ONLINE & MOBILE BANKING POLICY

FIRST STATE BANK OF HARVEY

Board Approval: December 13, 2024

FIRST STATE BANK OF HARVEY

TABLE OF CONTENTS

STATEMENT OF NEED AND DEFINITION 1

PURPOSE 1

SPECIFIC GOALS 1

AUTHORITY 1

POLICY ELEMENTS 2

- SERVICES OFFERED 2

MOBILE BANKING RISKS AND CONTROLS 2

RISK ASSESSMENT 2

RISK CONTROL ELEMENTS 3

MOBILE BANKING REQUIREMENTS 4

MOBILE DEPOSIT REQUIREMENTS 4

OPERATIONAL ELEMENTS 4

- OPERATING PROCEDURES 4
- VENDORS AND OUTSOURCING 4
- PLANNING AND DEPLOYMENT 4
- MOBILE APP CHANGES 5
- AUDIT AND REVIEW 5
- SECURITY MONITORING 5
- TRANSACTION MONITORING 5
- PERFORMANCE MONITORING 5
- REPORTING 5
- EMPLOYEE EDUCATION AND TRAINING 5
- CUSTOMER TRAINING 6
- CONTINGENCY PLANNING/BUSINESS CONTINUITY 6
- SECURITY INCIDENT HANDLING 6

REVIEW OF POLICY 6

RELATED DOCUMENTS 6

Functional Area:	**Operations**
Policy For:	**Mobile Banking**
Board Approved:	**Pending October 19, 2018**
Last Revision Date:	**New Policy**

STATEMENT OF NEED AND DEFINITION

Management has determined that the offering of Mobile Banking services to our customer base is necessary to remain competitive with banks sharing common markets. Mobile Banking will allow customers to view account balances, transfer funds between their accounts, view recent transactions and make payments to pre-established third parties. Additional types of banking services may be offered in the future.

Mobile Banking is offered to Online Banking customers via Mobile Text Messaging (SMS), Mobile Web Browser, or through applications available for certain mobile devices, such as Androids, iPhones and iPads.

Bank has elected to operate its Mobile Banking through its online banking service provider, DCI. The financial institution recognizes that, as with any outsourced product or service, reliance on service providers and software vendors requires sound risk management practices and vendor due diligence.

To protect the bank's customers, as well as its physical assets, the board of directors directs the bank to develop and implement a written Mobile Banking Policy and Procedures for the bank.

PURPOSE

The purpose of this policy is to delegate authority for and provide operational guidelines for Mobile Banking and to establish guidance on how to identify, measure, monitor, and control risks arising from the use of Mobile Banking. It also sets forth the expectations of company management and Bank's Board of Directors when implementing and operating Mobile Banking systems. This policy is to be used in conjunction with the Internet Banking Policies and Procedures.

SPECIFIC GOALS

The specific goals of the policy are to:

- Establish authority and responsibility for the implementation and ongoing administration of Mobile Banking
- Identify the services that will be made available to customers through Mobile Banking
- Establish guidelines to limit risk and resulting exposure
- Establish procedures that assist in monitoring customer satisfaction
- Establish employee training requirements

AUTHORITY

The ISO will serve as the Mobile Banking Coordinator and is responsible for development and implementation of Mobile Banking products and maintaining this policy. Responsibility also includes making recommendations to the board of directors regarding mandatory or desirable changes to the policy.

The ISO reassigns specific responsibility for the day-to-day operations of the procedures. This day-to-day responsibility may be assigned to other department managers, supervisors and employees.

POLICY ELEMENTS

SERVICES OFFERED

The following services/activities may be offered to Mobile Banking customers:

- View account balances and transactions
- Transfer funds between related accounts
- Make payments to pre-established third parties

MOBILE BANKING RISKS AND CONTROLS

Bank uses DCI as its software vendor and third-party processor to provide Mobile Banking services. The Bank has used DCI online banking system since 2008. We believe DCI has an excellent reputation, financial status and viability. Having a strong relationship with our vendor will help ensure that it performs as promised and that it is not only capable of keeping abreast of new or changing technology, but also committed to doing so. We have controls in place to monitor performance levels and to swiftly respond to any problem or emergency. This monitoring is ongoing and will continue to improve over time as our Mobile Banking services mature.

