NORTHEAST SECURITY BANK

Online / Mobile Banking Agreement and Disclosure

Requirement: You must have an account with Northeast Security Bank to access Online / Mobile Banking.

Enrollment Instructions: If you are currently an accountholder with Northeast Security Bank we invite you to enroll in Online / Mobile Banking. Please visit www.banknsb.com and click enroll now to enroll for the Online / Mobile Banking Service.

Preface

Northeast Security Bank is pleased to offer you Online / Mobile Banking. Our Online / Mobile Banking product allows you to conduct your banking at your convenience from home, work, or wherever you may have access to the web. We are located on the web at www.banknsb.com. Northeast Security Bank's Online / Mobile Banking consists of Online banking, text message banking, mobile browser banking and downloadable Touch Banking app.

Northeast Security Bank's Online / Mobile Banking services allow our customers to:

	Online Banking	Text Message Banking	Mobile Browser Banking	Downloadable App Banking
View Account Balances	X	X	X	X
View Transaction History	X	X	X	X
View Loan Payment History	X	X	X	X
Transfer Between Accounts	X		X	X
Make Loan Payments	X		X	X
Print Account Statements	X			
Send E-Mails to NSB	X		X	X
Mobile Deposit				X
Pay Bills	X			

****Important Note****

Online / Mobile banking transactions have a cut-off time of 6:00 p.m. If you conduct an Online / mobile transaction before 6:00 p.m. 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 p.m. on Monday through Friday or on a day we are not open, we will consider that the transaction was made on the next business day we are open. ***An exception to this is Mobile deposits, which have a cut-off of 2:00 p.m. on business days that we are open.

****Important Note****
All loan payment transfers through Online / Mobile Banking are automatically paid to principal and interest. If you would like to pay off a loan please stop in or call Northeast Security Bank.

1. Introduction.

This Online/Mobile Banking Agreement and Disclosure governs your use of Online / Mobile Banking. Throughout this agreement the Agreement and Disclosure will be referred to as "Agreement". By using Online / Mobile 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 Online / Mobile Banking services ("Services") to be provided by Northeast Security Bank ("Bank"), "Customer", "You", "Your", refers to the person(s) subscribing to or using the Service. "We", "Us", "Our", refers to Northeast Security Bank and any agent, independent contractor, designee, or assignee Northeast Security Bank may involve in the provision of Online / Mobile Banking. "Business Day" refers to any calendar day other than Saturday, Sunday, or any holidays recognized by Northeast Security Bank.

3. <u>Privacy Policy</u>

Northeast Security Bank recognizes and respects our responsibility to protect our customers' private information. In continuing our commitment to provide quality service to our customers, Northeast Security Bank has adopted the following privacy policy. This privacy policy applies to individuals, and Northeast Security Bank reserves the right to amend it at any time. If your relationship with Northeast Security Bank changes and/or is terminated, we will continue to adhere to the privacy practices described in this policy.

<u>Our Collection, Use and Retention of Customer Information</u>
We collect, use, and retain information about our customers only where we reasonably believe it would be useful in administering our business, and providing products, services, and other opportunities to our customers. We collect and retain information only for specific business purposes – and will tell you why we are collecting and retaining it upon your request. We use information to protect and administer our customers' records, accounts, and funds; to comply with certain laws and regulations; to help design or improve our products and services; and to understand your financial needs in order to provide you with quality products and outstanding service. Nonpublic personal information is nonpublic information about you that we obtain in connection with providing a financial product or service to you. For example, nonpublic

personal information includes information regarding your account balance, payment history, etc. We may collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other loan and account forms;
- Information about your transactions with us, our affiliates, or others; and
- Information we receive from third parties such as credit bureaus.

Disclosure of Customer Information

We are permitted under law to disclose specific information about your accounts or other personally identifiable data to either affiliated or non-affiliated third parties in the following circumstances:

- When you have requested or authorized it;
- When the information is provided to help complete a transaction initiated by you;
- When the information is provided to a reputable credit bureau or similar credit reporting agency;
- When the disclosure is lawfully permitted or required (for instance, in accordance with a court order, or a regulatory examination);
- When the information is disclosed to either affiliated or non-affiliated third parties to assist us in servicing your loan or account with us;
- When the information is disclosed to our affiliates and the information is about our experiences or transactions with you or your accounts; and
- In any other circumstance permitted or required by law.

