1ST COMMUNITY BANK
24/7 ONLINE BANKING AGREEMENT AND DISCLOSURE

Requirement: You must have an account with 1st Community Bank to access 24/7 Online Banking.

Enrollment Instructions: If you are currently an accountholder with 1st Community Bank, we welcome you to enroll in 24/7 Online Banking. After filling in the First Time User Information, please review this 24/7 Online Banking Agreement and Disclosure and click on the "Accept" button at the bottom of this document. Your request will be forwarded to us and after a verification period we will contact you with enrollment information.

Preface: 1st Community Bank is pleased to offer you 24/7 Online Banking. Our internet banking product allows you to conduct your banking at your convenience from home, work, or wherever you may have access to the world-wide web. We are located on the world-wide web at www.1stcommunitybanks.com. 1st Community Bank's 24/7 Online Banking consists of an online banking website that provides a complete array of financial services to our customers.

1st Community Bank's 24/7 Online Banking system currently allows our customers to:

- View accounts (balances, transaction history, loan payment history, etc.)
- Schedule a one-time transfer between accounts
- Schedule a recurring transfer between accounts
- Make payment transfers to your 1st Community Bank loan accounts
- Print account transaction histories

****Important Note****
24/7 Online Banking transactions have a cut-off time of 6:00 pm CST. If you conduct an internet transaction before 6:00 pm CST on Monday through Friday on a business day that we are open, we will consider that day to be the day of your transaction. However, if you conduct a transaction after 6:00 pm CST on Monday through Friday or on a day we are not open, we will consider the transaction to be made on the next business day we are open.

1. Introduction

This 24/7 Online Banking Agreement and Disclosure governs your use of 24/7 Online Banking. Throughout this document, the Agreement and Disclosure will be referred to as "Agreement". By using 24/7 Online Banking, you agree to all of the terms of this Agreement. Please read it carefully and retain a copy for your records.

2. The Service

In consideration of the 24/7 Online Banking services ("Services") to be provided by 1st Community Bank ("Bank"), "Customer", "You", "Your", refers to the person(s) subscribing to or using the Service. "We", "Us", "Our", refers to 1st Community Bank and any agent, independent contractor, designee, or assignee 1st Community Bank may involve in the provision of 24/7 Online Banking. "Business Day" refers to any calendar day other Saturday, Sunday, or any holidays recognized by 1st Community Bank.

3. Privacy Policy

As a 1st Community Bank customer, you provide us with personal and financial information. We believe it is our responsibility to safeguard this important information. While some financial institutions share customer information with other businesses, 1st Community Bank is committed to keeping it confidential.

To ensure you the confidentiality you deserve, we have developed the following privacy policy. It is our pledge to you that we will adhere to these guidelines.

The Information That We Collect

We collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us or others; and
- Information from a consumer reporting agency.

Information We Disclose About You

We do NOT disclose any nonpublic personal information about you to anyone, except as permitted by law.

Nonpublic Personal Information and Former Customers

If you decide to close your account(s) or become an inactive customer, we will adhere to the privacy policies and practices as described in this notice.

The Confidentiality, Security, and Integrity of Your Nonpublic Personal Information

We restrict access to your personal and account information to those employees who need to know that information to provide products and services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

4. Your User Code and Password

Each individual who has access to 24/7 Online Banking, including each individual named on joint accounts, must designate a User Code and a Password. Your Password must be a minimum

of 8 characters. It must have at least 2 numeric characters and 2 alpha characters and it is case sensitive. For example, your Password may be Banker12. You will be given a temporary Password to access the system the first time. Upon logging in for the first time you will be prompted to change your Password immediately. You will be required to change your Password every 6 months. If you leave your 24/7 Online Banking session and do not log out manually, you will automatically be logged out after 10 minutes and will need to enter your User Code and Password again to regain access to the system. If there are 3 consecutive failed log-in attempts to 24/7 Online Banking, the user will be locked out of the system and will need to call 1st Community Bank to regain access to the system.

5. Internet Security

1st Community Bank is pleased to offer internet banking. Delivering these services requires a solid security framework that protects you and our institution's data from outside intrusion. We are committed to working with our internet service and communications providers to produce the safest operating environment possible for our customers. The information below summarizes our security framework which incorporates the latest proven technology. A section at the end also summarizes your responsibilities as a user of the internet banking system with regard to security. There are several levels of security within our security framework. User Level deals with cryptography and Secure Sockets Layer (SSL) protocol, and is the first line of defense used by all customers accessing our Banking Server from the public internet. Server Level focuses on firewalls, filtering routers, and our trusted operating system. Host Level deals specifically with our internet banking services and the processing of secure financial transactions.