Control items should include, but not be limited to, our financial institution's ability to perform audits, either internally or on an outsourced basis. Bank will obtain copies of the provider's third-party audit report of internal controls. The User Considerations identified in the report will also be reviewed and evaluated annually.

RISK ASSESSMENT

All financial products and services contain an element of risk making effective risk management essential. Risk management is comprised of several factors:

- Identifying the risk
- Understanding the implications of the risk
- Measurement of the risk
- Setting acceptable risk tolerances and parameters
- Maintaining risk at acceptable levels

The following matrix describes risk factors that management feels may relate to Mobile Banking:

RISK CATEGORY	IMPLICATION OF RISK	MEASUREMENT	ACCEPTABLE PARAMETERS
Compliance risk – violation of regulations, policies and standards	Fines, penalties, damages, contractual problems, diminished reputation	Management, internal and external audit review	Low risk – regulations, policies and standards must be followed
Strategic risk – poor business decisions, poor implementation	Unable to meet related strategic goals	Management conducts due diligence of vendor and product.	Medium risk – new technology requires some strategic risk. However, not a new vendor.
Reputation risk – negative public opinion	Deter new relationships and ability to service existing customers, accelerate customer runoff	Management review of reports tracking negative customer comments. Maintain high levels of security and customer service. Review vendor's business continuity & disaster recovery tests to ensure availability of product.	Medium risk – must be aggressive in security and customer service
Transaction risk – problems with service and product delivery, monetary loss from bill pay transactions	Customer confidence and monetary damages	Management oversight and internal audit. Review of vendor's internal control audit report to ensure appropriate risk management practices. Bank's compliance with vendor's client considerations. Effective monitoring of bill pay activities, and NSF collection practices.	Low risk – do not offer mobile check deposits

RISK CONTROL ELEMENTS

Security Controls
Existing controls include: Token authentication, risk limits, daily review of unusual login reports and large transactions, notify me security alerts, account masking, strong password requirements, internal transfers only, website educational programs, SSL certification for website.

Data facilities have IPS/IDS in place to detect and prevent network attacks in addition to firewall and router event logs.

Database Security
The Device Analytics feature enhances security by controlling access to mBanking through the Mobile Application. Device Analytics works in the background, as soon as the user launches the app. It automatically performs a risk factor analysis on the user's mobile device, looking at key aspects of the device's operating system and configuration for potential risks. The risk factor analysis score is therefore generated before the user even begins to attempt login to mBanking. If Device Analytics detects significant risk factors on the user's device, it can either require the user to answer security questions for additional authentication, or deny access if the risk is severe.

Handset Security
The product leaves no financial data on the mobile device once a mobile banking session has ended. In the case of SMS, balance and transaction description data may remain in the user's inbox, but does not include full account numbers or any other sensitive information. There is both a local (mobile side) and server side session timeout that is built into mBanking. So, if a user logs in and then sets down the phone, the phone will time out after a 3-minute period of

inactivity. After a timeout, the user must sign on again before any data can be viewed. Both the Mobile Browser and Mobile Application modes transmit all data via HTTPS with 128-bit encryption, the same level of protection typically found in Online Banking sites. Text Banking relies on an industry standard SMPP interface between the mobile banking application and the SMS aggregator. The data transmitted via text is in the clear, hence the reason for recommended use of balance and transaction inquiry functions only.

Passcode Masking
During entry, the passcode is represented by asterisk characters to avoid being viewed by an outside individual.

