Kinderhook Bank

Consumer Online Banking Security

Kinderhook Bank uses the most advanced security available on the Internet today. The same level of security used in our branches and ATM machines is also employed in our Online Banking product. All sensitive information is encrypted and online access requires a Personal User ID and a password known only to you. (Note: Only valid account-holders should know the Online Banking User ID and Online Banking User Password)

Kinderhook Banks' state-of-the-art technologies are designed to provide cutting edge protection of your personal information.

About Security

At Kinderhook Bank, we recognize security concerns and we are serious about security issues. In addition to our high security standards offline, we incorporate many security tiers into Kinderhook Banks' system. Every possible effort is made to ensure that your account information is protected from unauthorized access. For questions regarding security issues, please call (518) 758-7101 and ask for the Online Banking Department.

SSL and Firewalls

Kinderhook Banks Online Banking application ***eCom*** is accessed through a Secure Socket Layer (or SSL). This means all data transmitted to or from Kinderhook Banks' online banking system is encrypted using the most sophisticated security available to protect your money and privacy. Firewalls exist to prevent unauthorized access to the system and to ensure your information is accessible only by using a correct Online Banking User ID and Online Banking User Password.

Email Solicitation

Kinderhook Bank **does not** solicit information (SSN, account numbers, credit card numbers, passwords, etc) by means of email. If you receive an email requesting confidential information from someone claiming to represent Kinderhook Bank, do not respond to the email. Please call (518) 758-7101 to report any solicitation of this kind that you receive.

Other Solicitations

The Bank will never contact any customer and request electronic banking credentials. If you get a call asking for your credentials, hang up and call our Online Banking Department at (518) 758-7101.

Passwords

As an added layer of security, our Online Banking application requires that your password contain certain characters such as upper and lower-case letters, numbers and special characters. Passwords containing such characters are considered "strong passwords" and are difficult for others to guess.

Three Strikes Rule

It is very important that only you know your Access ID and Password. This is the only way your account may be accessed. After three (3) unsuccessful access attempts, eCom will lock out the User from accessing their account. If a user becomes locked out, he/she must call the Kinderhook Bank Online Banking Department at (518) 758-7101 to have their access reset.

Extended Validation (EV) Certificate

Our Online Banking application utilizes an Extended Validation (EV) certificate which can be identified by the GREEN URL address bar on our password page. This security feature provides our customers with visual confirmation that they are on our VALID website and NOT a fraudulent, spoofed website designed to look like our website.

The EV certificate triggers web browsers to display a GREEN address bar and the website identification certificate will identify our site provider's name (Fiserv, Inc.).

Account Numbers Not Visible

When viewing your account online, your account number is truncated or masked meaning that only part of your account number can be viewed to help you distinguish between your accounts while protecting your full account number from view.

Automatic Log Off

After a ten-minute period of inactivity, the system will automatically log you off and force you to re-enter your User ID and Password.

Changing Your Password

Changing your password periodically is an important step in protecting your information online. In order to ensure this protection, we require that your change your password every ninety (90) days.

Your Role in Security

- Choose a good User Password! You should carefully select a Password that is hard to guess and never use a word that can be found in the dictionary.
- Memorize your User Password! Even the best password is worthless if it's written on a note attached to your computer or an entry in your checkbook.
- Don't share your Online Banking User Password with anyone else. Your User Password is designed to protect the privacy of your banking information, but it will only work if you keep it to yourself. If you think your User Password has been compromised, change it immediately online and immediately contact the Bank. Call us at (518) 758-7101 or send us a note using the tab labeled Contact Us link at the top of our web page.
- Change your Password as often as you wish.
- Don't leave your computer unattended during an *eCom* session - click on "Log Out" to end your session.
- Once you have finished conducting your banking online, always sign off before visiting other Internet sites.
- Avoid using Public Internet Access Terminals when conducting your Online Banking.

Online Banking Security Precautions

Recently, Kinderhook Bank ("Bank") has seen significant changes in the Online banking threat landscape. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits. Fraudsters are responsible for losses of hundreds of millions of dollars resulting from online account takeovers and unauthorized funds transfers. The Bank is providing the below security awareness information for your use and action to help protect your online account and transaction information.

Tips to Reduce Online Banking Risk and Avoid Online Fraud:

- **Sign up for electronic statements** to help prevent mail fraud (https://www.nubk.com/personal-banking-convenience-services.htm).
- **Sign up for Messenger** to receive text or email alerts about account activity.
- **Review your account activity** regularly to detect fraud earlier.