Information We Disclose for Joint Marketing Purposes

We may disclose all of the information we collect, as described above, to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

Safeguarding the Security of Customer Information

We maintain physical, electronic, and procedural information safeguards that comply with federal standards to protect nonpublic personal information. We continually evaluate and assess new technology for protecting information.

Limited Employee Access to Information

We have procedures and security levels that limit employee access to personally identifiable information to those with a business reason to know such information. The importance of confidentiality and customer privacy is addressed with utmost seriousness. Appropriate measures are taken to enforce employee privacy responsibilities.

Maintenance of Accurate Information

We have implemented procedures to ensure that our customers' financial information is accurate, current, and complete in accordance with commercial standards and federal law. We also have procedures for responding to requests to correct inaccurate information in a timely manner, and to update information and remove non-current information. Customers should notify us immediately at (563) 578-3251/P. O. Box 269, Sumner, IA 50674 if they believe our records contain inaccurate or incomplete information.

Our Privacy Policy and You
If you have any questions about this policy or concerns about the privacy of your information, please contact us at (563) 578-3251.

4. Your Usercode / Access ID / Username and Password

Each individual who has access to Online / Mobile Banking, including each individual named on joint accounts, must designate a Usercode / Access ID / Username and Password. Your password must be a minimum of 8 characters and a maximum of 17 characters. It must have at least 1 numeric character and 1 alpha character. For example, your password may be: SAFE2345. You will be given a random 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. Your Username can be changed once upon initial log in. This is the only opportunity to change your Username. It is recommended that you change your password periodically to enhance security. If you leave your Online / Mobile banking session and do not log out manually you will automatically be logged out after ten minutes and will need to enter your username and password again to regain access to the system. If there are three consecutive failed log-in attempts to Online / Mobile Banking the user will be locked out of the system and will need to call Northeast Security Bank to regain access to the system.

5. Online Security

Northeast Security Bank is pleased to offer Online / Mobile 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 Online service and communication 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 Online / Mobile Banking system with regard to security. There are several levels of security within our security framework. User Level deals with cryptography and Secure Socket Layer (SSL) protocol, and is the first line of defense used by all customers accessing our Banking Server from the public Online. Server Level focuses on firewalls, filtering routers, and our trusted operating system. Host Level deals specifically with our Online 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. SSL is an open protocol that allows a user's browser to establish a secure channel for communicating with our Online 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 that ensures that you are truly communicating with the Online/Mobile Banking Server and not a third party trying to intercept the transaction.

After a secure connection has been established between your device / browser and our server, you then provide a valid username and password to gain access to the services. This information is encrypted, logged by the server forming a 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 username and password from others. You must follow the password parameters we specify at the time you sign up for an Online Banking account. We also recommend changing your password often. Session time-outs and a limit on the number of login 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 online 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 Online / Mobile banking transactions using host data. In addition, communication timeouts ensure that the request is received, processed, and delivered within a given time frame. 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 Online security technology, users of the Online / Mobile Banking system 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 your Internet Browser.
- Your password must be kept confidential. You must follow our specific parameters for a password and change it frequently 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/device unattended while logged on to the Online / Mobile banking system. Others may approach your computer/device and gain access to your account information if you walk away.

- Click Log Off 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/device.
- Keep your computer/device free of viruses. Use virus protection software to routinely check for a virus on your computer/device. Never allow a virus to remain on your system while accessing the Online / Mobile banking system.
- Report all crimes to law enforcement officials immediately
- Do not choose an easily guessed password, and never write down your password

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

6. Equipment

You are solely responsible for the equipment (including, in the case of Online / Mobile Banking, your personal computer/device 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

Northeast Security Bank is not responsible for any electronic virus or viruses that you may encounter. We encourage our customers to routinely scan their PC/device using a reliable virus product to detect and remove any viruses. Undetected or un-repaired 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 8:30 a.m.- 4:00 p.m. Monday, Tuesday, Wednesday, Thursday, and Friday; and Saturday (Drive Up Only) 8:30 a.m. – 11:30 a.m. Everyday is a business day, except for Saturdays, Sundays, and Northeast Security Bank holidays. Our policy is to make funds available to you on the first business day after the day we receive your deposit/transfer. **However, Online / Mobile Banking transactions have a cut-off time of 6:00 p.m. If you conduct an internet transaction before 6:00 p.m. 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 p.m. on Monday through Friday or on a day we are not open, we will consider that the transaction was made on the next business day we are open.** As for mobile deposits the same applies as above, but the cut-off time is 2:00 p.m. You are free to schedule online / mobile transfers / payments 24 hours a day, seven days a week with Online / Mobile banking as allowed, except during maintenance periods.