Touch ID Biometric Signon/Face ID
Users of the mBanking native app on compatible iPhone devices can use the Touch ID feature of those devices to sign on to the app. Touch ID signon is available on Touch ID-capable iPhone models running iOS 8 or later. With Touch ID, entry of a user ID and password is not necessary to access mBanking—just a fingerprint. The Touch ID signon capability is optional. The user can enable or disable Touch ID signon for the app at any time, and even when it is enabled, signon using user ID and password is still possible. Touch ID takes advantage of the fingerprint data stored on the iPhone device. This means that one or more fingerprints must have already been stored on the device to use Touch ID signon for the mBanking app.

MOBILE BANKING REQUIREMENTS

The following requirements are established for Mobile Banking:

- A Mobile Banking User must be an existing bank customer who has previously enrolled in Online Banking
- Mobile Banking uses the same logon authentication criteria as Online Banking
- Enrollment requires Online Banking credential knowledge and confidential data knowledge
- Mobile access to accounts require valid credentials and device identification
- Mobile access is locked at 3 incorrect login attempts
- The mobile banking solution will time out after 3 minutes of inactivity
- Users may disable their device in the Mobile Banking Center or may contact the bank to remove their device should it be lost or stolen

OPERATIONAL ELEMENTS

To facilitate a sound system, management has addressed the elements detailed below and will re-evaluate these needs as required. The following elements were considered prior to implementation of Mobile Banking and will be considered prior to adding new products or services.

OPERATING PROCEDURES

Each Mobile Banking product or service shall have specific guidelines for procedures, controls and monitoring. These guidelines will address controls to protect data integrity and guard against failure of desired results.

VENDORS AND OUTSOURCING

The bank may rely on third parties to provide Mobile Banking products and services. Third party selection may be based on the FFIEC guidelines regarding Outsourced Technology services. The due diligence review will consider the third party's financial condition and its ability to provide the products and services from a standpoint of internal controls, security, maintenance and upkeep of the system.

PLANNING AND DEPLOYMENT

Proper due diligence will occur with the development of any new Mobile Banking product or service. Related computer hardware, software, obsolescence, support, and similar issues will be carefully evaluated. Training will also be a part of the planning and deployment of any new product or service.

MOBILE APP CHANGES

Change requests for the Bank's Mobile Banking App are approved by the President. The ISO is responsible for effecting changes, and must rely on a third party vendor to assist. Content or design changes will be authorized.

The bank's internal auditor or compliance officer will review the app when changes are made and, thereafter, on a periodic basis to ensure compliance with applicable regulations.

AUDIT AND REVIEW

Audit and regulatory compliance risks shall be carefully evaluated and identified prior to implementation and on an ongoing basis. The bank's internal auditor will review all procedures and information disclosures to ensure compliance with applicable regulations. An internal risk assessment review is performed on an annual basis.

SECURITY MONITORING

Security reports are to be generated and monitored for irregular or suspicious events or activity. The following types of risk are some areas that will be monitored daily:

- Unauthorized user accessing information
- Loss of Data integrity
- Transaction flow

TRANSACTION MONITORING

FIXM monitoring service monitors the following activity for abnormalities on a daily basis:

- Frequent unsuccessful sign-on attempts
- Bill Payments

PERFORMANCE MONITORING

Bank has selected several key performance indicators to determine whether the Mobile Banking system is working as planned.

Indicators include system response times, system availability, types of customer inquiries, problem resolution and traffic volume. Performance monitoring reports can contribute significantly to identifying system inefficiencies, addressing performance problems and estimating capacity needs.

REPORTING

The Mobile Banking system generates sufficient reporting to satisfy daily monitoring and control of transactions and activities. Additionally, appropriate reports should be generated that provide the necessary information to track the effectiveness of the program.

Online and Mobile Banking activities will be reported to The Board of Directors on an annual or as needed basis, as part on the Online Banking Internal Audit.

EMPLOYEE EDUCATION AND TRAINING

Employees will be trained with regard to appropriate use of the Mobile Banking Service. Training will include the use of proper controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means. The introduction of new products will require additional training. Such training will occur during the initial introduction to employment and will be updated as needed. Employee transfers within the bank will require an update on certain procedures.