- **View images of cleared checks** to identify any irregularities.
- After signing up for Online Banking, **sign up for Bill Pay** to help prevent mail fraud.
- **Protect your password**.
- Ensure your operating system includes **firewall protection**.
- Install, run and maintain updates of **anti-virus or anti-spyware software**.
- Ensure that all Web **sites used for shopping or initiating transactions are secure**.
- **Avoid downloading programs from unknown sources**.
- Log off completely and **close your browser after logging off**.
- Always **disconnect** your online access when it is not in use.
- **Avoid replying to any e-mails requesting personal information**; never include personal information in an e-mail sent through an unsecured environment.
- Update your browser with at least **128-bit encryption**.
- **Check our Fraud Alerts** regularly to stay informed about the latest security issues and prevention advice.
- Provide full cooperation in the investigation and prosecuting of individuals responsible for unauthorized activity on your account.
- **Block cookies on your Web browser:** When you surf, hundreds of data points are being collected by the sites you visit. These data get combined together to form an integral part of your "digital profile," which is then sold without your consent to companies around the world. By blocking cookies, you'll prevent some of the data collection about you. Yes, you'll have to enter passwords more often, but it's a smarter way to surf.
- **Don't put your full birth date on your social-networking profiles**: Identity thieves use birth dates as cornerstones of their craft. If you want your friends to know your birthday, try just the month and day, and leave off the year.
- **Don't download Facebook apps from outside the United States**: Apps on social networks can access huge amounts of personal information. Some unscrupulous or careless entities collect lots of data and then lose, abuse, or sell them. If the app maker is in the U.S., it's probably safer, and at least you have recourse if something should ever go wrong.
- **Use multiple usernames and passwords**: Keep your usernames and passwords for social networks, online banking, e-mail, and online shopping all separate. Having distinct passwords is not enough nowadays: if you have the same username across different Web sites, your entire personal, professional, and e-commerce life can be mapped and re-created with some simple algorithms. It's happened before.

- Online Banking Problems, Concerns, or something doesn't look right? **Call us** at (518) 758-7101

Important Note: While we continue to do everything possible to ensure the security of our system, we are not responsible for any breach of security that is outside of our control.

Below are the protections and liabilities for consumer transactions using Kinderhook Banks' Online Banking program:

To access our Online Banking service, you must use the Access ID and/or other means of access we establish or provide for your Online Banking Customer Account together with a Password. It is your responsibility to safeguard the User ID and Password. Anyone to whom you give your Online Banking Access ID and Password or other means of access will have full access to your accounts even if you attempt to limit that person's authority

You or someone you have authorized by giving them your Online Banking User ID and Password or other means of access (even if that person exceeds your authority), can instruct us to perform the following transactions:

- Make transfers between your qualifying accounts to the extent authorized;
- Obtain information that we make available about your qualifying accounts;
- Obtain other services or perform other transactions that we authorize (e.g. bill payments)

You must have enough money or credit in any account from which you instruct us to make a payment or transfer. You also agree to the Terms & Conditions of your deposit account that you received when you opened your deposit account.

Statements

Your Online Banking payments and transfers will be indicated on the monthly or quarterly statements we provide. Please notify us promptly if you change your address or if you believe there are any errors or unauthorized transactions on any statement, or statement information.

UNAUTHORIZED TRANSACTIONS OR LOSS OF THEFT OF YOUR ONLINE BANKING ACCESS ID OR PASSWORD

If you believe that your Online Banking Access ID or password or other means of access have been lost or stolen, or that someone has used them without your authorization, call us immediately at (518) 758-7101, during normal business hours. After hours you may notify us by going to the "Contact Us" tab on our Website and completing the information in the box provided. Immediately contacting us by phone is the best way of reducing your possible losses. If you notify us by using the secure Contact Us form, we will send an e-mail back to you or call you as confirmation that we did receive it. If you have given someone your Online Banking Access ID or Password or other means of access and want to terminate that person's authority, you must contact our Online Banking Department at (518) 758-7101 to change your Access ID and Password or other means of access or take additional steps to prevent further access by such person.

You may terminate your Online Banking Agreement at any time upon giving the Bank written notice of the termination. If you terminate, you authorize us to continue making transfers you have previously authorized until we have had a reasonable opportunity to act upon your termination notice. Once we have acted upon your termination notice, we will make no further transfers or payments from your Online Banking Account. If we terminate your use of your Online Banking Account, we reserve the right to make no further transfers of payments from your account including any transactions you have previously authorized.