9. Notice of Your Rights and Liabilities

Security of your transactions is important to us. Use of the Services may therefore require a password. If you lose or forget your password, please call (563) 578-3251 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. Online / Mobile Banking Services enable 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 two (2) business days you can lose no more than $50.00. If you do NOT tell us within two (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 sixty (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 (563) 578-3251 during normal business hours listed above. **WE CANNOT ACCEPT NOTIFICATION OF LOST OR STOLEN PASSWORDS OR UNAUTHORIZED TRANSFERS VIA E-MAIL.**

10. Errors and Questions

In case of errors or questions about your electronic transfers call us at (563) 578-3251 or write us at:
Northeast Security Bank
108 North Carpenter P O Box 269
Sumner, IA 50674

Notify us immediately if you think your statement or receipt is wrong of 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.

(1) Tell us your name and account number.
(2) 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.
(3) 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 or 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 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.

11. Disclosure of Account Information to Third Parties

We may disclose information to third parties about your account or the transactions you make:
a) Where it is necessary for completing transactions or resolving errors involving the Services; or
b) In order to verify the existence and condition of your account for a third party, such as a credit bureau or a merchant; or
c) In order to comply with government agency rules, court orders, or other applicable law; or
d) To our employees, service providers, auditors, collection agents, affiliated companies, or attorneys in the course of their duties and to the extent allowed by law; or
e) If you give us permission.

12. Authorization to Obtain Information.

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

13. Termination

If you want to terminate your access to the Services, call us at (563) 578-3251. After receipt of your call, we will terminate your access to the Services. There are other instances where your access to the Services may be terminated. This may occur when the Services become dormant due to you not accessing the Services within a 6 month period. If your access to the Services is terminated due to dormancy, you may request that your access be re-established by calling the numbers listed above. The Services will also be terminated upon ending all account relationships with you. 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. Recurring transfers will not necessarily be discontinued because you terminate access to the services.
In that event, or in the event that you give us a notice of termination, 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 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.

14. 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 computer / device.

15. Waivers

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

16. Assignment

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

17. Governing Law

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

18. 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.

19. 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 web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986.

SPECIFICS OF MOBILE BANKING

TERMS AND CONDITIONS FOR MOBILE BANKING SERVICES

CONSENT: BY ENROLLING, YOU CONSENT TO BEING CONTACTED AT THE MOBILE PHONE NUMBER AND EMAIL ADDRESS THAT YOU PROVIDE. THIS INCLUDES, BUT IS NOT LIMITED TO, CONTACT THROUGH LIVE OPERATORS, TEXT MESSAGES, or EMAIL MESSAGES. CONTACT MAY OCCUR TO RESPOND TO YOUR INQUIRIES, TO OFFER YOU ADDITIONAL SERVICES, TO COLLECT MONEY YOU OWE US AND FOR OTHER CUSTOMER SERVICE PURPOSES. YOU CONSENT TO THESE CALLS AND TEXTS EVEN IF THE MOBILE PHONE NUMBER PROVIDED IS ON ANY STATE OR FEDERAL "DO-NOT-CALL" LIST AND EVEN IF YOU HAVE PREVIOUSLY REQUESTED US NOT TO CONTACT YOU AT THE MOBILE PHONE NUMBER.