CUSTOMER TRAINING

Customers have access online to a list of FAQs regarding mobile banking and video demos. Security information on scams and tips for protecting your PC and Mobile devices are available on the bank's website. Statement stuffers and brochures are also used for customer education.

CONTINGENCY PLANNING/BUSINESS CONTINUITY

The Mobile Banking product server is maintained at DCI's data center. As Bank's third-party provider, DCI has primary responsibility for physical security, maintenance, backups and current levels of software. As part of vendor due diligence, Bank has determined that DCI has developed business continuity and recovery plans for this server as part of an overall disaster recovery plan. Bank will review the disaster recovery test reports and their annual third party systems review.

SECURITY INCIDENT HANDLING

Security incidents will be handled according to the procedure outlined in the Information Technology and Security Policy

REVIEW OF POLICY

The board of directors will review this policy at least once each year and make any revisions and amendments it deems appropriate. The ISO will be responsible for suggesting more frequent revisions as situations or changes in laws or regulations dictate.

RELATED DOCUMENTS

- Internet Banking Policies and Procedures
- Information Technology and Security Policy
- First Data Mobile Manager mBanking Product Guide

First State Bank of Harvey-Online Banking Agreement and Disclosures

This Online Banking Agreement and Disclosure, along with all implementation forms, applications, user guides, fee schedules, and other documents provided to you when you begin this service or request additional services (collectively, "Agreement") states the terms and conditions that govern your use of First State Bank's Online Banking Service. The Online Banking service provides First State Banks customers access to perform a number of banking functions through the use of a personal computer or mobile access device, such as a smart phone or tablet, on Accounts linked to the service.
Please read this Agreement carefully. By requesting and using Online Banking, you agree with the terms and conditions of this Agreement and acknowledge that you have read it carefully.

Procedure
Customer is to start by filling out an online application at www.firstharvey.com once bank has verified the account, they will call the phone number on the account to let you know the steps to login.

Relation to Other Agreements
This Agreement is intended to supplement and not to replace other agreements between you and us relating to your Accounts, including, without limitation, our Deposit Account Terms and Conditions. Your other agreements with the Bank, including without limitation the Deposit Account Terms and Conditions and any agreements for loans and other services, continue to apply notwithstanding anything in this Agreement. In the event of a conflict between this Agreement and any other agreements between you and us, this Agreement shall control with respect to Online Banking and related services. You should review those agreements for any applicable fees, for limitations on the number of transactions you can make, and for other restrictions that might impact your use of an Account with Online Banking.
I. Definitions
The following definitions and rules of construction apply in this Agreement:
a. **"Account"** means any First State Bank account which you access using Online Banking.
b. **"Authorized Representative"** refers to a person with authority with respect to the Account;
c. **"Bill Pay Service"** is the online service that enables the scheduling of bill payments using a personal computer;
d. **"Consumer account"** means a checking or savings account established by an individual primarily for personal, family, or household purposes.
e. **"ISP"** refers to your Internet Service Provider;
f. **"Online Banking"** is the internet-based service providing access to your Bank account(s);
g. **"Password"** is the customer-generated code selected by you for use during the initial sign-on, or the codes you select after the initial sign-on, that establishes your connection to Online Banking;
h. **"PC"** means your personal computer which enables you, with the Internet browser and ISP, to access your Account online;
i. **Time of day** references are to Central time;
j. **"We", "Us", or "Bank"** refer to First State Bank which offers Online Banking and holds the Accounts accessed by the Online Banking service;
k. **"You" or "Your"** refers to the owner of the Account or the Authorized Representative.

Schedule of Fees
There are currently no monthly or periodic fees for Online Banking. Fees disclosed separately to you for separate services provided via Online Banking in which you enroll or in connection with your Accounts, such as charges for dropping below minimum balances, insufficient funds, or check stop payment fees will apply. Please consult our current fee schedule for a complete list of fees. We reserve the right to change applicable fees at any time and will provide you with any notice required by law.