User Level

There are several components of User Level security that ensure the confidentiality of information sent across the public internet. The first requires your use of a fully SSL-compliant 128 bit encrypted browser such as Microsoft Internet Explorer or Netscape Navigator. SSL is an open protocol that allows a user's browser to establish a secure channel for communicating with our internet server. SSL utilizes highly effective cryptography techniques between your browser and our server to ensure that the information being passed is authentic, cannot be deciphered, and has not been altered en route. SSL also utilizes a digitally signed certificate which ensures that you are truly communicating with the 24/7 Online Banking Server and not a third party trying to intercept the transaction.

After a secure connection has been established between your browser and our server, you then provide a valid User Code and Password to gain access to the services. 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 system is processed. Although SSL utilizes proven cryptography techniques, it is important to protect your User Code and Password from others. You must follow the Password parameters we specify at the time you sign up for 24/7 Online Banking. We also require changing your Password every 6 months. Session time-outs and a limit on the number of logon attempts are examples of other security measures in place to ensure that inappropriate activity is prohibited at the User Level.

Server Level

All transactions sent to our Banking Server must first pass through a filtering router system. These filtering routers automatically direct the request to the appropriate server after ensuring the access type is through a secured 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 Banking Server is protected using the latest firewall platform. This platform defends against system intrusions and effectively isolates all but approved customer financial requests. The platform secures the hardware running the online applications and prevents associated attacks against all systems connected to the Banking Server. The system is monitored 24 hours a day, seven days a week for a wide range of anomalies to determine if attempts are being made to breach our security framework.

Host Level

Once authenticated, the customer is allowed to process authorized internet banking transactions using host data. In addition, communication timeouts ensure that the request is received, processed, and delivered within a given timeframe. Any outside attempt to delay or alter the process will fail. Further password encryption techniques are implemented at the host level, as well as additional security logging and another complete physical security layer to protect the host information itself.

User Responsibilities

While our service provider continues to evaluate and implement the latest improvements in internet security technology, users of 24/7 Online Banking also have responsibility for the security of their information and should always follow the recommendations listed below:

- Utilize the latest 128 bit encryption version of either Microsoft Internet Explorer or Netscape Navigator. 24/7 Online Banking is best viewed and is most secure when you use one of these two browsers, as they are both certified for use at our site.
- Your Password must be kept confidential. You must follow our specific parameters for a Password and change it at least every 6 months to ensure that the information cannot be guessed or used by others. Be sure others are not watching you enter information on the keyboard when using the system.
- Never leave your computer unattended while logged on to 24/7 Online Banking. Others may approach your computer and gain access to your account information if you walk away.
- Click Exit when you are finished using the system to properly end your session. Once a session has been ended, no further transactions can be processed until you log on to the system again.
- Close your browser when you are finished so that others cannot view any account information displayed on your computer.
- Keep your computer free of viruses. Use virus protection software to routinely check for a virus on your computer. Never allow a virus to remain on your computer while accessing the 24/7 Online Banking system.
- Report all crimes to law enforcement officials immediately.

When you follow these simple security measures, your interaction with 24/7 Online Banking will be completely confidential. We look forward to serving your online banking needs both today and into the future – securely!

6. Equipment

You are solely responsible for the equipment (including, in the case of 24/7 Online Banking, your personal computer and software) you use to access the Services. We are not responsible for errors or delays or your inability to access the Services caused by your equipment. We are not responsible for the cost of upgrading your equipment to stay current with the Services nor are we responsible, under any circumstances, for any damage to your equipment or the data resident thereon.

7. Virus Protection

1st Community Bank is not responsible for any electronic virus or viruses that you may encounter. We encourage our customers to routinely scan their personal computer and diskettes using a reliable virus product to detect and remove any viruses. Undetected or unrepaired viruses may corrupt and destroy your programs, files, and even your hardware. Additionally, you may unintentionally transmit the virus to other computers.

8. Business Days/Hours of Operation

Our lobby hours are 9:00–4:00 pm Monday, Tuesday, and Thursday; Wednesday, 9:00-12:00 pm; Friday, 9:00-4:30 pm; and Saturday, 8:00-12:00 pm. Everyday is a business day, except for Saturdays, Sundays, and 1st Community Bank holidays. Our policy is to make funds available to you on the same day we receive your deposit/transfer. However, 24/7 Online Banking transactions have a cutoff time of 6:00 pm CST. If you conduct an internet transaction before 6:00 pm CST on Monday through Friday on a business day that we are open, we will consider that day to be the day of your transaction. However, if you conduct a transaction after 6:00 pm CST on Monday through Friday or on a day we are not open, we will consider the transaction to be made on the next business day we are open. You are free to schedule internet transfers/payments 24 hours a day, seven days a week with 24/7 Online Banking, except during maintenance periods.