As used in these Terms and Conditions (these "Terms"), "you" and "your" mean the person enrolled in our Mobile Banking Services and "we," "us" and "our" mean **Northeast Security Bank 108 North Carpenter, Sumner, IA 50674.** Your use of the mobile banking services that we make available now or in the future (the "Services") means you agree to the following:

General Terms

1. Eligibility. These are optional Services and you are free to discontinue use at any time. You acknowledge that the Services may change over time and that if you wish to receive the Services, you may be required to download certain apps and updates from time to time. Additional enrollments may be required for some of the Services. You must be the authorized user for the mobile device that you wish to enroll and it must have the functions needed to support the Services (e.g., it must be web-enabled and/or have the capacity to receive texts). The Services may not be accessible in all geographic locations and may not function with some devices, wireless carriers and mobile plans. Your wireless carrier's message and data rates may apply. You are solely responsible for charges imposed by your carrier or any third party based on the use of your device. Not all customers are eligible for the Services. You may not be able to enroll if you are not eligible or if you do not follow all enrollment instructions. You represent that the information you supplied with your enrollment was accurate. You agree to keep the information in your mobile banking profile accurate and up-to-date and you should notify us in advance if your phone number or address is going to change. You consent to receiving electronic communications from us through your mobile device and our website.

2. Your responsibility generally. You agree to use ordinary care in using the Services. You agree not to share your mobile device or your username or password with others. You agree to protect your device against loss, theft or unauthorized use and you agree to follow the security recommendations that we make to you from time to time. You must not leave your mobile device unattended while logged into the Services and you must log off immediately at the completion of each session. You agree to notify us immediately if your device is lost or stolen or if you believe the security of your username or password has been compromised. You are responsible for protecting your mobile device against viruses, key loggers, malware and other unwanted functionalities. You must not use your mobile device through an unsecured network (such as public Wi-Fi) or from a location outside the United States. You also agree to monitor the activity in your bank accounts and to keep informed of any changes the Services by diligently using the Services and other information we make available. You understand that we may monitor any and all communications and transactions in connection with the Services. You agree to cooperate with any reviews, audits or investigations that we conduct related to your use of the Services. **FAILURE TO PROTECT YOUR MOBILE DEVICE OR YOUR USERNAME AND PASSWORD OR FAILURE TO COMPLY WITH THESE TERMS MAY RESULT IN SOMEONE ELSE BEING ABLE TO ACCESS THE SERVICES AND/OR YOUR BANK ACCOUNTS IN YOUR NAME. WE WILL**

CONSIDER ANY ACCESS AND ANY TRANSACTION USING YOUR USERNAME AND PASSWORD AS AUTHORIZED BY YOU. YOU ASSUME, TO THE FULLEST EXTENT ALLOWED BY LAW, ALL RISK OF FRAUDULENT OR UNAUTHORIZED ACCESS AND TRANSACTIONS MADE WITH YOUR USERNAME AND PASSWORD.

3. Your responsibility for losses. You accept responsibility for the losses we suffer in connection with providing the Services to you. More specifically, you agree to indemnify, defend and hold us harmless from and against any and all liabilities, claims, losses, costs, damages and expenses (including reasonable attorneys' fees) related to: (i) any third party claims arising out of our provision of the Services to you, including any responsibility that we have to third parties for handling or being associated with any transaction you initiate or any item or file that we create to collect your deposit; (ii) your failure to fulfill your responsibilities or your breach of any of your representations or agreements in these Terms or any other agreement with us; or (iii) your acts, omissions, errors, requests, instructions, transactions or deposits. You are not required to indemnify us for our willful misconduct. Your responsibility under this paragraph survives any termination of the Services or our relationship.

4. Additional terms. These Terms supplement our Deposit Account Agreement(s) for your account(s). Limitations, fees and other terms in those agreements may apply to the Services when relevant (and references in those agreements to "Services" should be considered to include the mobile banking services). Termination of those agreements or relationships will result in the Services being unavailable to you. The Services may involve the use of clearing systems or other networks or associations (altogether, the "Associations"). The Services are provided subject to the Associations' rules, all which you agree to comply with when relevant. You agree that we are not responsible for the acts or omissions of any Association or its members. If you download an app in connection with the Services, you agree to comply with the terms and conditions applicable to that app, in addition to these Terms. You have no right, title, or interest in any app that you download or in any intellectual property relating to that app. You agree not to copy, reproduce, reverse engineer, decompile or disassemble any app. You agree not to use any app except to access the Services.