Service Access; Consumer and Non-consumer
Online Banking Agreement and Disclosures Hardware and Software Required When you request the use of the Online Banking service, the Bank will provide instructions on how to access and use the service. You will need to have an Internet-enabled device, ISP, User ID, and Password to access Online Banking.
We may update these requirements at any time in our sole discretion. You are solely responsible for having the required hardware and software and for securing an ISP. You also are responsible for any and all fees relating to communications carriers (e.g., telephone, cable, DSL or satellite), software providers (other than software that we may

provide you) and/or internet service fees that may be assessed by your communications carrier and/or internet service provider,

Availability and Business Days
Online Banking is generally available 24 hours a day, seven (7) days a week; however, availability of Online Banking or certain services may be suspended for brief periods of time for purposes of maintenance, updating and revising the software. The Bank's business days are Monday through Friday, excluding Federal holidays. All Online Banking transaction requests received after 2:30 p.m. on business days and all transactions which are requested on Saturdays, Sundays, or holidays on which the Bank chooses to remain closed will be processed on the Bank's next business day. The Bank's business day begins at 8:30 a.m.

Consumer Accounts
Certain provisions of this Agreement apply only to Consumer Accounts. The consumer protection provisions of the federal Electronic Funds Transfer Act and Regulation E apply only to electronic fund transfers involving Consumer Accounts. Please refer to the Electronic Fund Transfer Disclosure and your Deposit Account Terms and Conditions for more information.

Non-consumer Accounts
If your Accounts are owned by an entity other than a natural person or were established primarily for business, commercial or agricultural purposes, then any Online Banking electronic fund transfer will be considered an "authorized use," and your liability for any Online Banking transaction relating to that Account will be unlimited, notwithstanding the provisions of the Electronic Fund Transfer Act, Regulation E, or any standardized literature or disclosures we may send you.

Online Banking Services
a. Transfers Between Deposit Accounts: You can transfer funds between your deposit Accounts with us (i.e., your checking or savings Accounts).
b. Transfers Between Your Deposit Accounts and Loan Accounts.
c. Bill Pay Service: If you enroll in the Bill Pay Service, you may pay bills directly from your deposit Accounts in the amounts and on the days you request. Limits for bill pay are set to ACH $2500.00 and check as $5000.00. We must have a written agreement approved by loan officer to change the default settings.
d. Transfers Outside First State Bank to Account You Own at Other Financial Institutions: If you enroll in external transfers, you may transfer funds from your deposit Accounts to accounts you own at other financial institutions. The account will first need to be verified by the financial institution. Daily Amount limits are set to $1000.00 unless approved by the bank.
e. Stop Payment- you may submit stop payments through online banking.

Online Banking Agreement and Disclosures
In addition, as noted herein, we reserve the right to refuse to pay any person or entity to which you may direct a payment through Online Banking. We will notify you promptly if we decide to refuse to pay a person or entity designated by you; however, this notification is not required if you direct us to make any payment which is otherwise prohibited under your agreements with us.

Use of User ID and Password
In order for you to access Online Banking, you must obtain a unique User ID and Password. When you sign onto Online Banking using your User ID and Password, you authorize us to follow the instructions we receive relating to your Accounts and to charge and credit your Accounts according to those instructions. Because your User ID and Password are the principal security measures to protect access to your Accounts, you agree to keep all User ID and Password information confidential and to take all reasonable precautions to protect the secrecy of this information. You acknowledge that no person from the Bank will ever ask for your Password and that our employees do not need and should not ask for your Password. You therefore agree never to provide your Password to anyone claiming to represent us. If you give your User ID or Password or make it available to another person, you authorize that person to access your accounts through Online Banking and to give the Bank instructions relating to your Accounts as an authorized user. You also authorize us to comply with those instructions even if that person exceeds your authorization. The Bank has no responsibility for establishing the identity of any person who uses your Password. You agree that you are liable for any transaction received by the Bank that includes your Password.