9. Notice of Your Rights and Liabilities

Security of your transactions is important to us. Use of the Services therefore requires a Password. If you lose or forget your Password, please call 309-582-3531 or 309-593-2117 during normal business hours listed above. We may accept as authentic any instructions given to us through the use of your Password. You agree to keep your Password secret and to notify us

immediately if your Password is lost or stolen or if you believe someone else has discovered your Password. You agree that if you give your Password to someone else, you are authorizing them to act on your behalf, and we may accept any instructions they give us to make transfers or otherwise use the Services. 24/7 Online Banking enables you to change your Password and we require that you do so regularly. We may be liable for certain security breaches to the extent required by applicable law and regulation. We do not assume any other liability or otherwise guarantee the security of information in transit to or from our facilities. Please note that we reserve the right to (1) monitor and/or record all communications and activity related to the Services; 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 with us and appropriate law enforcement authorities in identifying and prosecuting the perpetrator; and (2) provide reasonable assistance requested by us in recovering any unauthorized transfer of funds.

Notify us immediately if you believe your Password has been lost or stolen. Telephoning is the best way to keep your possible losses down. You could lose all of the money in your account (plus your maximum line of credit). If you tell us within 2 business days you can lose no more than $50.00. If you do NOT tell us within 2 business days after you learn of the loss or theft of your Password, and we can prove we could have stopped someone from using your Password without your permission if you had told us, you could lose as much as $500.00. Also, if your statement shows transfers that you did not make, tell us at once. If you do not tell us within 60 days after the statement was mailed to you, you may not get back any funds you lost after the 60 days if we can prove that we could have prevented someone from taking the funds if you had told us in time. 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 309-582-3531 or 309-593-2117 during normal business hours listed above. **WE CANNOT ACCEPT NOTIFICATION OF LOST OR STOLEN PASSWORDS OR UNAUTHORIZED TRANSFERS VIA E-MAIL.**

10. Error and Questions

In case of errors or questions about your electronic transfers call us at 309-582-3531 or write us at:

1st Community Bank
PO Box 147
Aledo, IL 61231-0147

Notify us immediately if you think your statement or receipt is wrong or if you need more information about a transaction listed on the statement or receipt. We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error first appeared.

(a) Tell us your name and account number.

(b) Describe the error or the transfer you are unsure about and explain as clearly as you can why you believe it is an error or why you need more information.
(c) Tell us the dollar amount of the suspected error.

If you tell us orally, we may require that you send us your complaint or question in writing within 10 business days.

We will determine whether an error occurred within 10 business days (20 business days for new accounts) after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days (90 days for new accounts, point-of-sale, or foreign-initiated transfers) to investigate your complaint or question. If we decide to do this, we will credit your account within 10 business days (20 business days for new accounts) for the amount you think is in error so that you will have use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not credit your account for 30 days after the first deposit is made, if you are a new customer.

We will tell you the results within 3 business days after completing our investigation. If we decide that there was no error, we will send you a written explanation. You may ask for copies of the documents that we used in our investigation.

11. Termination

If you wish to terminate your access to the Services, call us at 309-582-3531. After receipt of your call, we will send you a written termination authorization for your signature and return to us. **Recurring transfers will not necessarily be discontinued because you terminate access to the Services.** We reserve the right to terminate the Services, 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 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 the Services 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 User Code and/or Password as an indication of an attempted security breach. Termination of the Services does not affect your obligations under this Agreement with respect to occurrences before termination.

12. Limitation of Liability

Except as otherwise provided in this Agreement or by law, we are 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 your personal computer equipment.

13. Waivers

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

14. Assignment

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

15. Governing Law

The laws of the State of Illinois shall govern this Agreement and all transactions hereunder. Customer acknowledges that he/she has reviewed this Customer Agreement, understands the terms and conditions set forth herein, and agrees to be bound hereby.

16. Indemnification

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

17. Security Procedures

By accessing the Services, you hereby acknowledge that you will be entering a protected web site owned by the Bank, which may be used only for authorized purposes. The Bank may monitor and audit usage of the System, and all persons are hereby notified that use of the Services constitutes consent to such monitoring and auditing. Unauthorized attempts to up-load information and/or change information on these websites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986.