that inappropriate activity is prohibited at the User Level. All transactions sent to the BANK server must first pass through a filtering router system. These filtering routers automatically direct the request to the appropriate server after ensuring that the access type is through a secure browser and nothing else. The routers verify the source and destination of each network packet and manage the authorization process of letting packets through. The filtering routers also prohibit all other types of Internet access methods at this point. This process blocks all non-secured activity and defends against inappropriate access to the server. The server used for the Service is protected using the latest in firewall protection. This platform defends against system intrusions and effectively isolates all but approved customer financial transactions, transfers, and requests. The platform secures the hardware running the Service and prevents associated attacks against all systems connected to the server. The server and the applicable mechanics of the Service are monitored 24 hours a day, seven days a week for a wide range of anomalies to determine if attempts are being made to breach the security framework. While BANK's service provider (Fiserv, Inc.) continues to evaluate and implement the latest improvements in Internet security technology, the Customer also has the responsibility for the security of his/her/their personal information and should always follow the recommendations listed below:

    • Utilize the latest industry standard encryption web browser on your computer. It is also recommended that your computer have an anti-virus program in place with current virus definitions.
    • Customer's Username and Password must be kept confidential. Customer is encouraged to change their Password frequently so that the information cannot be compromised, guessed or used by others. Customer should be certain that others are not watching Customer enter this information on the keyboard when Customer is accessing the Service.
    • Customer should NEVER leave his/her/their computer unattended while logged on to the Service. Others may approach Customer's computer and gain access to Customer's account information if Customer walks away.
    • Customer should click "Log Out" when finished using the Service to properly end his/her/their session. Once a session has been ended, no account information can be displayed or further transactions or transfers processed until Customer logs on to the Service again.
    • Customer should close his/her/their browser when finished using the Service so that others cannot view any account information displayed on his/her/their computer. When Customer follows these simple security measures, his/her/their interaction with the Service will be confidential and secure.
    • Customer using mobile devices such as mobile phones and tablets should enable security controls such as password protection, device encryption, remote find and wipe, and mobile antivirus protection.
    • If Customer loses a mobile device used to access the Service, please notify BANK immediately so that mobile access can be turned off. Customer may also disable mobile device access by logging into the Service and disabling mobile banking under "Profile."
    • Customer should not expose his/herself to mobile device vulnerabilities by rooting or jailbreaking his/her phone or tablet. In the event that your device is in this condition, it is highly recommended that Customer restore the device security by upgrading the device operating system with the latest security patches prior to accessing the Service on this device.
    • Customer using mobile devices to access the Service should be cautious to only connect to trusted WiFi hotspots.

20. Electronic Messages & Notices. Customer should send BANK inquiries concerning System maintenance and other issues via our email address: ebanking@choosethechief.com. Customer acknowledges that this email address is not located on a secured, encrypted server so the information Customer enters could be intercepted and viewed by others. Customer should never use regular email to initiate any banking transactions. Electronic mail may be used to send Customer notices, disclosures and other information that is required under the Electronic Funds Transfer Act and Regulation E of the Federal Reserve Board of Governors. If Customer has provided BANK with an email address at the time of application for the Service, BANK is entitled to rely on that provided address and assume that messages sent to that address will be received by Customer, until Customer gives BANK notice in writing that the provided address is no longer valid. Customer is encouraged to save and/or print a copy of any notice sent to him/her/them by email for future reference.

21. Authorization to Charge Account(s). Customer is responsible for all transfers and transactions he/she/they or his/her/their authorized representative makes using the Service. By agreeing to these terms, Customer authorizes BANK to debit his/her/their designated account(s) for any transactions completed with the Service. Customer agrees that BANK may comply with transfer/transaction instructions entered by any one person using an authorized Username or Password regardless of the restrictions placed at the account level, i.e., "Two Signatures Required" or "Minor Account - No Withdrawals Allowed". If Customer permits another person to use the Service or give them his/her/their Username or Password, Customer is responsible for transactions, transfers and/or advances that any person makes from the accounts linked to Customer's application even if that person acts fraudulently, criminally or exceeds Customer's authorized withdrawal limits. It is Customer's responsibility to maintain current information on all of its accounts and to notify BANK immediately of any personnel changes regarding account access. Customer agrees to hold BANK or any of its agents harmless for any transactions performed in good faith by BANK with out-dated or incorrect Customer information.

22. Current Fee Schedule. eCHIEF Internet Banking Service Fee: The basic service is FREE. All other applicable fees are in accordance with BANK's Fee Schedule as published and distributed in conjunction with BANK's Account Terms & Conditions. I/We am/are the owner(s) of the following account number(s) to be included in the List of Accounts to be viewed

through the eCHIEF Internet Banking Service. Business accounts are subject to authorization as defined by the resolution. I/We understand that I/We am/are the only individual(s) authorized to use eCHIEF Internet Banking as it pertains to My/Our account(s) and that use of eCHIEF Internet Banking signifies My/Our agreement to the terms and conditions set forth in this eCHIEF Internet Banking Agreement which has been furnished to, received, and reviewed by Me/Us.

**eStatements & eNotices**

1. Availability. You may choose to receive your monthly statements of account electronically through eStatements rather than paper statements of account. The eStatements will be made available to you each month at the same time a paper statement would be available. An eStatement notification will be sent to your email account when notice is available online. Upon beginning eStatement services, we will discontinue sending your monthly statements via U.S. mail.

2. Paper Statements. If you choose to receive your eStatements electronically, you will no longer receive paper statements of account by mail.

3. Registration Process. The eStatements electronic statement service requires that you complete the initial registration process. The steps to register are as follows: Enroll within your eCHIEF Profile or fill out the eStatement Enrollment Form from the ChoosetheChief.com website. You may drop off the completed paper form to a Customer Service Representative at any branch or mail to:

**Blackhawk Bank & Trust**
**ATTN: eBanking Department**
**P.O. Box 1100, Milan, IL 61264-1100**

4. Email Address. We will send notification of your periodic account statement(s) to the email address provided by you. You agree to notify us promptly in writing by letter sent via U.S. Mail or through online banking under Profile if your email address changes. We will verify your identity against information you have provided previously. If you have not notified us in writing of any change to your email address, you agree that your failure to provide us with a good email address is the lack of ordinary care on your part. If we become aware that you are not receiving your eStatement(s) and notices, and our attempts to contact you have failed, we will send your statement(s) and notice(s) to you via U.S Mail to your last address known to us.

5. NOTICE OF UNAUTHORIZED ACCESS. If you believe that someone has obtained access to your eStatement file(s) without your permission, or if your password has been compromised, lost, or stolen, call us as soon as possible at (309) 787-9575.

6. PROMPT REVIEW OF eStatements. Our eStatements will be dated the day the eStatement is sent to you by email (the “email date”). You must promptly review your eStatements and any accompanying items and notify us in writing or via email at info@choosethechief.com within two (2) business days, of any error, unauthorized signature, lack of signatures, alterations, or other irregularities. Any applicable time periods within which you must notify us of any errors on your account statement(s) shall begin on the email date regardless of when you receive and/or open the eStatements. eStatements should be received within one (1) business day of your statement date. If you do not receive an expected emailed notification, immediately contact us at (309) 787-9575. Please do not send private, confidential or sensitive information via unsecured email.