Security
You understand the importance of your role in preventing misuse of your Accounts through Online Banking and you agree to promptly examine your periodic paper and/or electronic statement for each of your Accounts as soon as you receive it. You agree to protect the confidentiality of your Account and Account number, your User ID and Password, and your personal identification information, such as your driver's license number and social security number. You understand that personal identification information by itself or together with information related to your Account may allow unauthorized access to your Account.
Your User ID and Password are intended to provide security against unauthorized entry and access to your Accounts. Data transferred via Online Banking utilizes identification technology to verify that the sender and receiver of the transmissions can be appropriately identified by each other. Notwithstanding our efforts to ensure that Online Banking is secure, you acknowledge that the internet is inherently insecure and that all data transfers, including electronic mail, occur openly on the internet and potentially can be monitored and read by others. We cannot and do not warrant that all data transfers utilizing Online Banking, or e-mail transmitted to and from us, will not be monitored and read by others. We recommend that you use the secure messaging feature within the Online Banking system.
We will rely and act on instructions we receive through Online Banking. You are responsible and liable for those transactions to the extent allowed by law and as provided in this Agreement and all of our other agreements with you. All such instructions will be considered as having been given to us directly by you and shall have the same authority as your written signature in authorizing us to comply with the instructions. You agree that you have been provided with a disclosure of the security procedures that will be used to authenticate transactions through Online Banking. You agree that those security procedures, including without limitation the use of the User ID, Password, and identification technology as described herein, are commercially reasonable security procedures for the Online Banking services you utilize and that we may rely upon any instructions we receive upon authentication using these Online Banking Agreement and Disclosures agreed upon security procedures. We may update the security procedures at any time in our sole discretion. Your implementation and use of the revised security procedures constitutes your agreement to the changes and your agreement that the procedures are commercially reasonable.

Virus/Malware/Spyware Protection
The Bank is not responsible for any electronic viruses, malware, or spyware that you may encounter. You are responsible for taking and maintaining security precautions to protect your computer, data, and system. You agree that we are not responsible for any electronic virus, spyware, or malware that you may encounter using Online Banking. We encourage you to routinely scan your PC, Mobile Device, and diskettes using any up-to-date, reliable virus, spyware, and malware protection product to detect and remove any virus, spyware, and malware found.

Stopping Payment of Checks
You may also use Online Banking to stop payment of a check you have written on your deposit Account. Any stop payment request must precisely specify the Account number, the check number, and the amount, date and payee of the check. You acknowledge that if you provide us with incorrect information, even if the information is a close approximation of the actual information, we will not be liable for payment of the check. The check stop payment order must be given in the manner required by law and must be received by us in such a time and manner as to afford the Bank a reasonable opportunity to act on it. Once received the bank will call and you will be asked to stop in and sign a form.
Without limiting the foregoing, we will not be liable for cashing a check within one Business Day of receiving a stop-payment order for the check. A check stop payment order will automatically expire six (6) months after receipt unless you renew it by completing a new check stop payment order. Only the person who initiated the check stop payment order can cancel it by coming into the branch and signing a release form. You will need to stop in and sign the check stop payment order. Please refer to the fee schedule for the applicable fees for stop payment requests.

Statements
You will receive your regular account statement monthly or quarterly, depending on the type of Account. These statements are available to you electronically within Online Banking on a rolling eighteen (18) month period.

Email
If you send the Bank an email message, the Bank will be deemed to have received it on the following business day. You should not rely on email if you need to report an unauthorized transaction from one of your Accounts or if you need to stop a payment that is scheduled to occur.
Online Banking Agreement and Disclosures sensitive information such as Account numbers, Passwords, or other Account information via any public email system. You acknowledge that you understand the risk of using e-mail and that we are unable to guaranty the authenticity, privacy or accuracy of information received or sent via e-mail or to

monitor the authorization of persons using your e-mail address. If you wish to contact the Bank electronically, please use the Message Center provided in the Online Banking site. Use the secure form to email the Bank regarding inquiries about electronic fund transfer error resolutions, to report unauthorized transactions, or to discuss other Banking concerns confidential in nature. Please note that the Bank will never contact you via email and ask for your Online Banking logon credentials.