You are responsible for all transfers you authorize using the Online Banking services under your Online Banking Agreement. If you permit other persons to use your Access Code, you are responsible for any transactions they authorize or conduct on any of your accounts. However, tell us at once if you believe anyone has used your Access Code and gained entry to your accounts without your authority. Telephoning is the best way of keeping your possible losses down.

Consumer Accounts - The following three paragraphs apply only to **consumer accounts** (an account belonging to a natural person and used primarily for personal, family, or household purposes):

For Online Banking transactions for **consumer accounts**, if you tell us within 2 business days, you can lose no more than $50 if someone accessed your account without your permission. If you do not tell us within 2 business days after you learn of the unauthorized use of your account or Access ID, and we can prove that we could have prevented the unauthorized transaction(s) if you had told us in time, you could lose as much as $500 or more. Your liability for unauthorized loan transactions through the Online Banking service will not exceed $50.00. Also, if your statement shows Online Banking transfers that you did not make, tell us at once. If you do not tell us within sixty (60) days of the mailing date of your statement, you may be liable for the full amount of the loss if we can prove that we could have prevented the unauthorized transactions if you had told us in time. Should some emergency such as extended travel or hospitalization prevent you from contacting us, a reasonable extension of time will be allowed.

If you tell us orally, we may require that you send us your complaint or question in writing within ten (10) business days. We will tell you the results of our investigation within ten (10) business days after we hear from you and will correct any error promptly. For errors related to transactions occurring within thirty (30) days after the first deposit to the account (new accounts), we will tell you the results of our investigation within twenty (20) business days. If we need more time, however, we may take up to forty-five (45) days to investigate your complaint or question (ninety (90) calendar days for new account transaction errors, or errors involving transactions initiated outside the United States). If we decide to do this, we will re-credit your account within ten (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. If we ask you to put your complaint or

question in writing and we do not receive it within ten (10) business days, we may not re-credit your account.

If we decide after our investigation that an error did not occur, we will deliver or mail to you an explanation of our findings within three (3) business days after the conclusion of our investigation. If you request, we will provide you copies of documents (to the extent possible without violating other members' rights to privacy) relied upon to conclude that the error did not occur.

Limitation of Liability for Online Banking Services - The Bank's sole responsibility for an error in a fund transfer or bill payment will be to correct the error, but in no case shall the Bank be liable for any indirect, punitive, special, incidental, or consequential damages (even if you have informed us of the possibility of such damages). You agree that neither we nor the service providers shall be responsible for any property damage or loss, whether caused by the equipment, software, the Bank, or by Online browser providers such as Netscape (Netscape Navigator browser) and Microsoft (Microsoft Internet Explorer browser), or by Internet access providers or by online service providers or by an agent or subcontractor of any of the foregoing. Neither we nor the service providers will be responsible for any direct, indirect, special or consequential economic or other damages arising in any way out of the installation, download, use, or maintenance of the equipment, software, the Bank Online Banking services or Internet Browser or access software. In this regard, although we have taken measures to provide security for communications from you to us via the Bank Online Banking Services, and may have referred to such communication as "secured," we cannot and do not provide any warranty or guarantee of such security. In states that do not allow the exclusions or limitation of such damages, our liability is limited to the extent permitted by applicable law.

Additionally, the Bank will not be liable for the following:

- If, through no fault of ours, you do not have enough money in your account to complete a transaction, your account is inactive or closed, or the transaction amount would exceed the credit limit on your line of credit.
- If you used the wrong Access ID or you have not properly followed any applicable computer, Internet, or the Bank user instructions for making transfer and bill payment transactions.
- If your computer fails or malfunctions or the Online Banking service was not properly working and such problem was or should have been apparent when you attempted such transaction.
- If, through no fault of ours, a bill payment or funds transfer transaction does not reach a particular creditor and a fee, penalty, or interest is assessed against you.
- If circumstances beyond our control (such as fire, flood, telecommunications outages, strikes, equipment or power failure) prevent the transaction.
- If the funds in your account are subject to legal process or other claim, or if your account is frozen because of a delinquent loan, overdrawn account, or suspected fraud.

- If the error was caused by a system beyond the Bank's control such as a telecommunications system, or Internet service provider.
- If you have not given the Bank complete, correct, or current information so the Bank can process a transaction.

Billing Errors - In Case of Errors or Questions about Your Electronic Transfers, telephone us at (518) 758-7101 or write us at Kinderhook Bank, 1 Hudson St. Kinderhook, NY 12106 or E-mail us using our secure online Contact Us page at: https://www.nubk.com/a_contact.asp as soon as you can, if you think your statement or receipt is wrong or if you need more information about a transfer 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 appeared.

(1) Tell us your name and account number (if any).

(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 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. 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 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.