5. IMPORTANT NOTICE REGARDING CHANGES IN TERMS AND DISCONTINUATION OF SERVICES. Subject to applicable law, we may unilaterally change these Terms from time to time. This includes modifications, deletions and the addition of new provisions and fees. If we make changes, we will update these Terms on our website and we will send you notice of the change if required by law. Changes will be automatically effective on the date we specify and without the necessity of any further assent on your part. We may suspend or discontinue the Services at any time, with or without cause. These Terms will survive after any suspension or discontinuation.

6. Our liability. We will use ordinary care in providing the Services. We do not guarantee that the Services will be uninterrupted or error free. We are not responsible for problems with your mobile device, for interruptions to or problems with your wireless service, or for losses or errors that occur during the transmission of information to or from us. We may have liability to you imposed by statute which cannot be waived -- except for that liability, **IN NO EVENT WILL WE BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, REGARDLESS OF WHETHER WE WERE INFORMED OF THEIR POSSIBILITY. THE SERVICES ARE PROVIDED AS IS AND WE DISCLAIM ANY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WRITTEN OR ORAL IN RESPECT OF THE SERVICES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.** The preceding limitations of liability apply regardless of whether any limited remedy herein fails of its essential purpose.

Mobile Deposit

7. What is the mobile deposit service and how does it work? The mobile deposit service provides a way for you to deposit certain checks and other instruments (collectively, "checks") by using your mobile device to send us certain information along with an image of the checks. A mobile deposit may not be

provisionally credited to your account until the next business day (every day is a business day, except Saturdays, Sundays and federal holidays) if we receive it after 2:00 p.m. Central Time or on a day that is not a business day. Funds from these deposits will not be available immediately. These deposits are not addressed by the Funds Availability Policy that we have previously provided to you. We may nonetheless choose (but are not obligated) to treat them as subject to that policy, including the exceptions and holds referenced in that policy. Funds from these deposits will not be made available faster than any other deposit. We may convert the information and images you submit into a differently formatted item and may then collect that item in the manner we choose. Even though we may have sent you a confirmation or receipt, if your items are not finally paid or are returned to us for any reason, we may reverse the credit to your account. Returned items will be available to you in a format we select.

8. There are limitations. You may not use the mobile deposit service to deposit any single item that exceeds $1,000 or multiple deposits that exceed $3,000 on any one business day. If we allow you to exceed these limits, your deposit will still be subject to these Terms and we will not be obligated to let you exceed the limits again. These limitations are subject to change at any time without advance notice. We may reject any image or deposit that you submit because it does not satisfy our requirements or for other reasons or no reason. We may reject a deposit even if we have indicated to you that the image was successfully submitted. We are not responsible for the losses you may suffer because we reject an image or a deposit. If we reject an image or a deposit, you may still attempt an in-person deposit of the original paper check.

9. Proper use of the service. You agree to comply with the instructions and restrictions we provide from time to time (this includes, for example, the instructions provided via our mobile banking app). You agree not to deposit any check that has been previously negotiated or: (1) any check drawn on a Northeast Security Bank account that you own; (2) any check drawn on an institution located outside the United States; (3) any check that is damaged, illegible, altered or incomplete; (4) any check that is marked "nonnegotiable," that is more than 6 months old or that is not the original of the check; (5) any US Treasury check; or (6) any other check that we designate as ineligible. You are responsible for assuring that:

(a) each check you deposit is properly endorsed before you make an image of it. After a mobile check deposit has been "Accepted" you must write the words "ALREADY DEPOSITED" on the front of your check;

(b) each image you submit is completely legible and that it accurately represents all of the information on the front and back of the original check, including all endorsements;

(c) all information you send with each check image accurately reflects the original check and the image of the check you send us;

(d) no deposit will include any duplicate checks and no deposit will include any amount for a check that has already been presented to or deposited with us or any other institution;

(e) no check reflected in a mobile deposit with us or any image of such a check will be subsequently transferred to anyone else or presented to or deposited with another institution;

(f) after you make your mobile deposit, the original paper checks will be stored securely by you for no less than 14 days and no more than 180 days. You will make those original checks available to us on request; and

(g) the original checks will be completely and securely destroyed following the above time period, unless doing so would be a violation of law (original checks should not be disposed of in the garbage unless they are shredded first). You may not make or keep any other copies of the checks you deposit.