Account Alerts

Account alerts allow you to choose optional alert messages for your Accounts. Each account alert has different options available, and you will be asked to select from among these options upon activation of an account alert. We may add new alerts from time to time, cancel old alerts, and change or terminate the account alert process at any time without notice. Alerts will be sent to the email address you have provided as your primary email address for Online Banking. If you change your email address, you are responsible for informing us of that change.

We do not guarantee the delivery or accuracy of account alerts, and they may be delayed or prevented by factors that are beyond our control (such as system failure or misdirected delivery). You agree that we are not liable for any delays, failure to deliver, or misdirected delivery of any alert; for any errors in the content of an alert; or for any actions taken or not taken by you or a third party as the result of an alert. Because alerts are not encrypted, we will never include your full Account number. However, alerts may include your name and some information about your Accounts. Depending upon the type of alert, information such as your Account balance, transaction information, or the due date for a loan payment may be included. Anyone with access to your alerts will be able to view the contents of these messages.

Information Disclosure to Third Parties

We will disclose information to third parties about your Account or the transfers you make, as permitted by law and by our Privacy Policy, including, without limitation:

- Where it is necessary for completing or tracing transfers or resolving errors or claims;
- In order to verify the existence and condition of your Account for a third party, such as a credit bureau or merchant or other financial institution;
- In order to comply with government agency, bank regulators, court orders or other legal process;
- To our employees, auditors, service providers or attorneys in the course of their duties;
- To other companies affiliated with us;
- To others with your consent; and
- Whenever required by law.

Applicability

The provisions in this Section are only applicable to electronic fund transfers that credit or debit a consumer account and are subject to the federal Electronic Funds Transfer Act and Regulation E. When applicable, the Bank may rely on any exceptions to these provisions that are contained in Regulation E. All terms that are not defined in this Agreement but which are defined in Regulation E shall have the same meaning when used in this Section. If your Accounts are not consumer accounts, see the below Section regarding liability and error resolution provisions applicable to accounts other than consumer accounts.

Contact in Event of Unauthorized Transaction

If you believe your Password or User ID has been lost or stolen or that someone has transferred or may transfer money from your Account without your permission, call 1-701-324-2285 or write us at:

First State Bank of Harvey
700 Lincoln Ave
Harvey, ND 58341

We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error appeared. When you contact us:

1) Tell us your name and Account number (if any).
2) 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.
3) Tell us the dollar amount of the suspected error.

We will determine whether an error occurred within 10 business days after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days to investigate your complaint or question. If we decide to do this, we will credit your Account within 10 business days for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation.

For errors involving new Accounts, point-of-sale, or foreign- initiated transactions, we may take up to 90 days to investigate your complaint or question. For new Accounts, we may take up to 20 business days to credit your Account

for the amount you think is in error. We will tell you the results within three 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.

Our Liability for Failure to Make Transfers

If we do not complete a transfer to or from your Account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages. However, there are some exceptions. We will not be liable, for instance:

- If through no fault of ours, you do not have enough money in your Account to make the transfer.
- If the money in your Account is subject to legal process or other encumbrances restricting the transfer.
- The person or entity to which you direct payment mishandles, delays, or fails or refuses to accept a payment sent by us.
- You have provided us with incorrect, incomplete or inaccurate data or other Account information, including but not limited to date related errors, or you have otherwise failed to comply with the payment or transfer instruction requirements set forth in this Agreement.
- There are technical problems in our receipt of information or instructions from you (for example, problems arise with computers, software, modems, or telephone communications, including but not limited to date related problems).
- If the transfer would go over the available balance in your overdraft account.
- If a terminal or system was not working properly and you knew about the breakdown when you started the transfer.
- If circumstances beyond our control (such as fire or flood) prevent the transfer or use of First State Bank Online Banking, despite reasonable precautions that we have taken.
- If we have a reasonable basis for believing that unauthorized use of your Account(s) has occurred or is occurring, if you are in default under this or any other Agreement with us, or if you or we have terminated or suspended your use of First State Bank Online Banking.
- If your operating system is not properly installed or properly functioning.
- For errors or failures from any malfunctions of your browser, internet service provider, computer, computer virus or other problems relating to the computer equipment you use to access First State Bank Online Banking.
- This Agreement or any applicable authorization has been terminated.
- Unusual or extraordinary circumstances exist which indicate improper or unlawful use of your Account.