After you submit a mobile check deposit you should later return to the Touch Banking application and verify the mobile deposit has been "Accepted". Notify us right away if you don't receive this message. If you do not do this within one business day after submitting your item you agree not to make a claim later about that deposit. You agree not to use the Services in any manner or in connection with any activity that constitutes a violation of any law or that may subject us to legal action.

10. Your responsibility for these deposits. Each time you use the mobile deposit service, you are authorizing us to accept the relevant deposit to your account and you are representing to us that:
(a) the deposit is of a check payable to and endorsed by you and reflects a bona fide payment to you by the drawer of the check;
(b) the check is not being deposited, directly or indirectly, for the benefit of any other person or entity;
(c) you are not aware of any reason that the check will not be paid; and
(d) as to each check reflected in a deposit: (i) you are a person entitled to enforce the check; (ii) the check has not been altered; (iii) the check bears all endorsements applied by parties that previously handled the check in any form (if any); and (iv) no person will be charged for the check, or another paper or electronic representation of the check, such that they will be asked to make payment for a check or item that they have already paid.
For each check and the item it is converted into, you also accept the same responsibilities and liabilities that you would have had if you had deposited the original check in person. You have all these responsibilities and are subject to these Terms with respect to every deposit that is made using your username and password. You agree to notify us immediately if any original checks are lost or stolen after they are deposited.

Northeast Security Bank Alerts Terms and Conditions

Alerts. Your enrollment in Northeast Security Bank Online Banking and/or Mobile Banking (the "Service") includes enrollment to receive transaction alerts and notifications ("Alerts"). Alerts are electronic notices from us that contain transactional information about your Northeast Security Bank account(s). Account Alerts and Additional Alerts must be managed and/or added online through the Service. We may add new alerts from time to time, or cancel old alerts. We usually notify you when we cancel alerts, but are not obligated to do so. Northeast Security Bank reserves the right to terminate its alerts service at any time without prior notice to you.

*Methods of Delivery. We may provide alerts through one or more channels ("**endpoints**"): (a) a mobile device, by text message, (b) a mobile device, by push notification; (c) an email account, by an e-mail message; or (d) your Northeast Security Bank Online Banking message inbox. You agree to receive alerts through these endpoints, and it is your responsibility to determine that each of the service providers for the endpoints described in (a) through (c) above supports the email, push notification, and text message alerts provided through the alerts service. Please be advised that text or data charges or rates may be imposed by your endpoint service provider. Alert frequency varies by account and preferences. You agree to provide us a valid mobile phone number or email address so that we may send you alerts. If your email address or your mobile device's number changes, you are responsible for informing us of that change. Your alerts will be updated to reflect the changes that you communicate to us with regard to your primary and secondary email addresses or mobile device number.*

Alerts via Text Message. To stop alerts via text message, **text "STOP" to 96924 at anytime.** Alerts sent to your primary email address will be unaffected by this action. To restore alerts on your mobile phone, just visit the alerts tab in Northeast Security Bank Online Banking. For help with SMS text alerts, text "HELP" 96924. In case of questions please contact customer service at 563-578-3251. Our participating carriers include (but are not limited to) AT&T, SprintPCS, T-Mobile®, U.S. Cellular®, Verizon Wireless, MetroPCS.

Limitations. {name of Financial Institution} provides alerts as a convenience to you for information purposes only. An alert does not constitute a bank record for the deposit or credit account to which it pertains. We strive to provide alerts in a timely manner with accurate information. However, you acknowledge and agree that your receipt of any alerts may be delayed or prevented by factor(s) affecting your mobile phone service provider, internet service provider(s) and other factors outside Northeast

Security Bank's control. We neither guarantee the delivery nor the accuracy of the contents of each Alert. You agree to not hold Northeast Security Bank, its directors, officers, employees, agents, and service providers liable for losses or damages, including attorneys' fees, that may arise, directly or indirectly, in whole or in part, from (a) a non-delivery, delayed delivery, or the misdirected delivery of an Alert; (b) inaccurate or incomplete content in an Alert; or (c) your reliance on or use of the information provided in an Alert for any purpose.

Alert Information. As alerts delivered via SMS, email and push notifications are not encrypted, we will never include your passcode or full account number. You acknowledge and agree that alerts may not be encrypted and may include your name and some information about your accounts, and anyone with access to your alerts will be able to view the contents of these messages.