Limitation on Liability

IN NO EVENT WILL THE BANK OR ANY OF ITS OFFICERS, DIRECTORS, SHAREHOLDERS, PARENTS, SUBSIDIARIES, AFFILIATES, AGENTS, LICENSORS, OR THIRD PARTY SERVICE PROVIDERS BE LIABLE FOR ANY CONSEQUENTIAL (INCLUDING WITHOUT LIMITATION, LOSS OF DATA, FILES, PROFIT OR GOODWILL OR THE COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICE), INDIRECT, INCIDENTAL, SPECIAL OR PUNITIVE DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT,NEGLIGENCE OR ANY OTHER THEORY, ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, ONLINE BANKING, THE INABILITY TO USE ONLINE BANKING, ANY MERCHANDISE OR SERVICES PURCHASED OR OBTAINED USING ONLINE BANKING, OR ANY MESSAGES RECEIVED VIA ONLINE BANKING OR ANY TRANSACTIONS THEREUNDER, EVEN IF THE BANK HAS BEEN SPECIFICALLY ADVISED OF THE POSSIBLITY OF SUCH DAMAGES.

No Liability for Certain Failures

Except as specifically provided in this Agreement or where applicable law requires a different result, neither we nor our service providers or other agents will be liable for any loss or liability resulting in whole or in part from any act or failure to act of your equipment or software, or that of an internet browser, by an internet access provider, by an online service provider or by an agent or subcontractor of any of them, nor will we or our service providers or other agents be responsible for any direct, indirect, special or consequential, economic or other damages arising in any way out of your access to or use of, or failure to obtain access to Online Banking.

Liability and Error Resolution Provisions Applicable to Accounts Other than Consumer Accounts Customer's Responsibility for Accounts other than consumer accounts, you bear the risk of using Online Banking, including the risk of erroneous and fraudulent transactions and the risk of all transactions using your User ID and Password, and your liability for any Online Banking is unlimited. Unless otherwise required by applicable law, we are responsible

only for performing Online Banking services as delineated in this Agreement. We will not be liable to you for failure to make a requested transfer or otherwise in the instances set forth in the Section above as to consumer accounts.

Recommended Best Practices for Consumer Online Banking
User ID and Password Guidelines
• Create a "strong" Password with at least 8 characters that includes a combination of letters and numbers.
• Use Multifactor authentication or biometrics whenever possible to enhance security.
• Change your Password frequently.
• Never share Account information, User ID or Password information.
• Never leave your Account information within range of others.
• Avoid using an automatic login feature that saves User ID and Passwords.
• Do not send privileged Account information such as User ID and Passwords in any public e-mail system.

General Guidelines
• Do not use public or other unsecured computers for logging into Online Banking.
• Check your last login date and time, and transfer history every time you log in.
• Review Account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to the Bank.
• Whenever possible, use Bill Pay instead of checks to limit Account number dissemination exposure and to obtain better electronic record keeping.
• Take advantage of and regularly view system alerts, such as balance alerts and transfer alerts.
• Don't use Account numbers, your Social Security number, or other Account or personal information when creating Account nicknames or other titles.
• Review historical reporting features of your Online Banking application on a regular basis to confirm payment and other transaction data.
• Never leave a computer unattended while using Online Banking.

Online Payments, Account Transfers & Account Data
• When you have completed a transaction, ensure you log off to close your computer connection.
• Reconcile by carefully monitoring Account activity and reviewing all transactions on a daily basis.
• Review historical and audit reports regularly to confirm transaction activity.
• Utilize available alerts for funds transfer activity.